Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт Кибернетики
Направление подготовки 09.04.01 Информатика и вычислительная техника
Кафедра Информационных систем и технологий

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка программно- аппаратного комплекса автоматизированной оплаты проезда в общественном транспорте

УДК 004.3/.4:656.025.222-52

Студент

Группа	ФИО	Подпись	Дата
8ВМ5А	Россамахин Дмитрий Игоревич		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель каф. ИСТ	Друки Алексей Алексеевич	к.т.н.		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. МЕН	Конотопский Владимир Юрьевич	к.э.н., доцент		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. ЭБЖ	Извеков Владимир Николаевич	к.т.н., доцент		

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
Зав. кафедрой ИСТ	Мальчуков Андрей Николаевич	к.т.н., доцент		

Томск – 2017 г.

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт Кибернетики
Направление подготовки 09.04.01 Информатика и вычислительная техника
Кафедра Информационных систем и технологий

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка программно- аппаратного комплекса автоматизированной оплаты проезда в общественном транспорте

УДК 004.3/.4:656.025.222-52

Студент

Группа	ФИО	Подпись	Дата
8ВМ5А	Россамахин Дмитрий Игоревич		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель каф. ИСТ	Друки Алексей Алексеевич	к.т.н.		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. МЕН	Конотопский Владимир Юрьевич	к.э.н., доцент		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. ЭБЖ	Извеков Владимир Николаевич	к.т.н., доцент		

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
Зав. кафедрой ИСТ	Мальчуков Андрей Николаевич	к.т.н., доцент		

Томск – 2017 г.

ЗАПЛАНИРОВАННЫЕ РЕЗУЛЬТАТЫ ПО ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ ПОДГОТОВКИ МАГИСТРОВ 09.04.01 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА», ИК ТПУ, ПРОФИЛЬ «КОМПЬЮТЕРНЫЙ АНАЛИЗ И ИНТЕРПРЕТАЦИЯ ДАННЫХ»

Планируемые результаты обучения

Код результатов	Результат обучения (выпускник должен быть готов)	Требования ФГОС ВО (ФГОС 3+), критерии АИОР, заинтересованных работодателей и студентов
Общепрофессиональные компетенции		
P1	Воспринимать и самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте.	Требования ФГОС 3+ (ОПК-1; ПК 3-6; ОК-4), критерий 5 АИОР (п. 1.1), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
P2	Владеть и применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях.	Требования ФГОС 3+ (ОПК-5; ПК-7; ОК-7), критерий 5 АИОР (п. 1.1, 1.2), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
P3	Демонстрировать культуру мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных, анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде	Требования ФГОС 3+ (ОПК-6; ПК-1,2; ОК-1,2), критерий 5 АИОР (п. 1.2), соответствующий международным стандартам EUR-ACE и

Код результатов	Результат обучения (выпускник должен быть готов)	Требования ФГОС ВО (ФГОС 3+), критерии АИОР, заинтересованных работодателей и студентов
	аналитических обзоров с обоснованными выводами и рекомендациями.	FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р4	Анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности. Владеть, по крайней мере, одним из иностранных языков на уровне социального и профессионального общения, применять специальную лексику и профессиональную терминологию языка.	Требования ФГОС 3+ (ОПК-3,4; ПК-11,12; ОК-3), критерий 5 АИОР (п. 1.6, п. 2.2), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Профессиональные компетенции		
Р5	Выполнять инновационные инженерные проекты по разработке аппаратных и программных средств автоматизированных систем различного назначения с использованием современных методов проектирования, систем автоматизированного проектирования, передового опыта разработки конкурентно способных изделий.	Требования ФГОС 3+ (ПК-8–12; ОПК-2, ПК-7,6), критерий 5 АИОР (п. 1.3), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р6	Планировать и проводить теоретические и экспериментальные исследования в области проектирования аппаратных и программных средств автоматизированных систем с использованием новейших достижений науки и техники, передового отечественного и зарубежного опыта. Критически оценивать полученные данные и делать выводы.	Требования ФГОС 3+ (ПК-1–7; ОПК-6; ОК-4,9), критерий 5 АИОР (п.1.4), соответствующий международным стандартам EUR-ACE и FEANI.

Код результатов	Результат обучения (выпускник должен быть готов)	Требования ФГОС ВО (ФГОС 3+), критерии АИОР, заинтересованных работодателей и студентов
		Запросы студентов, отечественных и зарубежных работодателей.
Р7	Осуществлять авторское сопровождение процессов проектирования, внедрения и эксплуатации аппаратных и программных средств автоматизированных систем различного назначения.	Требования ФГОС 3+ (ПК-13–19; ОПК-5; ОК-8), критерий 5 АИОР (п. 1.5), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Общекультурные компетенции		
Р8	Использовать на практике умения и навыки в организации исследовательских, проектных работ и профессиональной эксплуатации современного оборудования и приборов, в управлении коллективом.	Требования ФГОС 3+ (ОК-5,8; ОПК-1,6; ПК-6,7,11,12), критерий 5 АИОР (п. 2.1, п. 2.3, п. 1.5), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р9	Осуществлять коммуникации в профессиональной среде и в обществе в целом, активно владеть иностранным языком, разрабатывать документацию, презентовать и защищать результаты инновационной инженерной деятельности, в том числе на иностранном языке.	Требования ФГОС 3+ (ОК-2,9; ОПК-4; ПК-1), критерий 5 АИОР (п. 2.2), соответствующий международным стандартам EUR-ACE и FEANI.

Код результатов	Результат обучения (выпускник должен быть готов)	Требования ФГОС ВО (ФГОС 3+), критерии АИОР, заинтересованных работодателей и студентов
		Запросы студентов, отечественных и зарубежных работодателей.
Р10	Совершенствовать и развивать свой интеллектуальный и общекультурный уровень. Проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности.	Требования ФГОС 3+ (ОК-1,6; ОПК-2; ПК-1,2), критерий 5 АИОР (п. 2.4, п. 2.5) , соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р11	Демонстрировать способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности, способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, способность к педагогической деятельности.	Требования ФГОС 3+ (ОК-3,4,7; ОПК-3; ПК-7), критерий 5 АИОР (п. 2.6), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт Кибернетики
Направление подготовки 09.04.01 Информатика и вычислительная техника
Кафедра Информационных систем и технологий

УТВЕРЖДАЮ:
Зав. кафедрой
_____ _____ Мальчуков А.Н.
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Магистерской диссертации

Студенту:

Группа	ФИО
8ВМ5А	Россамахин Дмитрий Игоревич

Тема работы:

Разработка системы бесконтактной оплаты проезда с функцией сбора статистики	
Утверждена приказом директора (дата, номер)	От 20.02.2017 №898/с

Срок сдачи студентом выполненной работы:	13.06.2017

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе	Спроектировать систему бесконтактной оплаты проезда в общественном транспорте с функцией сбора статистики.
Перечень подлежащих исследованию, проектированию и разработке вопросов	1. Провести анализ имеющихся средств защиты информации для устройств, не обладающих достаточными ресурсами. 2. Реализовать алгоритмы работы программ компонентов системы. 3. Реализовать web – сервер и базу данных, задачей которых будет сбор статистики, управление клиентскими картами, а также другими элементами системы.
Перечень графического материала	1. Структурные схемы алгоритмов функционирования устройств систем.

	2. Структурные схемы разрабатываемых устройств, электрические схемы, структурно-функциональные схемы. 3. Примеры работы реализованных программ.

Консультанты по разделам выпускной квалификационной работы	
Раздел	**Консультант**
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Конотопский Владимир Юрьевич
Социальная ответственность	Извеков Владимир Николаевич

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	

Задание выдал руководитель:

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Старший преподаватель кафедры ВТ	Друки А.А.	к.т.н		

Задание принял к исполнению студент:

Группа	**ФИО**	**Подпись**	**Дата**
8ВМ5А	Россамахин Дмитрий Игоревич		

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт Кибернетики
Направление подготовки (специальность) 09.04.01 Информатика и Вычислительная техника
Уровень образования магистр
Кафедра Информационных систем и технологий
Период выполнения Весенний семестр 2017 учебного года

Форма представления работы:

Магистерская диссертация

(бакалаврская работа, дипломный проект/работа, магистерская диссертация)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	13.06.2017

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
15.02.17	Анализ литературных источников и исходных данных	10
28.02.17	Построение архитектуры системы	10
15.03.17	Разработка аппаратной части	25
30.03.17	Отладка	5
15.04.17	Разработка программной части	25
30.04.17	Отладка	5
15.05.17	Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	10
29.05.17	Социальная ответственность	10

Составил преподаватель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель кафедры ИСТ	Друки А.А.	к.т.н.		

СОГЛАСОВАНО:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8ВМ5А	Россамахин Дмитрий Игоревич

Институт	Кибернетики	Кафедра	Информационных систем и технологий
Уровень образования	Магистрант	Направление/специальность	09.04.01 Информатика и вычислительная техника

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих*	
2. *Нормы и нормативы расходования ресурсов*	
3. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Оценка коммерческого и инновационного потенциала НТИ*	
2. *Разработка устава научно-технического проекта*	
3. *Планирование процесса управления НТИ: структура и график проведения, бюджет, риски и организация закупок*	
4. *Определение ресурсной, финансовой, экономической эффективности*	
Перечень графического материала *(с точным указанием обязательных чертежей):*	
1. *«Портрет» потребителя результатов НТИ* 2. *Сегментирование рынка* 3. *Оценка конкурентоспособности технических решений* 4. *Матрица SWOT* 5. *График проведения и бюджет НТИ* 6. *Оценка ресурсной, финансовой и экономической эффективности НТИ* 7. *Потенциальные риски*	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. МЕН	Конотопский Владимир Юрьевич	к.э.н., доцент		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ5А	Россамахин Дмитрий Игоревич		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8ВМ5А	Россамахин Дмитрий Игоревич

Институт		**Кафедра**	
Уровень образования		**Направление/специальность**	

Исходные данные к разделу «Социальная ответственность»:	
1. *Описание рабочего места (рабочей зоны, технологического процесса, механического оборудования) на предмет возникновения:* – *вредных проявлений факторов производственной среды (метеоусловия, вредные вещества, освещение, шумы, вибрации, электромагнитные поля, ионизирующие излучения)* – *опасных проявлений факторов производственной среды (механической природы, термического характера, электрической, пожарной и взрывной природы)* – *негативного воздействия на окружающую природную среду (атмосферу, гидросферу, литосферу)* – *чрезвычайных ситуаций (техногенного, стихийного, экологического и социального характера)*	
2. *Перечень законодательных и нормативных документов по теме*	
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Анализ выявленных вредных факторов проектируемой производственной среды в следующей последовательности:* – *физико-химическая природа вредности, её связь с разрабатываемой темой;* – *действие фактора на организм человека;* – *приведение допустимых норм с необходимой размерностью (со ссылкой на соответствующий нормативно-технический документ);* – *предлагаемые средства защиты (сначала коллективной защиты, затем – индивидуальные защитные средства)*	
2. *Анализ выявленных опасных факторов проектируемой произведённой среды в следующей последовательности* – *механические опасности (источники, средства защиты;* – *термические опасности (источники, средства защиты);* – *электробезопасность (в т.ч. статическое электричество, молниезащита – источники, средства защиты);* – *пожаровзрывобезопасность (причины, профилактические мероприятия, первичные средства пожаротушения)*	
3. *Охрана окружающей среды:* – *защита селитебной зоны* – *анализ воздействия объекта на атмосферу (выбросы);* – *анализ воздействия объекта на гидросферу (сбросы);* – *анализ воздействия объекта на литосферу (отходы);*	

– *разработать решения по обеспечению экологической безопасности со ссылками на НТД по охране окружающей среды.*	
4. Защита в чрезвычайных ситуациях: – *перечень возможных ЧС на объекте;* – *выбор наиболее типичной ЧС;* – *разработка превентивных мер по предупреждению ЧС;* – *разработка мер по повышению устойчивости объекта к данной ЧС;* – *разработка действий в результате возникшей ЧС и мер по ликвидации её последствий*	
5. Правовые и организационные вопросы обеспечения безопасности: – *специальные (характерные для проектируемой рабочей зоны) правовые нормы трудового законодательства;* – *организационные мероприятия при компоновке рабочей зоны*	
Перечень графического материала:	
При необходимости представить эскизные графические материалы к расчётному заданию (обязательно для специалистов и магистров)	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ5А	Россамахин Дмитрий Игоревич		

РЕФЕРАТ

Выпускная квалификационная работа 131 с., 27 рис., 14 табл., 32 источников, 3 прил.

Ключевые слова: беспроводные технологии, RFID, общественный транспорт, DES шифрование, LW кодирование, web-server, SQL

Объектом исследования являются процесс бесконтактной оплаты, процессы передачи и сбора статистики

Цель работы – проектирование системы бесконтактной оплаты проезда в общественном транспорте, реализация процедуры сбора и вывода статистики.

В процессе исследования проводился обзор существующих систем, выявление преимуществ и недостатков существующих систем, аналитический обзор и подбор компонентов.

В результате исследования были спроектированы структурные, функциональные и электрические схемы устройств, реализована база данных для хранения статистических данных, реализован WEB сервер для отображения статистической информации, реализовано LW кодирование содержимого карты алгоритмом DES, реализовано отладочное устройство для работы с RFID картами.

Основные конструктивные, технологические и технико-эксплуатационные характеристики: работа от бортового АКБ транспортного устройства.

Напряжение питания: +12 В±5%.

Температурный диапазон работы: от минус 40 до плюс 85 градусов по Цельсию.

Относительная влажность окружающей среды от 30 до 80%.

Атмосферное давление в пределах 84-106 кПа.

Степень внедрения:

Область применения: городской общественный транспорт

Экономическая эффективность/значимость работы

В будущем планируется реализация системы в виде стенда, отладка взаимодействия компонентов системы, доработка программной и аппаратной части. Разработка мобильного приложения с привязкой проездного билета к мобильному телефону для проведения платежей

Оглавление

ВВЕДЕНИЕ

Актуальность работы подтверждается новостными источниками г. Томска – «Томичи не хотят работать кондукторами» [1], цитата:

«…к 15 декабря томские перевозчики, выигравшие аукционы, представили в мэрию сведения о кондукторах, и практически все автобусы были обеспечены кондукторами согласно контрактам. Однако позже перевозчики сообщили, что после ввода новой маршрутной схемы кондукторы отработали по два-три дня и ушли, некоторые ушли еще перед Новым годом…

… «Все говорят, что работа очень тяжелая, не соглашаются на эту работу. Претендент на роль кондуктора сразу оценивается, иногда и по внешнему виду не подходит. Те, кто подходит, когда поступают уже на место, почему-то сразу отказываются и уходят. Неоднократно перевозчики говорили, что воровство процветает, то есть, кондуктор получает зарплату и умудряется каким-то образом изъять выручку.»

Власти получают жалобы от пассажиров на работу маршруток, в первую очередь на отсутствие кондукторов, однако это связано с отсутствием желающих идти на эту работу [2].

Водитель маршрутного автобуса, выполняя одновременно возложенные на него обязательства по управлению транспортом и роль кондуктора, что негативно сказывается на концентрации, увеличивая риск аварийных и опасных ситуаций на дороге, а также не может полностью контролировать пассажиропоток и обилечивать всех граждан. Чтобы решить эту проблему, предлагается спроектировать систему автоматизированной оплаты проезда.

Автоматизированная система оплаты проезда(АСОП) предназначена для организации безналичной оплаты проезда и создания технологической основы для реализации новых разнообразных схем обслуживания пассажиров. Система позволяет перевести расчеты за проезд в безналичную форму, большой объем собранных данных о проездах дает возможность их последующего анализа, а в

дальнейшем оптимизации работы транспорта, при этом учесть потребности города, пассажиров и транспортников. АСОП переводит работу всех участников в электронный вид, придает в совокупности с другими электронными системами (глобального позиционирования, систем составления расписания, систем безопасности) больший эффект и современный вид.

Задачи в рамках дипломного проекта:

- Спроектировать систему бесконтактной оплаты проезда в общественном транспорте с функцией сбора статистики.
- Провести анализ имеющихся средств защиты информации для устройств, не обладающих достаточными ресурсами.
- Реализовать алгоритмы работы программ компонентов системы.
- Реализовать web – сервер и базу данных, задачей которых будет сбор статистики, управление клиентскими картами, а также другими элементами системы.

Объект исследования и предмет. Объектом исследования в представляемой работе являются процесс бесконтактной оплаты, процессы передачи и сбора статистики. Предметом исследований является технология бесконтактной передачи данных.

Научная новизна представленной работы состоит в нестандартном технологическом подходе к таким процессам как оплата проезда и сбор статистики. В разрабатываемой системе применяются альтернативном подходы к процессам по обмену и хранению информации и работы с ней. Данная система, при ее полной реализации, позволит значительно упростить операции по построению транспортной логистики города, сделает оплату проезда еще более простой, а также облегчит работу персонала занятой в этой сфере.

Апробация работы. Результаты данной работы отмечены дипломом второй степени в рамках международной научно-технической конференций студентов и молодых ученых «Молодежь. Наука. Технологии» в г.

Новосибирске. Также работа была представлена на Международной научно-технической конференции студентов, аспирантов и молодых учёных «Научная сессия ТУСУР – 2017», посвящённая 55-летию ТУСУРа.

Краткое описание **содержания представленной работы:**

В **первой главе** приведено описание известных аналогов разрабатываемой системы. Проведен анализ достоинств и недостатков систем.

Во **второй главе** приведена общая модель системы, базовые основы исходя из которых проектировалась система, приведена и описана структура данных RFID – карт. Обозначены блоки, в которые происходит запись данных. Приведена краткая информация о методах взлома информации в подобных системах. Подробно описаны алгоритмы шифрования, которые подходят для систем не обладающими достаточными ресурсами.

В **третьей главе** представлена разработка структурных схем алгоритмов устройств, входящих в систему.

В **четвертой главе** приведен пример реализации программной части. Показан отладочный код клиент-сервер, сервер-клиент для связи web – сервера с основным устройством. Также представлена подробная реализация программы des шифрования передаваемой информации. Приведена разработанная база данных для хранения информации системы. Представлен разработанный web – сервер, отвечающий за сбор статистики и её отображение.

В **пятой главе** приведены расчёты и обоснование экономической эффективности проведённой работы.

В **шестой главе** описаны нормы социальной ответственности. Произведён расчёт освещения рабочего помещения, приведены планы эвакуации и меры противопожарной безопасности.

1.ОБЗОР АНАЛОГОВ

Основные системы, используемые в РФ:

- ЕКАРТА (г. Екатеринбург)
- ТРОЙКА (г. Москва)

Краткая информация по данным системам:

ЕКАРТА — система электронной оплаты проезда в общественном транспорте города Екатеринбурга. Реализована в екатеринбургском трамвае, троллейбусе, метрополитене и автобусе (муниципальные и большая часть коммерческих маршрутов). Оператором системы является компания «И-Сеть» (ОАО «Информационная сеть») [2]. 15 июля 2009 года было начато внедрение ЕКАРТЫ в метрополитене города Екатеринбурга. В тестовом запуске приняли участие 200 человек. Выбор участников осуществлялся случайным образом. Более 2,5 тысяч поездок было осуществлено с 15 июля по 2 августа. Продажа ЕКАРТ начались в метрополитене с 1 декабря. Выдача социальных билетов ЕКАРТ - с 7 декабря во всех отделениях Единого расчетного центра. Эксплуатация системы в наземном транспорте стартовала с 1 января 2010 года. Цена одной поездки на этот момент была одинаковой как при оплате ЕКАРТОЙ, так и за наличный расчет и составляла 12 рублей для владельцев социальной карты и 14 рублей для рядовых пассажиров. Помимо этого, ЕКАРТУ можно было использовать как единый проездной на 4 вида транспорта, тариф составлял 300 рублей для владельцев социальной карты и 1500 для других пассажиров, подобного тарифа среди бумажный проездных не существовало [3].

Плюсы системы:

- Универсальность системы
- Массовость системы

Минусы системы:

- Возможность сделать копию карты

- Для оплаты необходимо подносить карту к валидатору
- Необходимость участия кондуктора при оплате

ТРОЙКА – является бесконтактной пластиковой картой Mifare Plus X 2k, которая используется для хранения средств в целях проезда на транспорте; по факту является транспортным электронным кошельком.

Используется после изменения системы тарифов на пользование городским транспортом Москвы 2 апреля 2013 года.

Проездные на некоторое количество поездок ТАТ, «Автобус», «Единый» и «90 минут», без лимитные «Единый», «Автобус» и ТАТ и абонементы на пригородное железнодорожное сообщение можно бесплатно «записать» наа карту «ТРОЙКА»

Перед тем, как это сделать, держателю карты необходимо, если она была приобретена ранее 20 сентября 2013 года, обновить программу носителя (карты) путём пополнения счёта через автоматы по реализации билетов Московского метрополитена, за исключением билетных автоматов, снабженные технологией MasterCard PayPass.

При наличии обновлённой карты держатель может через кассу «записать» необходимый билет. Но использовать денежные средства, уже положенные на счёт для оплаты билета транспортная карта «Тройка» не позволяет. В связи с этим, хоть и на карте может быть достаточное количество денег на счету, держатель не сможет их потратить на покупку билета. Но тем не менее, в связи с этой особенности карты, у пассажира всегда есть возможность оплатить проезд картой, даже если поездки по «записанному» билету кончились или срок его действия истёк [4].

Плюсы системы:

- Универсальность системы

- Отлаженность технологии
- Глобальная сеть по сбору статистики (в метро)
- Высокая степень защищенности системы (в метро)

Минусы системы:

- Возможность сделать копию карты (наземный транспорт)
- Для оплаты необходимо подносить карту к валидатору

2. СПОСОБЫ ЗАЩИТЫ ДАННЫХ

Одним из немаловажных аспектов работы любой системы, связанной с передачей и хранением данных, является их защита от непреднамеренного доступа и изменения. Система, разрабатываемая в данной работе, является наиболее уязвимой, так как присутствует как удаленная передача данных от устройства к устройству (динамическое состояние), так и web - сервера на которых будет храниться большой объем информации (статическое состояние). Защита статической информации на данной уровне системы не является приоритетной, так как в дальнейшем каждый пользователь будет иметь свой вариант по оборудованию для хранения информации и ПО для управления процессов статичной информации.

Наиболее значимым представляется оградить передаваемые данные, исключить утечки и иные вредные воздействия. В связи с этим, возникает потребность понимать принципы кражи динамических данных и соответствующие способы защиты.

Принцип кражи динамических данных - это принцип, согласно которому существует: отправитель данных, получатель данных, канал передачи данных.

Правонарушитель при этом пытается добыть данные в момент, когда информация находится в процессе передачи по каналу данных. На рисунке 1 показано схематичное представление динамической кражи данных:

Рисунок 1. Схематичное представление динамической кражи данных

Как видно из выше приведенного рисунка, правонарушитель работает только с каналом передачи данных, с отправителем или получателем правонарушитель не взаимодействует. Взаимодействовать с каналом передачи данных можно разными способами как с помощью различных программных средств, так и с помощью специализированных физических устройств [5].

Наиболее распространённым способом защиты информации от любых видов перехватов является шифрование данных.

Шифрование данных — это обратимое преобразование данных в целях скрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней [6].

2.1 Алгоритмы шифрования

Алгоритмы шифрования делятся на два больших класса: асимметричные (RSA, El-Gamal) и симметричные (CAST, AES, Blowfish, ГОСТ, DES). В симметричных алгоритмах шифрования используются одни и те же ключи для шифрования данных и для ее расшифровывания, а асимметричные алгоритмы используют два ключа - один для зашифровывания, другой для расшифровывания.

В асимметричных алгоритмах шифрования данных необходимо применять длинные ключи (512 битов и больше). Длинный ключ сильно увеличивает время шифрования. При этом, генерация ключей происходит весьма долго. Зато распределять ключи можно по незащищенным каналам [7].

В симметричных системах используют короткие ключи, т. е. шифрование происходит в разы быстрее. Но в таких системах сложное распределение ключей [8].

Так как в данной системе большую роль играет скорость работы системы, а именно время обработки карты клиента, мы будем рассматривать только симметричные алгоритмы шифрования.

2.2 Алгоритмы LW (low weight)

LW-криптографии - раздел криптографии, который ставит своей целью разработку алгоритмов, применяемых в устройствах, которые по какой либо причине не способны обеспечить большинство существующих алгоритмов шифрования достаточными ресурсами для функционирования.

Ясно, что создание нового алгоритма шифрования с более высокой стойкостью, относительно имеющихся, является довольно сложной задачей, однако существуют несколько алгоритмов показывающих неплохие результаты и некоторые из них способны обеспечивать безопасность RFID-устройств на неплохом уровне [9].

На данный момент существуют как поточные, так и блочные LW-алгоритмы. Известными являются только три поточных LW-шифра, имеющие приемлемые характеристики (MICKEY, Trivium и GRAIN). Однако, из-за особенностей каждого из шифров данные алгоритмы неприменимы в пассивных RFID-системах. Так, в свою очередь, Trivium необходимо достаточно много площади на чипе, превышающая допустимую более чем в полтора раза (3488GE против 2000GE доступных). На текущую версию шифра GRAIN довольно успешно проводятся атака на связанных ключах. Говоря относительно алгоритма MICKEY, разработчиками было проверены лишь несколько способов взлома, этого недостаточно для обеспечения уверенности в его стойкости [10].

Таким образом, на данный момент, можно сделать вывод, что алгоритмы поточных шифров не могут удовлетворять RFID-системам.

Рассмотрим подробнее блочные LW-алгоритмы.

Ниже, в таблице 2 приведены сравнительные характеристики алгоритмов.

Таблица 2. Сравнительные характеристики алгоритмов шифрования

Алгоритм	Размер ключа	Размер блока	Циклов/Блоков	Скорость, kbps	Кол-во, GE
DESL	56	64	144	44.4	1848
KATAN32	80	32	256	12.5	812
KATAN64	80	64	255	25.1	1027
PRESENT-80	80	64	547	11.7	1075
PRESENT-128	128	64	559	11.45	1391
Trivium	80	1	1	100	2599
Grain	80	1	1	100	1294

Для того чтобы использовать алгоритм DES в RFID-системах были проведены его модификации. Были исключены такие перестановки как IP и IP-1, которые не влияют на надежность шифра, однако занимают необходимое место на схеме. Затем, восемь S-блоков, используемых в DES алгоритме, были заменены одним, повторенных в каждом блоке. Создатели данной модификации доказали на практике, что модифицированный ими алгоритм DES стоек к основным атакам, таким как линейный и разностный криптоанализ. Название полученного шифра DESL. Его относительным недостатком является малый размер ключа (56 бит). Но даже при этом, его раскрытие полным перебором требует несколько месяцев работы кластера из нескольких десятков компьютеров, на суперкомпьютере данная задача выполняется за три дня.

Следовательно, DESL алгоритм можно применять там, где требуемая важность защищаемых данных относительно невелика. Под алгоритм необходимо 1848GE, что удовлетворяет стандартам LW-шифрования [11].

Следующий блочный LW-алгоритм, удовлетворяющий всем требованиям RFID-систем - алгоритм PRESENT.

В отличие от алгоритма DESL данный шифр использует более длинный ключ (80 бит), что увеличивает его надежность. Разработчиками проведены исследования стойкости данного алгоритма к разностному и линейному анализу, алгебраической атаке и некоторым другим основным видам атак. PRESENT показал прекрасные результаты для шифра, созданного «с нуля». На данный момент не было проведено ни одной успешной атаки на полную версию алгоритма.

Существуют несколько модификаций PRESENT. Для самой компактной версии требуется всего 1000GE и это одни из лучших результатов среди LW-шифров.

Помимо RFID-систем, некоторые вариации PRESENT нашли применение в других ресурсозависимых устройствах. Так, к примеру, H-PRESENT-128 самая компактная хэш-функций которая существует на данный момент. Кроме того, известно применение LW-алгоритмов в качестве генераторов псевдослучайных чисел в схемах crypto-GPS.

Также среди LW-шифров можно выделить еще KATAN и KTANTAN.

Каждое из семейств представляется тремя шифрами, которые отличаются количеством раундов шифрования: 32, 48 или 64. Шифры имеют ключ из 80-бит. Отличие KTANTAN от KATAN состоит в том, что KTANTAN хватает меньшее количество ресурсов за счёт того, что ключ шифрования не может быть изменен, так как является неизменяемой частью системы. Разработчиками была продемонстрирована стойкость данного алгоритма к таким видам атак как разностный и линейный анализ, алгебраической атаке и на связанных ключах.

Аппаратные реализации разработчиков KTANTAN показывают самые лучшие результаты в области LW-криптографии. Так, алгоритм KTANTAN48

может быть реализован на площади всего 588GE, что почти в два раза меньше, чем самая компактная реализация PRESENT [12].

Однако, несмотря на достаточно неплохие результаты блочных шифров, для них также существует определенный ряд угроз, не позволяющий использовать их повсеместно. Как уже упоминалось ранее, алгоритм шифрования DESL использует относительно короткий ключ, что делает его не применимым для устройств, которым нужна серьезная защита. Алгоритмы PRESENT и KTANTAN несмотря на большое количество исследований, проведенных за последние года, могут нести в себе достаточно серьезные уязвимости, которые скажутся в дальнейшем на их пригодности.

Существует еще немало блочных LW-алгоритмов. Но все они имеют свои недостатки. Например, TWIS и MIBS показывают достаточно хорошие результаты, как в плане быстродействия работы шифра, так и экономичности, однако проведённое небольшое количество их исследований, не позволяет с должной уверенностью судить об их надежности. Другие LW-алгоритмы, такие как mCrypton или HIGHT, требуют для аппаратной реализации слишком много места на чипе.

Таким образом, обобщив выше сказанное, можно заключить, что задача создания как поточного, так и блочного алгоритма шифрования для пассивных RFID-меток до сих пор актуальна и требует решения.

2.3 Алгоритм DES

В данном разделе представлено более полное описание алгоритма DES.

Алгоритм DES — симметричный алгоритм шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт. Основой алгоритма является сеть Фейстеля с шестнадцатью раундами и ключом, имеющим длину 56 бит [13].

Основные достоинства алгоритма DES:

- Для расшифровки не обязательно использовать тот же пакет, что и при расшифровки
- Используется только один ключ длиной 56 битов
- Высокая скорость обработки информации
- Достаточно высокая стойкость алгоритма

Алгоритм DES осуществляет шифрование 64-битных блоков данных используя ключ в 56 бит. Дешифрование в DES является операцией обратной шифрованию и выполняется путем повторения операций шифрования в обратной последовательности.

Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, обратной перестановки битов (рисунок 2,3).

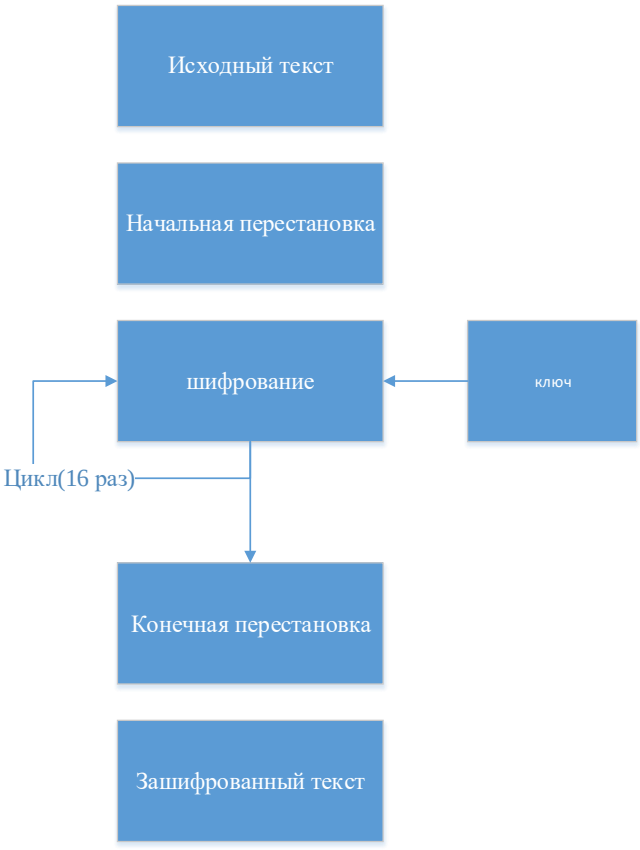


Рисунок 2. Обобщенная схема шифрования в алгоритме DES

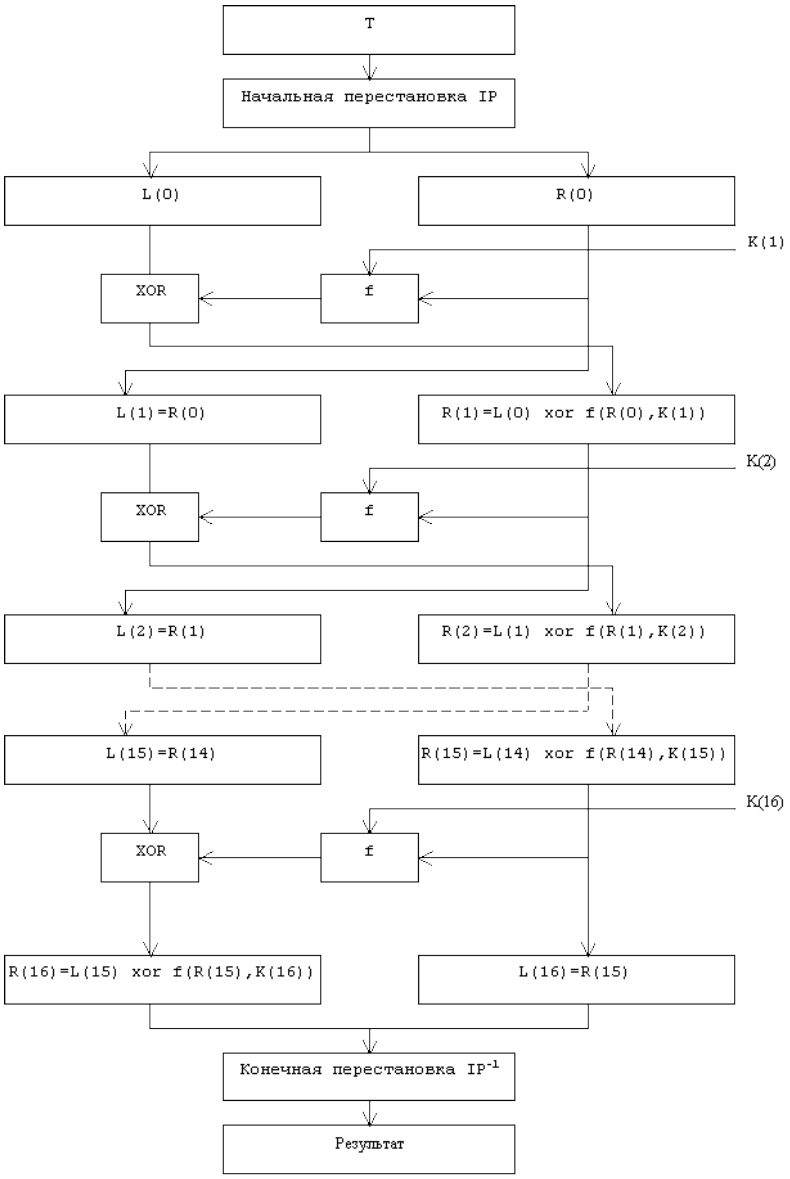


Рисунок 3. Подробная схема шифрования алгоритма DES.

Функция fi называется цикловой функцией, а ключ Ki, используемый для получения функции fi называется цикловым ключом. Как можно заметить, с цикловой функцией складывается только левая половина, а правая остается неизменной. Затем обе половины меняются местами. Это преобразование прокручивается несколько раз (несколько циклов) и выходом шифра является получившаяся в конце пара (l,r) [14].

2.4 Структура данных карты

На рисунке 4 представлена структура данных RFID - карты (сектора со 2-го по 13 не показаны - они идентичны остальным).

Сектор	Блок	Номер байта в блоке															Описание
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
15	3	Ключ А						Биты доступа				Ключ В						Сектор трайлер 15
	2																	Данные
	1																	Данные
	0																	Данные
14	3	Ключ А						Биты доступа				Ключ В						Сектор трайлер 14
	2																	Данные
	1																	Данные
	0																	Данные
(сектора со 2 по 13)																		
1	3	Ключ А						Биты доступа				Ключ В						Сектор трайлер 1
	2																	Данные
	1																	Данные
	0																	Данные
0	3	Ключ А						Биты доступа				Ключ В						Сектор трайлер 0
	2																	Данные
	1																	Данные
	0																	Блок производителя

Рисунок 4. Структура данных RFID - карты

Как видно из выше приведенной таблицы, память RFID - карты разбита на 16 секторов размером по 64 байт. Каждый сектор имеет 4 блока. Последний блок каждого сектора содержит ключи доступа к сектору, что позволяет использовать карту в шестнадцати различных приложениях. За счет того, что каждый сектор имеет индивидуальны ключ, разные приложения не будут конфликтовать друг с другом. Ключи каждого сектора позволяют разграничить права доступа внутри сектора для каждого приложения отдельно. Запись, чтение и на запись-чтение.

Блоки на арте могут быть двух типов, стандартные и блоки value.

Value - блоки, имеющие фиксированный формат и предназначенные для использования сектора в качестве «электронного кошелька».

Нулевой сектор в отличии от остальных содержит в себе только два блока на запись информации. Нулевой блок нулевого сектора содержит в себе идентификационный номер производителя, не подлежащий перезаписи и другим изменениям. Нулевой доступ открыт для чтения и записи всегда, остальным блокам для открытия требуется ключ [15].

На рисунке 5 изображены сектора карты и их блоки памяти, в которые записывается пользовательская информация.

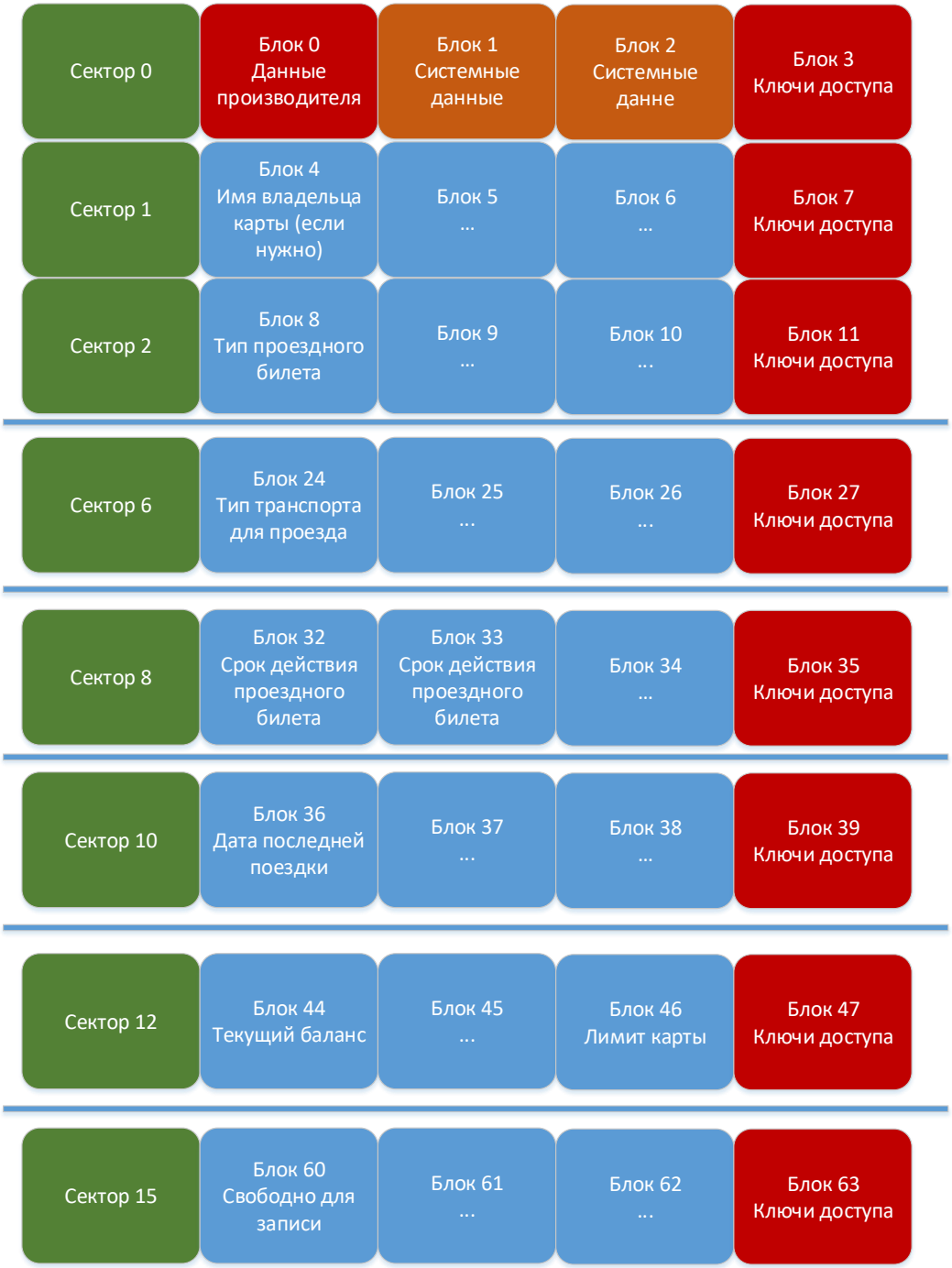


Рисунок 5. Сектора и блоки памяти с пользовательской информацией

3. СТРУКТУРНЫЕ СХЕМЫ АЛГОРИТОМОВ РАБОТЫ УСТРОЙСТВ

Ниже будут представлены структурные схемы алгоритмов работы устройств входящих в систему компонентов.

3.1 Структурная схема алгоритма для управляющего устройства

На рисунке 6 представлена структурная схема алгоритма по работе управляющего устройства с проездной картой.

Рисунок 6. Структурная схема алгоритма по работе с проездной картой

Описание блоков структурной схемы алгоритма по работе с проездной картой:

- Инициализация системы – на данном этапе происходит инициализация всех устройств системы, задание портов ввода/ вывода данных, устанавливается связь с сервером.
- Получение данных с карты – считывание данных с карт пользователей
- Дешифрование данных – информация на карте хранится в зашифрованном виде, для ее изменений требуется дешифровка.
- Проверка данных – после дешифровки происходит проверка карт по балансу и по срокам эксплуатации.
- Изменение данных – в случае корректности данных карты пользователя происходит их изменение, а именно списание поездки.
- Шифрование данных – для обратной записи информации данных снова шифруются.
- Запись данных на карту – после всех операций с данными происходит их запись на карту.

3.2 Структурная схема алгоритма работы управляющего устройства

На рисунке 7 представлена структурная схема алгоритма по работе управляющего устройства с сервером.

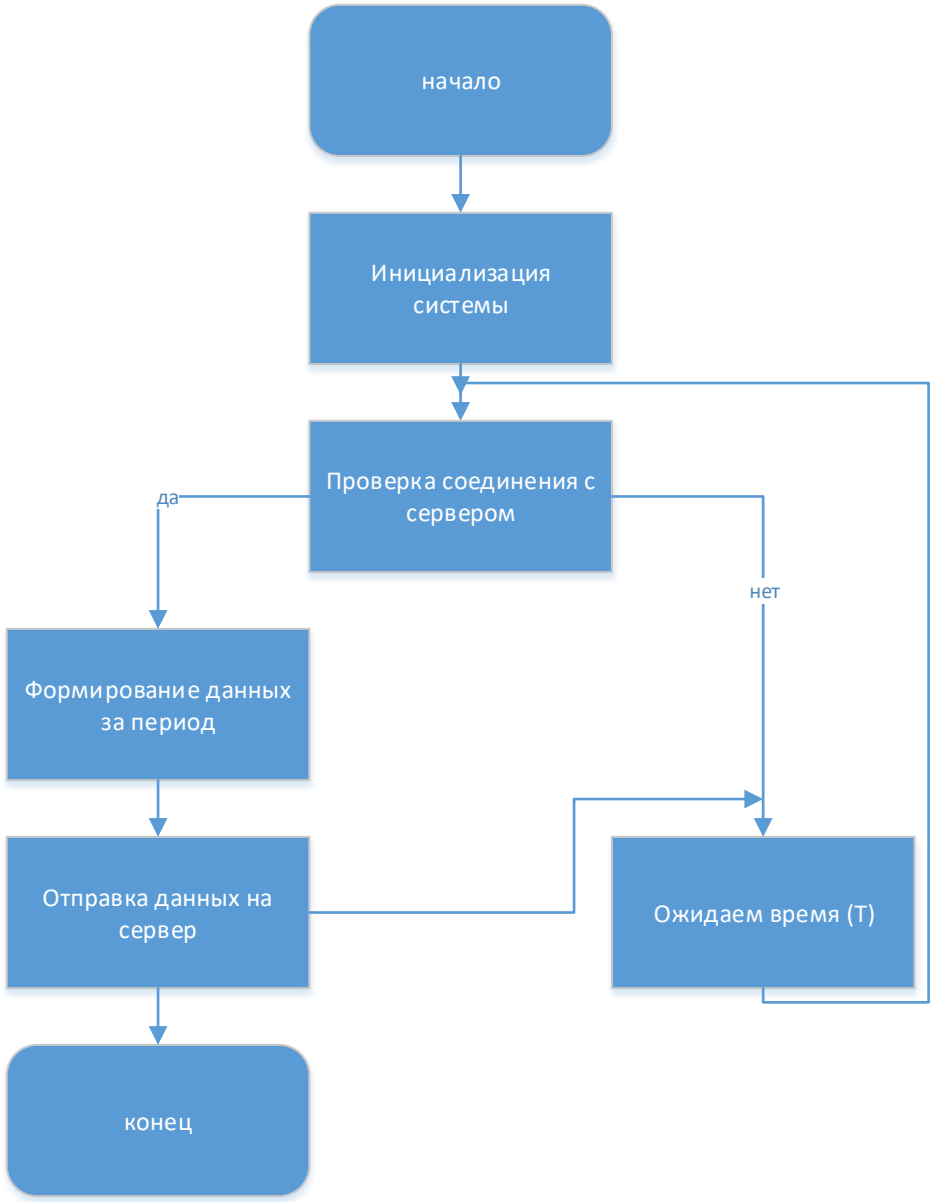


Рисунок 7. Структурная схема алгоритма по работе с сервером

Описание блоков структурной схемы алгоритма по работе с сервером:

- Инициализация системы – на данном этапе происходит инициализация всех устройств системы, задание портов ввода/ вывода данных, устанавливается связь с сервером.
- Проверка соединения управляющего устройства с сервером. В случае если соединение не установлено, устройство уходит в состояние ожидания до следующего сеанса передачи данных.
- На этапе формирования данных за период происходит формирование информации, собранной с системы. Передаются такие параметры как UID задействованных карт в период, время активации карты и координаты (широта, долгота) взаимодействия пользовательской карты с системой.
- После формирования данных происходит выгрузка их на сервер. Из полученной информации составляется общая статистика по загруженности транспортной сети.

3.3 Структурная схема алгоритма для терминала

На рисунке 8 представлена структурная схема алгоритма работы терминала.

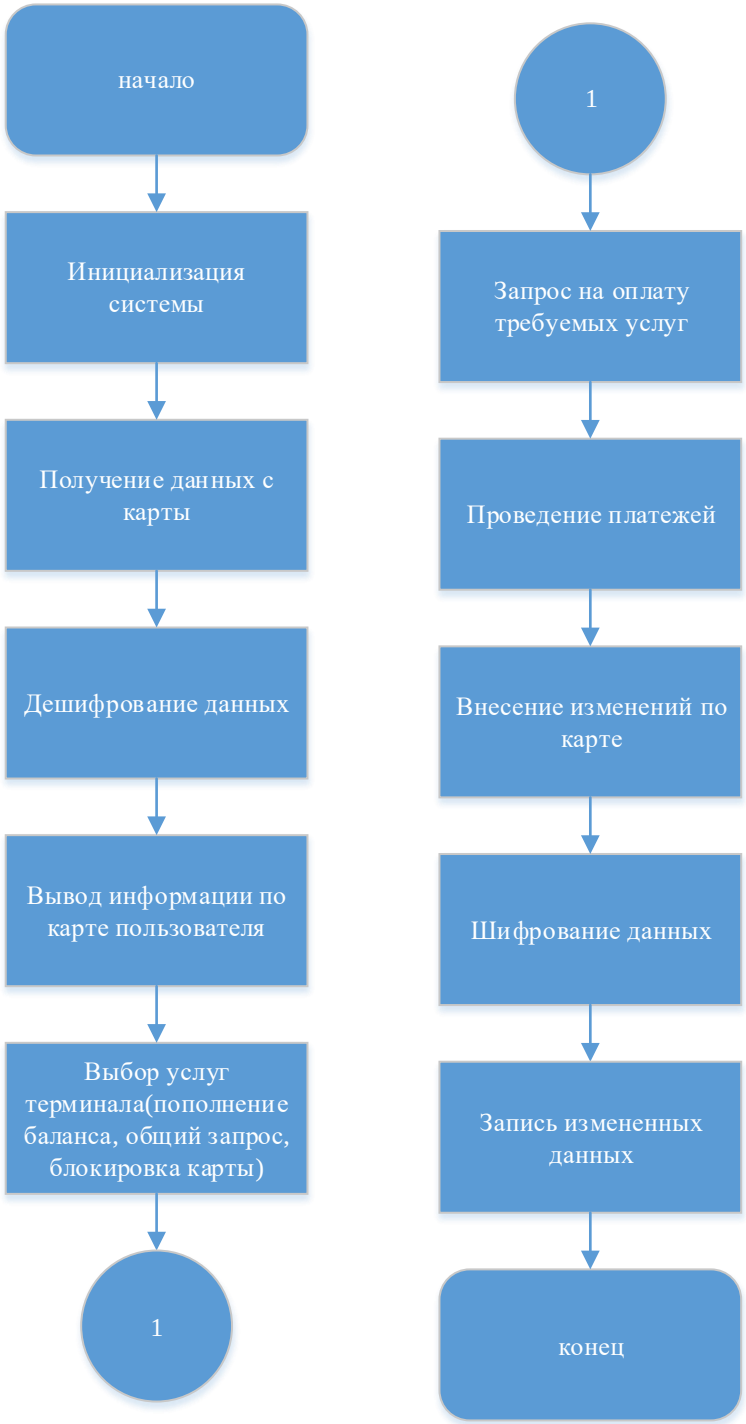


Рисунок 8. Структурная схема алгоритма работы терминала

Описание блоков структурной схемы алгоритма по работе с терминалом:

- Инициализация системы – на данном этапе происходит инициализация всех устройств системы, задание портов ввода/ вывода данных, устанавливается связь с сервером.
- Получение данных с карты – считывание данных с карт пользователей
- Дешифрование данных – информация на карте хранится в зашифрованном виде, для ее изменений требуется дешифровка.
- Вывод информации по карте пользователя– после дешифровки происходит проверка карт по балансу и по срокам эксплуатации и вывод соответствующей информации на дисплей терминала.
- Выбор услуг терминала – после выполнения проверки карты происходит выбор услуги клиентом (пополнение баланса, общий запрос, блокировка карты).
- Запрос на оплату требуемых услуг – для продолжения выполнения услуги, требуется выбрать способ оплаты.
- Проведение платежа – внесение через купюроприемник или банковской карты необходимых средств.
- Внесение изменений по карте – в соответствие с произведенными операциями происходит изменение данных.
- Шифрование данных – для обратной записи информации данных снова шифруются.
- Запись данных на карту – после всех операций с данными происходит их запись на карту.

3.4 Структурная схема алгоритма для контролирующего устройства

На рисунке 8 представлена структурная схема алгоритма работы контролирующего устройства.

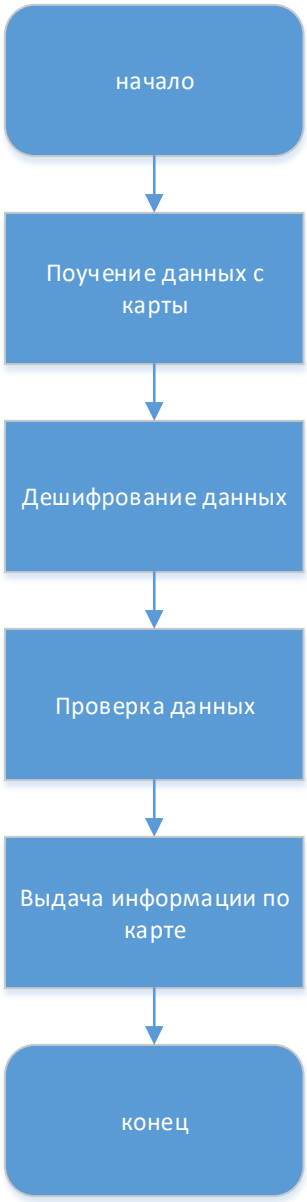


Рисунок 8. Структурная схема алгоритма работы контролирующего устройства

Описание блоков структурной схемы алгоритма по работе с сервером:

- Инициализация системы – на данном этапе происходит инициализация всех устройств системы, задание портов ввода/ вывода данных, устанавливается связь с сервером.
- Получение данных с карты – считывание данных с карт пользователей

- Дешифрование данных – информация на карте хранится в зашифрованном виде, для ее изменений требуется дешифровка.
- Проверка данных – после дешифровки происходит проверка карт по балансу и по срокам эксплуатации.
- Выдача информации по карте – на экран контрольного устройства выдается информация по карте клиента.

3.5 Структурная схема алгоритма для валидатора

На рисунке 9 представлена структурная схема алгоритма работы валидатора.

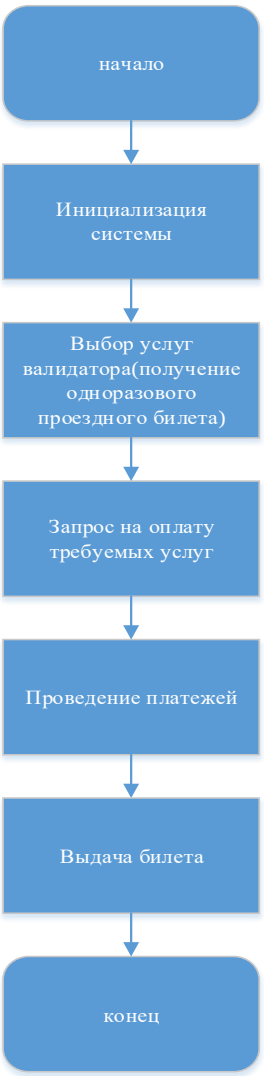


Рисунок 9. Структурная схема алгоритма работы валидатора

Описание блоков структурной схемы алгоритма по работе с валидатором:

- Инициализация системы – на данном этапе происходит инициализация всех устройств системы, задание портов ввода/ вывода данных, устанавливается связь с сервером.
- Выбор услуг валидатора – в данном случае единственной функцией является покупка одноразового билета.
- Проведение платежа – внесение через купюроприемник или банковской карты необходимых средств.
- Выдача билета – после проведения платежа устройством подается сигнал на печать чека.

4. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ

В этом разделе будут приведены примеры программ, под которыми работают компоненты системы.

4.1 GPRS связь с web-сервером

В данном разделе будет показан отладочный код работы GSM модуля, платы Arduino MEGA и web – сервера.

Будет отправляться следующая информация:

- Идентификаторы карт
- Время активации карт
- Координаты активации карты

Для клиента:

```
#include <SoftwareSerial.h>
      SoftwareSerial GSMport
(2, 3); // RX, TX
      int SerialPort = 48;
      int SerialState;
      int SerialLastState = HIGH;

      void setup() {
        delay(3000); //дадим время на инициализацию GSM модулю
        pinMode(SerialPort, INPUT);
        digitalWrite(SerialPort, HIGH);  //вкл. подтягивающий резистор 4,7ом
        Serial.begin(9600);  //скорость порта
        Serial.println("GPRS test");
        GSMport.begin(9600);
        gprs_init();
      }
      void loop() {
        SerialState = digitalRead(SerialPort);
        if (SerialState != SerialLastState) {  //есть ли новое значение с порта
             Serial.print("serial changed to: ");
             Serial.println(SerialState);
             SerialLastState = SerialState;
             gprs_send(String(SerialState));
             delay(100);
        }
        if (GSMport.available()) {  //если GSM модуль что-то послал нам, то
             Serial.println(ReadGSM());  //печатаем в монитор порта пришедшую строку
        }
        delay(100);
      }

      void gprs_init() {  //Процедура начальной инициализации GSM модуля
        int d = 500;
        int ATsCount = 7;
        String ATs[] = {  //массив AT команд
             "AT+SAPBR=3,1,\"CONTYPE\",\"GPRS\"",  //Установка настроек подключения
             "AT+SAPBR=3,1,\"APN\",\"internet.tele2.ru\"",
             "AT+SAPBR=3,1,\"USER\",\"tele2\"",
             "AT+SAPBR=3,1,\"PWD\",\"tele2\"",
             "AT+SAPBR=1,1",  //Устанавливаем GPRS соединение
             "AT+HTTPINIT",  //Инициализация http сервиса
```

```
            "AT+HTTPPARA=\"CID\",1"  //Установка CID параметра для http сессии
        };
        int ATsDelays[] = {6, 1, 1, 1, 3, 3, 1}; //массив задержек
        Serial.println("GPRG init start");
        for (int i = 0; i < ATsCount; i++) {
            Serial.println(ATs[i]);  //посылаем в монитор порта
            GSMport.println(ATs[i]);  //посылаем в GSM модуль
            delay(d * ATsDelays[i]);
            Serial.println(ReadGSM());  //показываем ответ от GSM модуля
            delay(d);
        }
        Serial.println("GPRG init complete");
      }

      void gprs_send(String data) {  //Процедура отправки данных на сервер
        //отправка данных на сайт
        int d = 400;
        Serial.println("Send start");
        Serial.println("setup url");
        GSMport.println("AT+HTTPPARA=\"URL\",\"http://crosstechno.ru/diplom/adm" +
data + "\"");
        delay(d * 2);
        Serial.println(ReadGSM());
        delay(d);
        Serial.println("GET url");
        GSMport.println("AT+HTTPACTION=0");
        delay(d * 2);
        Serial.println(ReadGSM());
        delay(d);
        Serial.println("Send done");
      }

      String ReadGSM() {  //функция чтения данных от GSM модуля
        int c;
        String v;
        while (GSMport.available()) {  //сохраняем входную строку в переменную v
            c = GSMport.read();
            v += char(c);
            delay(10);
        }
        return v;
      }
```

Для сервера (PHP):

```
<?php
  $ip = $_SERVER['REMOTE_ADDR']; //получаем IP адрес клиента
  $client = $_SERVER['HTTP_USER_AGENT']; //получаем идентификатор HTTP клиента
  $today = date("Y.m.d H:i:s"); //получаем текущие дату и время
  $f = fopen("log.csv","a"); //открываем файл для добавления данных
  $param = $_REQUEST['a']; //получаем значение посланной переменной "a"
  fwrite($f,"$today; $ip; $client; SerialState=$param\r\n----------------\r\n");
//запись данных в файл
  fclose($f); //закрываем файл
?>
<p>GPRS data read page</p>
```

4.2 DES шифрование

Для того, чтобы зашифровать сообщение алгоритмом DES, требуется выполнить следующие шаги:

- довести исходное сообщение до такого размера (в битах), чтобы оно нацело делилось на размер блока (sizeOfBlock = 128 бит);
- разделить исходное сообщение на блоки;
- довести длину ключа до длины половины блока;
- перевести ключ в бинарный формат (в нули и единицы);
- провести над каждым блоком прямое преобразование сетью Фейстеля в течении 16-ти раундов. После каждого раунда необходимо выполнять циклический сдвиг ключа на заданное количество символов;
- соединить все блоки вместе; таким образом получим сообщение, зашифрованное алгоритмом DES [16].

Расшифровка DES производится по аналогии. Используется обратное преобразование сетью Фейстеля [17].

Ниже будет представлен код программы, отвечающий за шифрование данных отправляемых как с основного устройства на сервер, так и при передачи данных основное устройство – пользовательская карта.

Объявление переменных:

```
private const int sizeOfBlock = 128; //в DES размер блока 64 бит, но поскольку в
unicode символ в два раза длинее, то увеличим блок тоже в два раза
private const int sizeOfChar = 16; //размер одного символа (in Unicode 16 bit)
private const int shiftKey = 2; //сдвиг ключа
private const int quantityOfRounds = 16; //количество раундов
string[] Blocks; //сами блоки в двоичном формате
```

Реализация методов необходимых для функционирования алгоритма des:

Метод, необходимый для увеличения размера строки. Этот процесс необходим для того чтобы в соответствии с алгоритмом, строка делилась на блоки. Размер строки увеличивается благодаря добавлению в конец символа “#”.

```
while (((input.Length * sizeOfChar) % sizeOfBlock) != 0)
   input += "#";
   return input;
```

Метод разбиения символьной строки на блоки.

```
Blocks = new string[(input.Length * sizeOfChar) / sizeOfBlock];
int lengthOfBlock = input.Length / Blocks.Length;
for (int i = 0; i < Blocks.Length; i++)
            {
                Blocks[i] = input.Substring(i * lengthOfBlock, lengthOfBlock);
                Blocks[i] = StringToBinaryFormat(Blocks[i]);
            }
        }
```

Перевод строки в двоичный формат.

```
    string output = "";

    for (int i = 0; i < input.Length; i++)
    {
        string char_binary = Convert.ToString(input[i], 2);

        while (char_binary.Length < sizeOfChar)
            char_binary = "0" + char_binary;

        output += char_binary;
    }

    return output;
```

Метод, изменяющий длину ключа до необходимой.

```
  if (input.Length > lengthKey)
        input = input.Substring(0, lengthKey);
    else
        while (input.Length < lengthKey)
            input = "0" + input;

    return input;
```

Ниже приведены по одному проходу шифровки, расшифровки алгоритма des.

```
{
    string L = input.Substring(0, input.Length / 2);
    string R = input.Substring(input.Length / 2, input.Length / 2);

    return (R + XOR(L, f(R, key)));
}
```

```
{
    string L = input.Substring(0, input.Length / 2);
    string R = input.Substring(input.Length / 2, input.Length / 2);

    return (XOR(f(L, key), R) + L);
}
```

В качестве шифрующей функции было решено использовать логическую операцию XOR.

```
{
    return XOR(s1, s2);
}
```

Ниже происходит вычисления ключа для следующего раунда DES Циклический сдвиг вправо.

```
{
    for (int i = 0; i < shiftKey; i++)
    {
        key = key[key.Length - 1] + key;
        key = key.Remove(key.Length - 1);
    }

    return key;
}
```

Ниже происходит вычисления ключа для следующего раунда DES Циклический сдвиг влево.

```
{
    for (int i = 0; i < shiftKey; i++)
    {
        key = key + key[0];
        key = key.Remove(0, 1);
    }

    return key;
}
```

Далее будут приведены сегменты кода в которых реализованы функции кнопок шифровки/расшифровки.

Шифровка:

```
{
    if (textBoxEncodeKeyWord.Text.Length > 0)
    {
        string s = "";

        string key = textBoxEncodeKeyWord.Text;

        StreamReader sr = new StreamReader("in.txt");

        while (!sr.EndOfStream)
        {
            s += sr.ReadLine();
        }

        sr.Close();
```

```
        s = StringToRightLength(s);

        CutStringIntoBlocks(s);

        key = CorrectKeyWord(key, s.Length / (2 * Blocks.Length));
        textBoxEncodeKeyWord.Text = key;
        key = StringToBinaryFormat(key);

        for (int j = 0; j < quantityOfRounds; j++)
        {
            for (int i = 0; i < Blocks.Length; i++)
                Blocks[i] = EncodeDES_One_Round(Blocks[i], key);

            key = KeyToNextRound(key);
        }

        key = KeyToPrevRound(key);

        textBoxDecodeKeyWord.Text = StringFromBinaryToNormalFormat(key);

        string result = "";

        for (int i = 0; i < Blocks.Length; i++)
                result += Blocks[i];

        StreamWriter sw = new StreamWriter("out1.txt");
        sw.WriteLine(StringFromBinaryToNormalFormat(result));
        sw.Close();

        Process.Start("out1.txt");
    }
    else
        MessageBox.Show("Введите ключевое слово!");
}
```

Расшифровка:

```
{
    if (textBoxDecodeKeyWord.Text.Length > 0)
    {
        string s = "";

        string key = StringToBinaryFormat(textBoxDecodeKeyWord.Text);

        StreamReader sr = new StreamReader("out1.txt");

        while (!sr.EndOfStream)
        {
            s += sr.ReadLine();
        }

        sr.Close();

        s = StringToBinaryFormat(s);

        CutBinaryStringIntoBlocks(s);

        for (int j = 0; j < quantityOfRounds; j++)
        {
            for (int i = 0; i < Blocks.Length; i++)
                Blocks[i] = DecodeDES_One_Round(Blocks[i], key);

            key = KeyToPrevRound(key);
        }

        key = KeyToNextRound(key);

        textBoxEncodeKeyWord.Text = StringFromBinaryToNormalFormat(key);
```

```
        string result = "";

        for (int i = 0; i < Blocks.Length; i++)
            result += Blocks[i];

        StreamWriter sw = new StreamWriter("out2.txt");
        sw.WriteLine(StringFromBinaryToNormalFormat(result));
        sw.Close();

        Process.Start("out2.txt");
    }
    else
        MessageBox.Show("Введите ключевое слово!");
}
```

Полный код представлен в приложении А.

Результаты работы программы приведены на рисунке 10, 11.

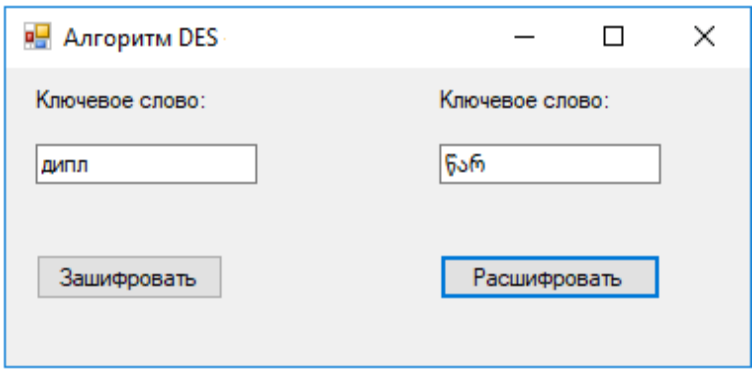
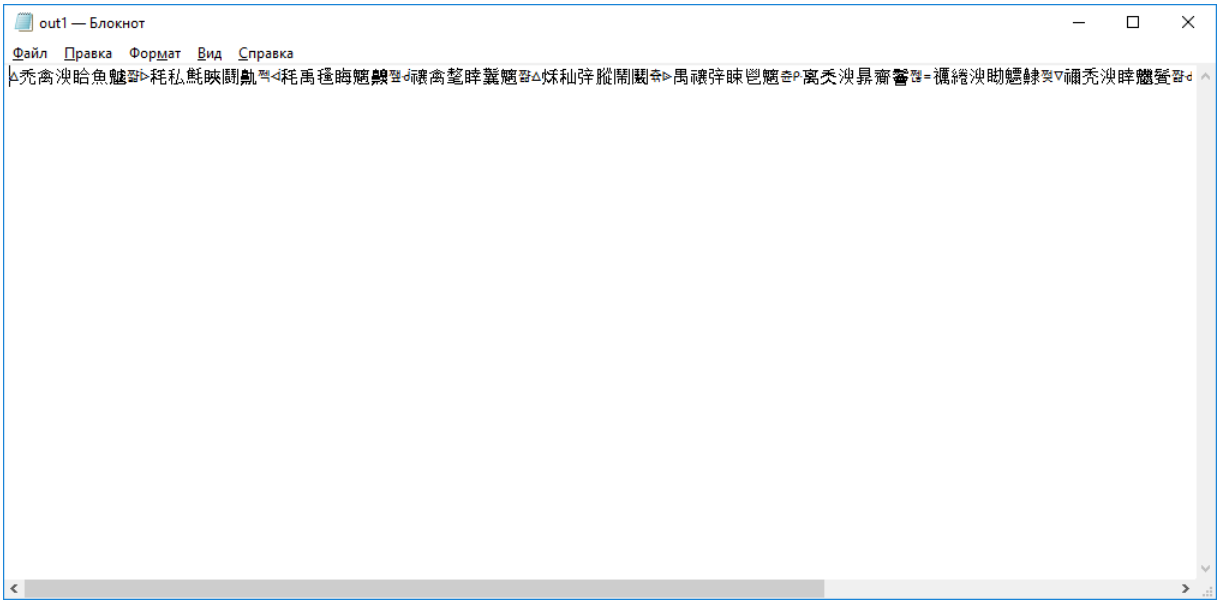


Рисунок 10. Вид рабочего окна программы.



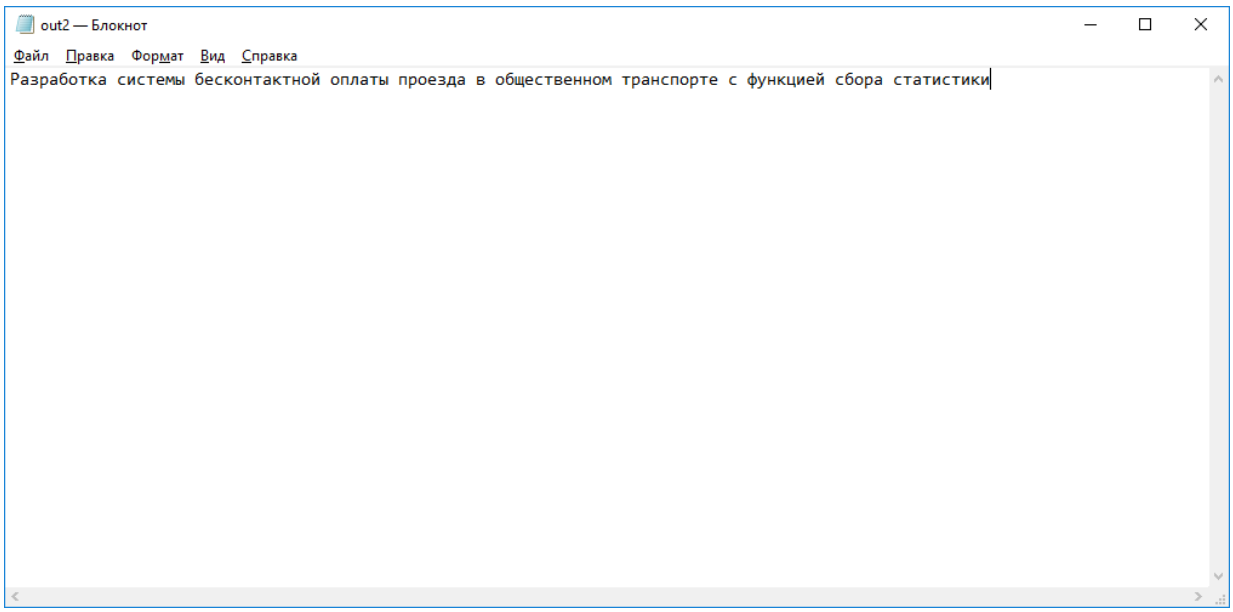


Рисунок 11. Результаты работы программы.

4.3 Web-сервер, база данных

4.3.1 База данных

Для полноценной работы системы по сбору статистики и мониторинга ошибок был реализован сервер, частью которого является база данных отвечающая за хранение информации.

Для написания базы данных использовался язык php. В качестве СУБД было использовано MySQL.

PHP – это широко используемый язык сценариев общего назначения с открытым исходным кодом. Говоря проще, PHP это язык программирования, специально разработанный для написания web-приложений (сценариев), исполняющихся на web-сервере [18].

MySQL – это одна из самых популярных и самых распространенных СУБД (система управления базами данных) в интернете. Она не предназначена для работы с большими объемами информации, но ее применение идеально для интернет сайтов, как небольших, так и достаточно крупных [19].

После создания базы данных, она была перенесена на хостинг phpmyadmin.masterhost.ru

Структура базы данных

На данном этапе база данных состоит из пяти таблиц:

- s_cars
- s_passengers
- s_routes
- s_stops
- s_Traffic

s_cars – таблица в которой хранится информация о транспорте, находящемся в автопарке (рисунок 12).

Параметры

	id	b_number	b_type	b_rem	b_status	b_curr_route	b_curr_lat	b_curr_long
	1	Т356ОК 70	bus	MAN, АТП-2	A	19	0	0
	2	У789ЕН 70	fixed-route	Газель	N	6	58	36

Рисунок 12. Таблица транспорта.

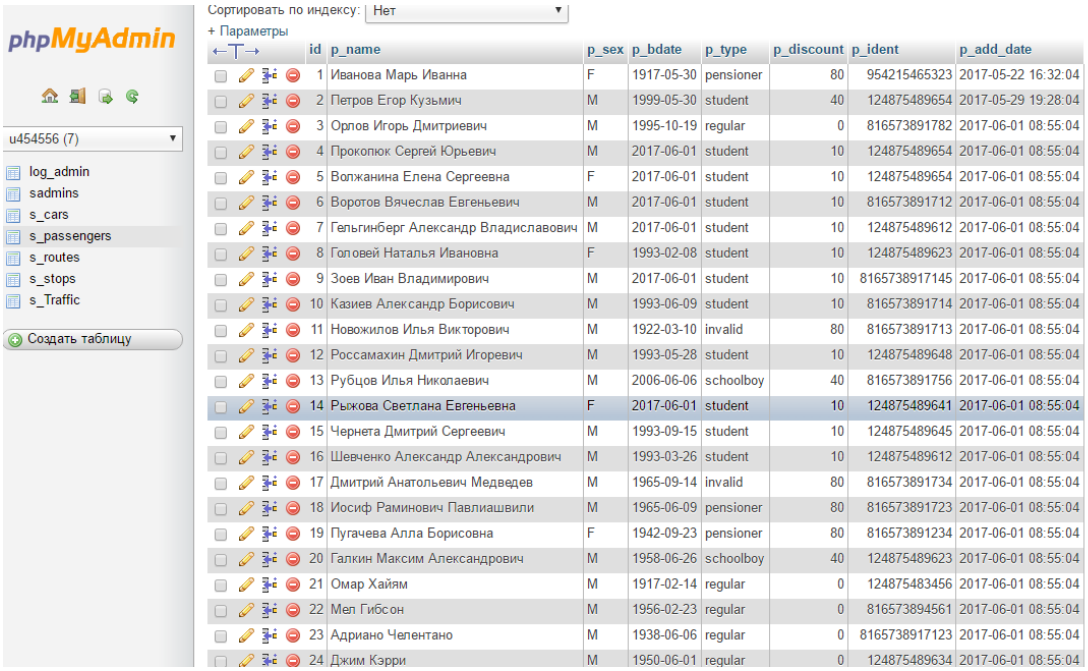
Таблица хранит в себе информацию:

- Id – порядковый номер
- b_number – гос. номер транспортного средства
- b_type – тип транспортного средства
- b_rem – примечание (марка транспортного средства и т.д.)
- b_status – статус активен/не активен
- b_curr_route – номер действующего маршрута
- b_curr_lat – координаты по широте
- b_curr_long – координаты по долготе

Координаты по широте и долготе берутся при активации карт клиентов и после этого сравниваются с координатами остановок рядом. Сопоставив

активацию карт и координаты остановок можно вывести определенную статистику по количеству людей, зашедших на остановке.

s_passengers – таблица в которой хранится информация о клиентах системы (рисунок 13).



id	p_name	p_sex	p_bdate	p_type	p_discount	p_ident	p_add_date
1	Иванова Марь Иванна	F	1917-05-30	pensioner	80	954215465323	2017-05-22 16:32:04
2	Петров Егор Кузьмич	M	1999-05-30	student	40	124875489654	2017-05-29 19:28:04
3	Орлов Игорь Дмитриевич	M	1995-10-19	regular	0	816573891782	2017-06-01 08:55:04
4	Прокопюк Сергей Юрьевич	M	2017-06-01	student	10	124875489654	2017-06-01 08:55:04
5	Волжанина Елена Сергеевна	F	2017-06-01	student	10	124875489654	2017-06-01 08:55:04
6	Воротов Вячеслав Евгеньевич	M	2017-06-01	student	10	816573891712	2017-06-01 08:55:04
7	Гельгинберг Александр Владиславович	M	2017-06-01	student	10	124875489612	2017-06-01 08:55:04
8	Головей Наталья Ивановна	F	1993-02-08	student	10	124875489623	2017-06-01 08:55:04
9	Зоев Иван Владимирович	M	2017-06-01	student	10	8165738917145	2017-06-01 08:55:04
10	Казиев Александр Борисович	M	1993-06-09	student	10	816573891714	2017-06-01 08:55:04
11	Новожилов Илья Викторович	M	1922-03-10	invalid	80	816573891713	2017-06-01 08:55:04
12	Россамахин Дмитрий Игоревич	M	1993-05-28	student	10	124875489648	2017-06-01 08:55:04
13	Рубцов Илья Николаевич	M	2006-06-06	schoolboy	40	816573891756	2017-06-01 08:55:04
14	Рыжова Светлана Евгеньевна	F	2017-06-01	student	10	124875489641	2017-06-01 08:55:04
15	Чернета Дмитрий Сергеевич	M	1993-09-15	student	10	124875489645	2017-06-01 08:55:04
16	Шевченко Александр Александрович	M	1993-03-26	student	10	124875489612	2017-06-01 08:55:04
17	Дмитрий Анатольевич Медведев	M	1965-09-14	invalid	80	816573891734	2017-06-01 08:55:04
18	Иосиф Раминович Павлиашвили	M	1965-06-09	pensioner	80	816573891723	2017-06-01 08:55:04
19	Пугачева Алла Борисовна	F	1942-09-23	pensioner	80	816573891234	2017-06-01 08:55:04
20	Галкин Максим Александрович	M	1958-06-26	schoolboy	40	124875489623	2017-06-01 08:55:04
21	Омар Хайям	M	1917-02-14	regular	0	124875483456	2017-06-01 08:55:04
22	Мел Гибсон	M	1956-02-23	regular	0	816573894561	2017-06-01 08:55:04
23	Адриано Челентано	M	1938-06-06	regular	0	8165738917123	2017-06-01 08:55:04
24	Джим Кэрри	M	1950-06-01	regular	0	124875489634	2017-06-01 08:55:04

Рисунок 13. Таблица клиентов системы.

Таблица хранит в себе информацию:

- Id – порядковый номер
- p_sex – пол клиента
- p_bdate – дата рождения
- p_type – тип проездной карты (без привилегий, школьник, студент, пенсионер, льготник, инвалид)
- p_discount – процент скидки на проезд
- p_ident – идентификационный номер клиента в системе
- p_add_date – дата регистрации в системе

s_routes – таблица в которой хранится информация о маршрутах (рисунок 14).

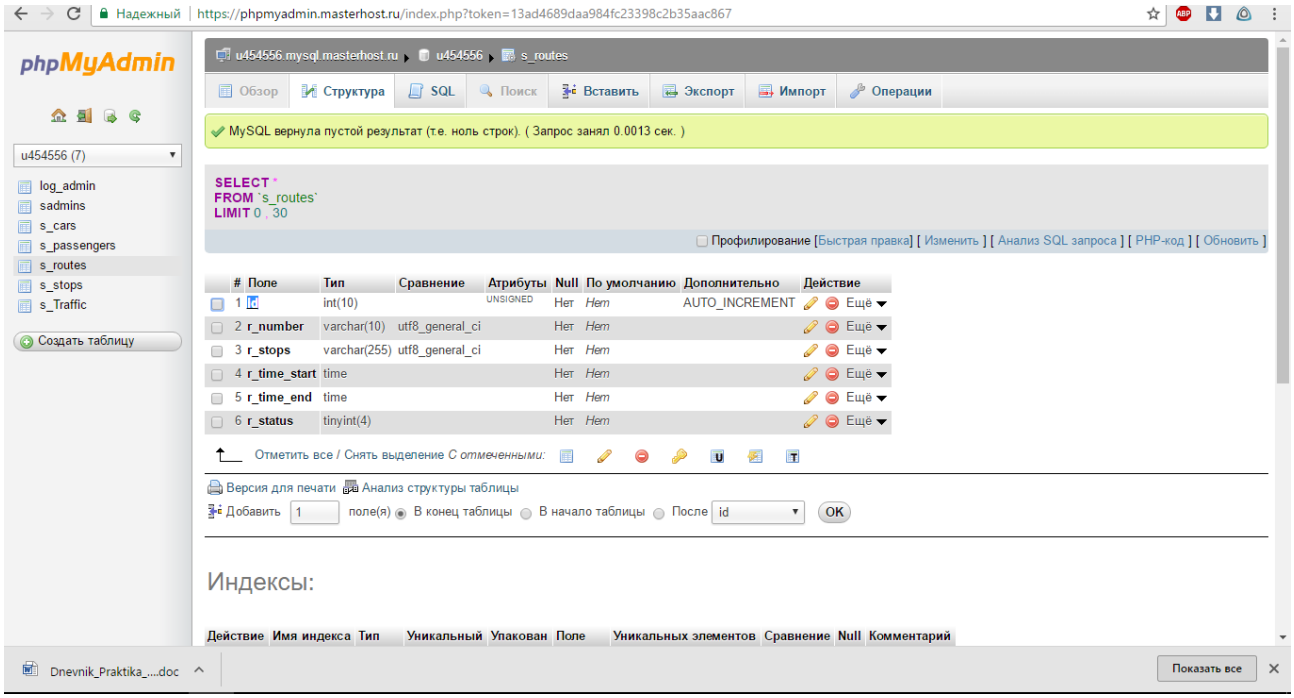


Рисунок 14. Таблица маршрутов

Таблица хранит в себе информацию:

- Id – порядковый номер
- p_sex – пол клиента
- p_bdate – дата рождения
- p_type – тип проездной карты (без привилегий, школьник, студент, пенсионер, льготник, инвалид)
- p_discount – процент скидки на проезд
- p_ident – идентификационный номер клиента в системе
- p_add_date – дата регистрации в системе

s_stops – таблица в которой хранится информация о остановках (рисунок 15).

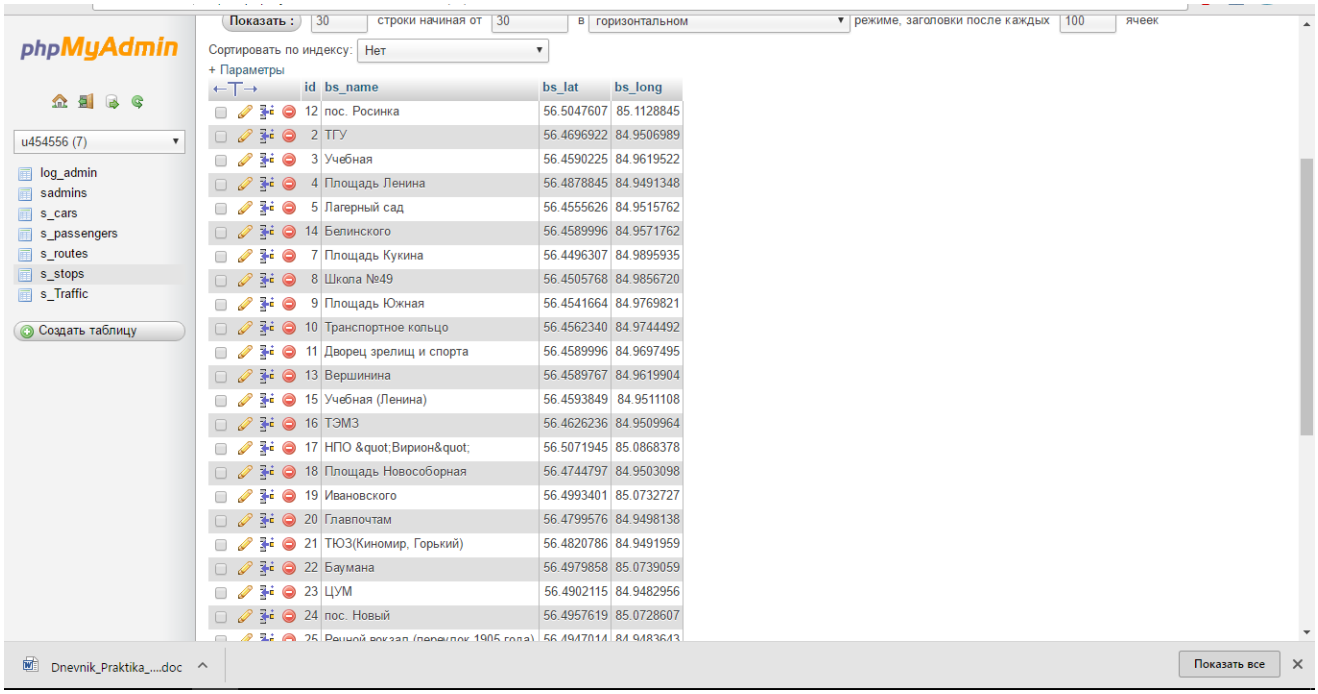


Рисунок 15. Таблица остановок

Таблица хранит в себе информацию:

- Id – порядковый номер
- bs_name – название остановки
- bs_lat – широта
- bs_long – долгота

bs_lat и bs_long – координаты необходимые для сопоставления остановки и активаций карт клиентов.

s_Traffic – таблица агрегирования статистики (рисунок 16).

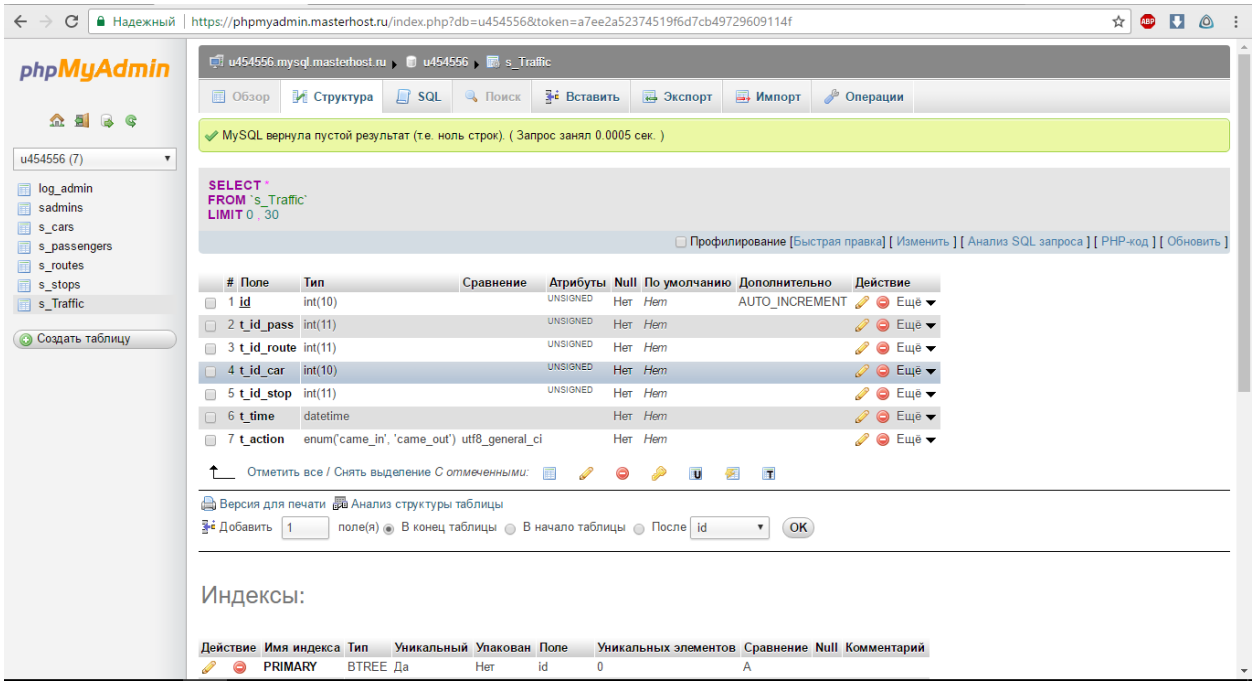


Рисунок 16. Таблица статистики

Таблица хранит в себе информацию:

- t_id_pass – идентификатор
- t_id_route– номер маршрута
- t_id_car – гос. номер транспортного средства
- t_id_stop – название остановки
- t_time– время входа
- t_action– поле со значением вошел/вышел

4.3.2 Web-сервер

Одним из самых важных элементов системы является web-сервер, через который происходит управление системой.

Логика работы и функционирование осуществлены на языке php, а математический аппарат реализован на языке java script.

Под управлением системой понимается:

- Сбор статистики о пассажиропотоке

- Добавление/удаление пользовательских карт
- Изменение данных пользовательских карт
- Добавление маршрутов
- Добавление транспорта и изменение информации о состоянии транспорта
- Вывод статистики в виде диаграмм, гистограмм

Ниже на рисунке 17 представлено главное меня web-сервера, а также вкладка, на которое приведен список пассажиров, добавленных в систему.

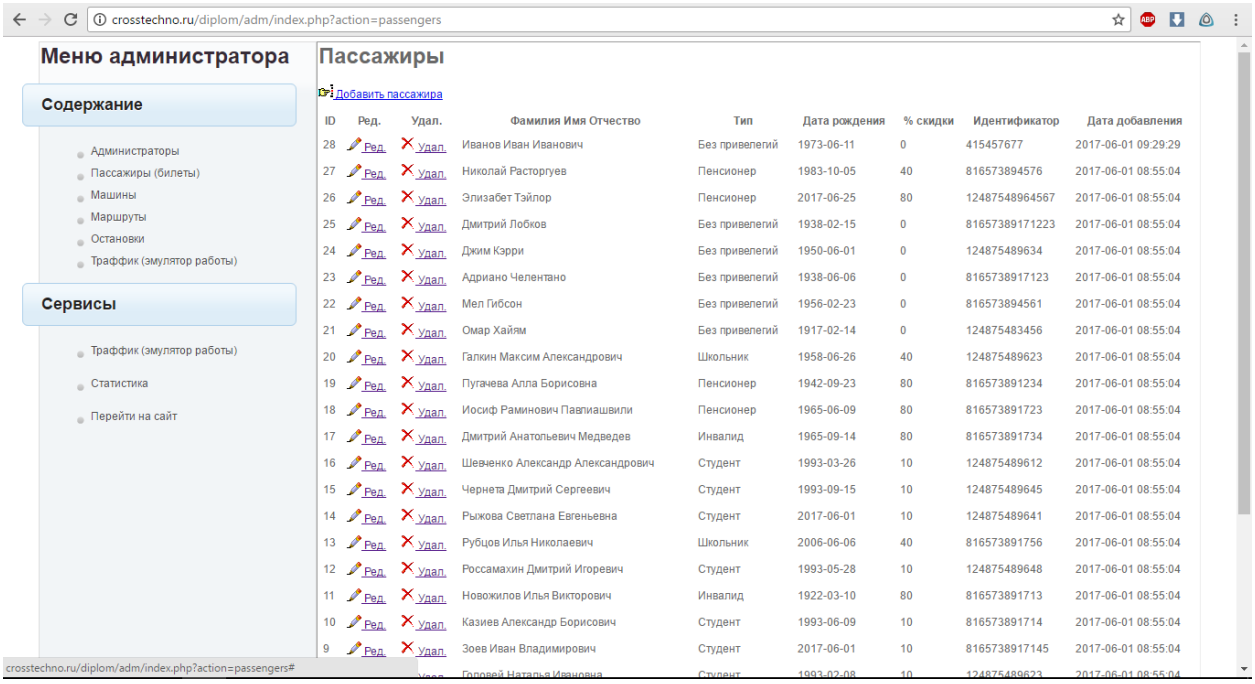


Рисунок 17. Вкладка пассажиров

Далее, на рисунке 18 представлено меню с добавлением карты нового клиента в систему.

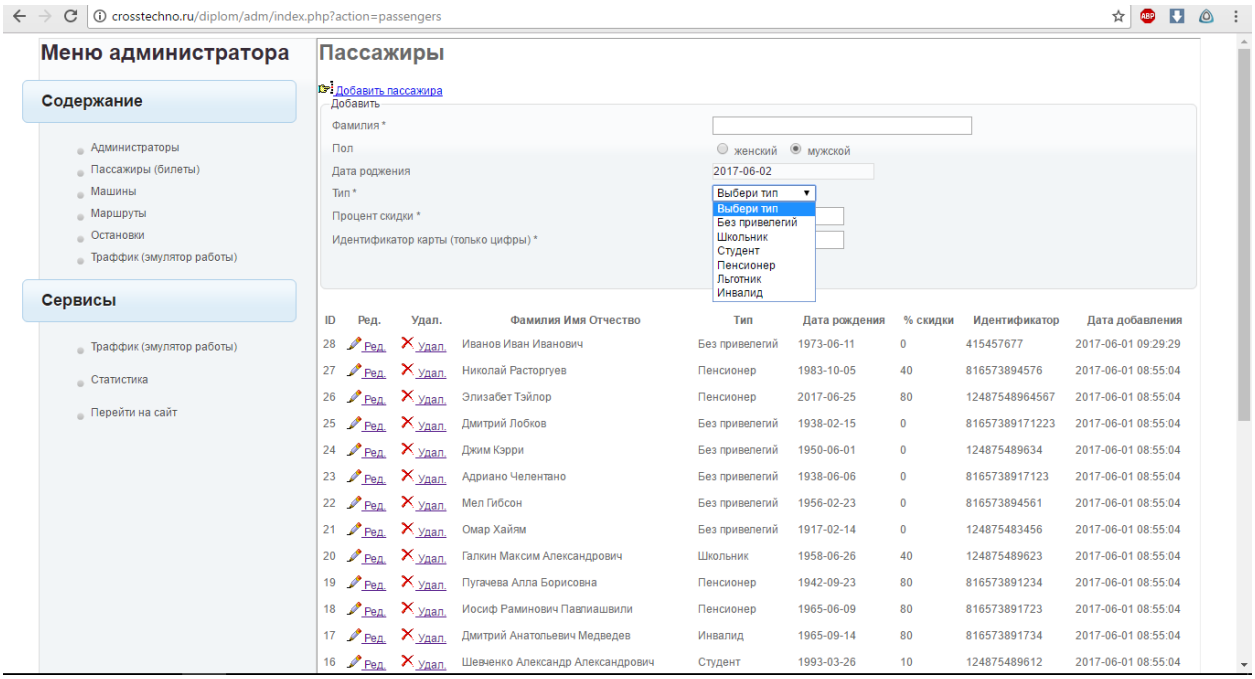


Рисунок 18. Меню добавления карт клиентов

При добавлении новой карты необходимо заполнить поля:

- Фамилия
- Пол
- Дата рождения
- Тип (без привилегий, школьник, студент, пенсионер, льготник, инвалид)
- Процент скидки
- Идентификатор карты

На рисунке 19 представлено меню транспортных средств. Здесь можно добавлять, удалять, корректировать информацию по каждому отдельному объекту.

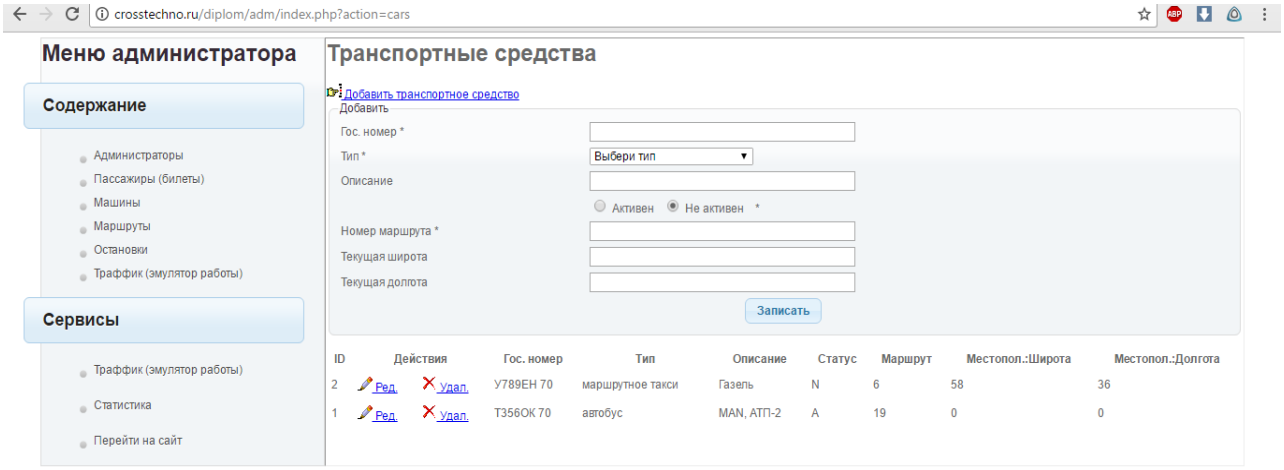


Рисунок 19. Меню транспортных средств

При добавлении новой транспорта необходимо заполнить поля:

- Гос. номер
- Тип (автобус, железные дороги, маршрутное такси, метрополитен, монорельсовый транспорт, речной трамвай, трамвай, троллейбус)
- Состояние
- Номер маршрута
- Текущая широта
- Текущая долгота

На рисунке 20 представлено добавление маршрутов в систему. При добавление нового маршрута требуется ввести соответствующий номер маршрута и внести порядковые номера остановок (каждой остановке присваивается порядковый номер).

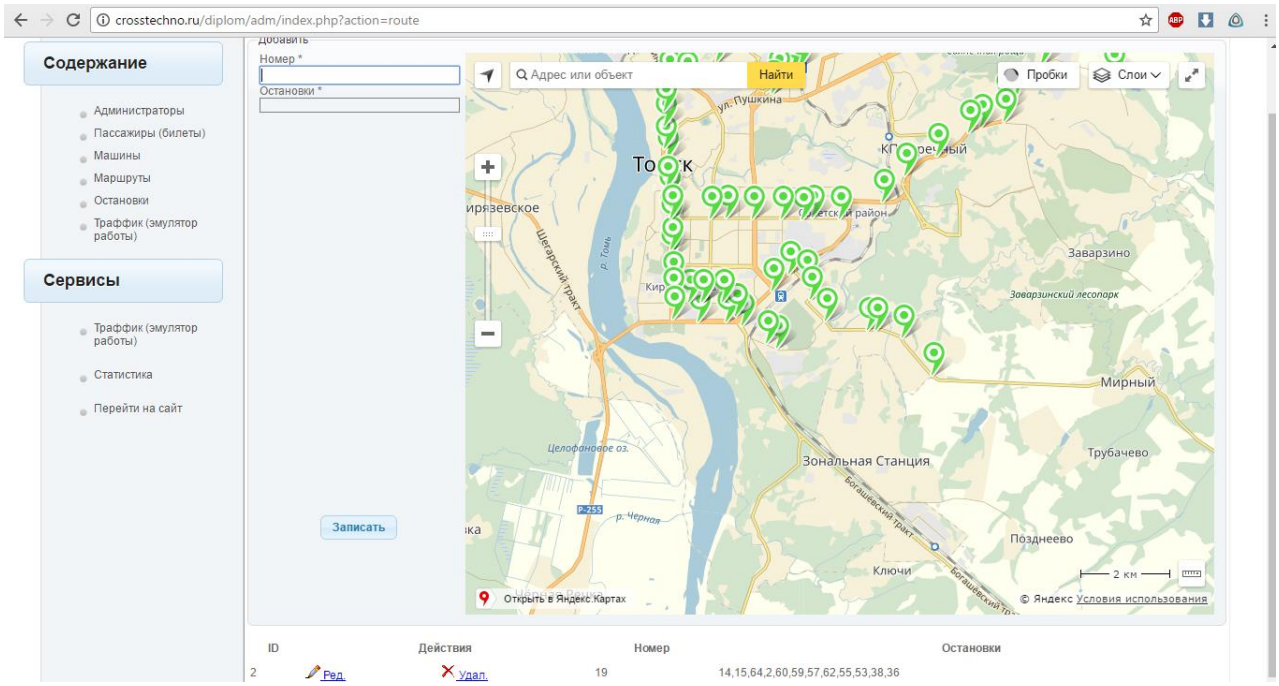


Рисунок 20. Меню добавления и отображения текущих маршрутов

Далее на рисунке 21 представлено меня добавления остановок. В данном меню вводится номер маршрута и номера всех остановок, соответствующих этому маршруту. Координаты можно вводить как в виде готовых в заданные поля, так и по средствам API Яндекс. Карт.

API Яндекс.Карт — это набор сервисов, которые позволяют использовать картографические данные и технологии Яндекса.

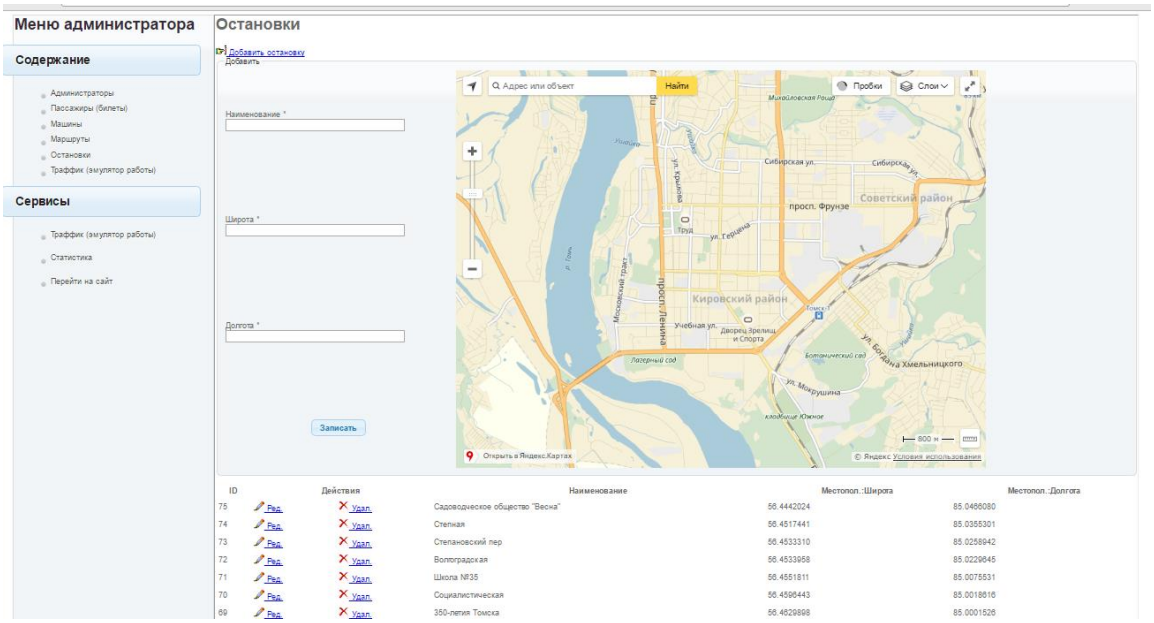


Рисунок 21. Меню добавления остановок

Ниже на рисунке 22 представлено меню со списком взаимодействий пользовательских карт с системой.

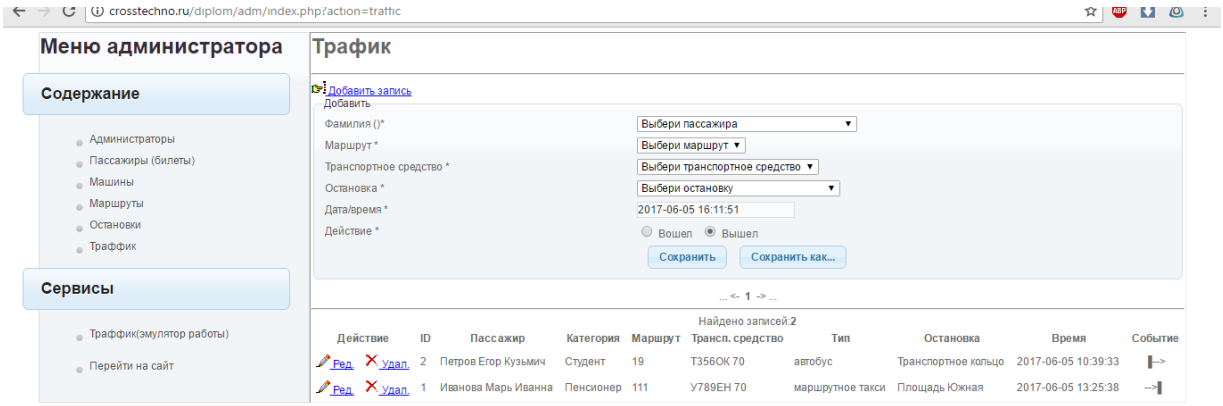


Рисунок 22. Меню взаимодействия карт с системой

При взаимодействии клиента с картой в таблице выводится его полная информация, а также время события.

5 ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ, И РЕСУРСОСБЕРЕЖЕНИЕ

Целью данного раздела является комплексный анализ и описание финансово-экономических аспектов выполненной работы. Необходимо оценить полные денежные затраты на проект, а также дать приближенную экономическую оценку результатов ее внедрения. Это, в свою очередь, позволит оценить экономическую целесообразность осуществления работы с помощью традиционных показателей инвестиций.

5.1 «Портрет» потребителя результатов НТИ

Разработка научно-технического решения ориентирована на пользователей общественного транспорта, т.е. на все слои населения, различных возрастов, различного пола и социально-семейного статуса. Потребитель может заниматься различной деятельностью, иметь различные интересы.

5.2 Организация и планирование работ

В данном пункте определяется перечень проводимых работ, их исполнители и оптимальная продолжительность выполнения. Для дальнейшего определения продолжительности этапов работ и их трудоемкости по каждому исполнителю, а также построения линейного графика реализации проекта этапы работы хронологически упорядочены и сведены в таблицу 3, где НР – научный руководитель, И – инженер (исполнитель проекта).

Таблица 3. Перечень работ и продолжительность их выполнения

Этапы работы	**Исполнители**	**Загрузка исполнителей**
Постановка целей и задач, получение исходных данных	НР, И	НР – 100 % И – 10 %
Составление и утверждение технического задания	НР, И	НР – 60 % И – 40 %

Подбор и изучение материалов по тематике	НР, И	НР – 10 % И – 100 %
Разработка календарного плана	НР, И	НР – 50 % И – 50 %
Изучение математических методов, вспомогательного программного обеспечения, специализированной литературы	НР, И	НР – 5 % И – 100 %
Построение модели системы	И	И – 100 %
Прототипирование основных узлов	И	И – 100 %
Отладка системы	И	И – 100 %
Корректировка данных, значений и параметров	И	И – 100 %
Анализ и обсуждение полученных результатов	НР, И	НР – 80 % И – 100 %
Оформление пояснительной записки	И	И – 100%

5.2.1 Продолжительность этапов работ

Расчет продолжительности выполнения этапов работ осуществлен опытно-статистическим методом с применением экспертного способа.

Ожидаемые значения продолжительности выполнения работ $t_{ож}$ определяются по формуле:

$$t_{ож} = \frac{3 \cdot t_{min} + 2 \cdot t_{max}}{5},$$

где t_{min} – минимальная продолжительность выполнения этапа, дн.;

t_{max} – максимальная продолжительность выполнения этапа, дн.

Расчет длительности выполнения каждого этапа работы в рабочих днях выполняется по формуле:

$$T_{\text{РД}} = \frac{t_{\text{ож}}}{K_{\text{ВН}}} \cdot K_{\text{д}},$$

где $t_{\text{ож}}$ – ожидаемая продолжительность этапа, дн.;

$K_{ВН}$ – коэффициент выполнения этапа, учитывающий влияние внешних факторов на соблюдение предварительно определенных длительностей. $K_{ВН} = 1$;

$K_{Д}$ – коэффициент, учитывающий дополнительное время на компенсацию непредвиденных задержек и согласование работ. $K_{Д} = 1{,}2$.

Для перевода значений длительности этапа в рабочих днях к их аналогам в календарных днях используется формула:

$$T_{\text{кд}} = T_{\text{РД}} \cdot T_{\text{к}},$$

где $T_{РД}$ – продолжительность выполнения этапа в рабочих днях;

$T_{К}$ – коэффициент календарности.

Значение $T_{К}$ определяется следующим образом:

$$T_{\text{К}} = \frac{T_{\text{КАЛ}}}{T_{\text{КАЛ}} - T_{\text{ВД}}},$$

где $T_{КАЛ}$ – календарные дни;

$T_{ВД}$ – выходные и праздничные дни;

$$T_{\text{К}} = \frac{365}{365 - 118} = 1{,}48.$$

Для пятидневной рабочей недели $T_{ВД} = 118$, следовательно, $T_{К} = 1, 48$.

Результаты выполненных расчетов по определению продолжительности этапов работ и их трудоемкости по исполнителям приведены в таблице 4.

Таблица 4. Трудозатраты на выполнение проекта

Этап	Исполнители	Продолжительность работ, дни			Трудоемкость работ по исполнителям чел.- дн.			
					$T_{РД}$		$T_{КД}$	
		t_{min}	t_{max}	$t_{ож}$	НР	$И_1$+$И_2$	НР	$И_1$+$И_2$
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1. Постановка целей и задач, получение исходных данных	НР, И	2	4	2,8	3,36	0,68	4,97	0,82
2. Составление и утверждение технического задания	НР, И	4	6	4,8	3,46	4,6	5,11	5,62
3. Подбор и изучение материалов по тематике	НР, И	8	10	8,8	1,06	21,2	1,29	25,76
4. Разработка календарного плана	НР, И	2	4	2,8	1,68	3,36	2,49	4,1

5. Изучение программного обеспечения, литературы	НР, И	7	10	8,2	0,49	19,68	0,73	24
6. Построение модели системы	И	5	7	5,8	–	13,92	–	16,98
7. Прототипирование основных узлов	И	7	9	7,8	–	18,72	–	22,84
8. Отладка системы	И	10	13	11,2	–	26,88	–	32,8
9. Корректировка данных, значений и параметров	И	12	15	13,2	–	31,68	–	38,64
10. Анализ и обсуждение полученных результатов	НР, И	2	5	3,2	3,07	7,68	4,54	9,36
11. Оформление пояснительной записки	И	14	20	16,4	–	39,36	–	48,02
Итого:				**85**	**13,12**	**187,76**	**19,13**	**228,94**

Таблица 5. Линейный график работ

Этап	НР	$И_1+И_2$	Февраль			Март			Апрель			Май		
			10	20	30	40	50	60	70	80	90	100	110	120
1	4,97	0,82												
2	5,11	5,62												
3	1,29	25,76												
4	2,49	4,1												
5	0,73	24												
6	–	16,98												
7	–	22,84												
8	–	32,8												
9	–	38,64												
10	4,54	9,36												
11	–	48,02												

НР – ; $И_1+И_2$ –

5.2.2 Расчет накопления готовности проекта

В данном пункте выполняется оценка текущих результатов работы над проектом. Величина накопления готовности работы показывает на сколько процентов, по окончанию текущего этапа, выполнен общий объем по проекту.

Введем обозначения:

$\text{ТР}_{\text{общ}}$ – общая трудоемкость проекта;

ТР_i (ТР_k) − трудоемкость i-го (k-го) этапа проекта, $i = \overline{1, I}$;

TP_i^H − накопленная трудоемкость i-го этапа проекта по его завершении;

TP_{ij} (TP_{kj}) − трудоемкость работ, выполняемых j-м участником на i-м этапе, здесь $j = \overline{1, m}$ − индекс исполнителя, в нашем примере m = 2.

Степень готовности определяется формулой:

$$\text{СГ}_i = \frac{\text{ТР}_i^{\text{Н}}}{\text{ТР}_{\text{общ.}}} = \frac{\sum_{k=1}^{i} \text{ТР}_k}{\text{ТР}_{\text{общ.}}} = \frac{\sum_{k=1}^{i} \sum_{j=1}^{m} \text{ТР}_{km}}{\sum_{k=1}^{I} \sum_{j=1}^{m} \text{ТР}_{km}}.$$

Результаты вычислений отражены в таблице 6.

Таблица 6 – Нарастание технической готовности работы и удельный вес каждого этапа

Этапы работы	***ТР$_i$, %***	***СГ$_i$, %***
Постановка целей и задач, получение исходных данных	3,46	3,46
Составление и утверждение технического задания	5,39	8,84
Подбор и изучение материалов по тематике	10,86	19,71
Разработка календарного плана	3,14	22,85

Изучение программного обеспечения, литературы	9,66	32,51
Прототипирование основных узлов	6,51	39,01
Отладка системы	8,75	47,77
Корректировка данных, значений и параметров	12,57	60,33
Анализ и обсуждение полученных результатов	14,81	75,14
Анализ и обсуждение полученных результатов	6,46	81,60
Оформление пояснительной записки	18,40	100,00

5.3 Расчет сметы затрат на выполнение проекта

К затратам на создание проекта относится величина всех расходов, которые необходимы для реализации комплекса работ, составляющих содержание разработки.

5.3.1 Расчет затрат на материалы

К данной статье расходов относится стоимость материалов, покупных изделий и других материальных ценностей, расходуемых в процессе выполнения работ. Цена материальных ресурсов определяется по соответствующим им ценникам. Сюда же включаются расходы на совершение сделки купли-продажи.

Кроме того, данная статья включает в себя транспортно-заготовительные расходы, которые связанны с транспортировкой от поставщика к потребителю, хранением и прочими процессами, обеспечивающими движение материальных

ресурсов от поставщиков к потребителю. ТРЗ составляют 5 % от отпускной цены материалов.

Таблица 7. Расчет затрат на материалы

Наименование материалов	**Цена за ед., руб.**	**Кол-во**	**Сумма, руб.**
Бумага для принтера формата А4	299	1 уп.	299
Картридж для принтера	1399	1 шт.	1399
Канцелярские принадлежности	120	1 комп.	120
Радиодетали	10	80 шт.	800
ЖК дисплей	1200	1 шт.	1200
Провод медный КГВВ/КГВВП	20	10 м.	200
Провод медный ПВ-1/ПУВ 16	60	100 м.	6000
Корпус пластиковый GB016	480	2 шт.	960
Набор для травления плат	460	1 комп.	460
Комплект монтажных принадлежностей	1120	1 комп.	1120
Итого			12558
ТЗР 5 %			627,9
Итого с ТЗР			13185,9

5.3.2 Расчет заработной платы

К данной статье расходов относится заработная плата научного руководителя и исполнителя проекта, а также премии, которые входят в фонд заработной платы. Расчет основной заработной платы выполняется на основе трудоемкости выполнения каждого этапа работы и величины месячного оклада.

Среднедневная тарифная заработная плата ($ЗП_{дн-т}$) рассчитывается по формуле:

$ЗП_{дн-т} = МО/20,58$.

Расчеты затрат на основную заработную плату приведены в таблице 7.6. При расчете учитывалось, что в году 247 рабочих дней и, следовательно, в месяце 20,58 рабочих дня. Затраты времени на выполнение работы по каждому исполнителю брались из таблицы 7.2. Для учета в ее составе премий, дополнительной зарплаты и районной надбавки используется следующий ряд коэффициентов: $К_{ПР}$ = 1,1; $К_{доп.ЗП}$ = 1,188; $К_р$ = 1,3. Таким образом, для перехода от базовой суммы заработка исполнителя, к соответствующему полному заработку необходимо первую умножить на интегральный коэффициент $К_и$ = 1,699. Вышеуказанное значение $К_{доп.ЗП}$ при пятидневной равно 1,113, соответственно в этом случае $К_и$ = 1,62.

Таблица 8. Затраты на заработную плату

Исполнитель	**Оклад, руб./мес.**	**Среднедневная ставка, руб./раб.день**	**Затраты времени, раб. дни**	**Коэффициент**	**Фонд з/платы, руб.**
НР	**23264,86**	933,58	14	1,699	22206,13
$И_1$+$И_2$	**7864,11**	315,57	94	1,62	48055,00
Итого					**70261,13**

5.3.3 Расчет затрат на социальный налог

К данной статье затрат относят единый социальный налог (ЕСН), который включают в себя отчисления в пенсионный фонд, на социальное и медицинское страхование. Отчисления по ЕСН определяются по следующей формуле:

$$С_{соц} = К_{соц} \cdot С_{осн},$$

где $К_{соц}$ – коэффициент отчислений. Значение данного коэффициента составляет 30 % от полной заработной платы по проекту.

$$С_{соц} = 0,3 \cdot 70261,13 = 21278,34.$$

5.3.4 Расчет затрат на электроэнергию

Данный вид расходов включает в себя затраты на электроэнергию, потраченную в ходе выполнения проекта на работу используемого оборудования. Затраты на электроэнергию рассчитываются по формуле:

$$C_{эл.об.} = P_{об} \cdot t_{об} \cdot Ц_Э ,$$

где $P_{ОБ}$ – мощность, потребляемая оборудованием, кВт;

$Ц_Э$ – тариф на 1 кВт·час;

$t_{об}$ – время работы оборудования, час.

Для ТПУ ЦЭ = 5,782 руб./кВт·час (с НДС).

Время работы оборудования вычисляется на основе итоговых данных таблицы 7.2 для инженера (TРД) из расчета, что продолжительность рабочего дня равна 8 часов.

$$t_{об} = T_{РД} * K_t,$$

где $К_t \leq 1$– коэффициент использования оборудования по времени, равный отношению времени его работы в процессе выполнения проекта к $T_{РД}$. В данном случае значение коэффициента принимается равным 0,9.

Мощность, потребляемая оборудованием, определяется по формуле:

$$P_{ОБ} = P_{ном.} \cdot К_С$$

где $P_{ном.}$ – номинальная мощность оборудования, кВт;

$K_С \leq 1$ – коэффициент загрузки, зависящий от средней степени использования номинальной мощности. Для технологического оборудования малой мощности данный коэффициент принимается равным 1.

Расчеты затрат на электроэнергию для технологических целей приведены в таблице 8.

Таблица 8. Затраты на электроэнергию технологическую

Наименование оборудования	**Время работы оборудования $t_{ОБ}$, час**	**Потребляемая мощность $P_{ОБ}$, кВт**	**Затраты $Э_{ОБ}$, руб.**
Персональный компьютер	750,72 · 0,9	0,15	585,98
Струйный принтер	28	0,1	16,02
Итого:			**602,1**

5.3.5 Расчет амортизационных расходов

В данной статье расходов рассчитывается амортизация используемого оборудования за время выполнения проекта. Для этого используется формула:

$$C_{АМ} = \frac{H_A \cdot Ц_{ОБ} \cdot t_{рф} \cdot n}{F_Д},$$

где H_A – годовая норма амортизации единицы оборудования;

$Ц_{ОБ}$ – балансовая стоимость единицы оборудования с учетом ТЗР;

$F_Д$ – действительный годовой фонд времени работы соответствующего оборудования;

$t_{рф}$ – фактическое время работы оборудования в ходе выполнения проекта, учитывается исполнителем проекта;

n – число задействованных однотипных единиц оборудования.

Так, H_A для персонального компьютера принимается равным 0,4, для струйного принтера H_A = 0,5.

Балансовая стоимость принимается равной действующей цене единицы оборудования, находящейся в прейскурантах. Для персонального компьютера $Ц_{ОБ}$ = 35000 рублей, для струйного принтера $Ц_{ОБ}$ = 7800 рублей.

Действительный годовой фонд времени работы оборудования берется из фактического режима его использования в текущем календарном году. Так, для персонального компьютера при 247 рабочих днях (пятидневная рабочая неделя) можно принять $F_Д$ = 247 * 8 = 1973 часа. Для струйного принтера $F_Д$ = 500 часов.

$$C_{АМ\ ПК} = \frac{0{,}4 \cdot 35000 \cdot 750{,}72}{2392} = 5326{,}95\ ;$$

$$C_{АМ\ Пр} = \frac{0{,}5 \cdot 7800 \cdot 28}{500} = 218{,}4\ .$$

Итого начислено амортизации 5545,35 рублей.

5.3.6 Расчет расходов, учитываемых непосредственно на основе платежных (расчетных) документов (кроме суточных)

К данной статье расходов относятся командировочные расходы, арендная плата за использование имуществом, оплата услуг завязи и услуг сторонних организаций.

Расходы по данному пункту составляют $С_{нр}$ = 0 рублей.

5.3.7 Расчет прочих расходов

В статье «Прочие расходы» отображены расходы на выполнение проекта, которые не учтены в предыдущих статьях. Данные расходы следует принять равными 10 % от суммы всех предыдущих расходов:

$$C_{проч.} = (C_{мат} + C_{зп} + C_{соц} + C_{эл.об.} + C_{ам} + C_{нр}) \cdot 0{,}1;$$

$$C_{проч} = (1908{,}9 + 70261{,}13 + 21278{,}34 + 547{,}5 + 4612{,}25 + 0) \cdot 0{,}1 = 9860{,}81.$$

5.3.8 Цена разработки ВКР

Проведя расчет по всем статьям сметы затрат на разработку, можно определить общую себестоимость проекта. Смета на разработку проекта представлена в таблице 8.

Таблица 8. Затраты на разработку проекта

Статья затрат	**Условное обозначение**	**Сумма, руб.**
Материалы и покупные изделия	$C_{мат}$	13185,9
Основная заработная плата	$C_{зп}$	70261,13
Отчисления в социальные фонды	$C_{соц}$	21278,34
Расходы на электроэнергию	$C_{эл.}$	602,1
Амортизационные отчисления	$C_{ам}$	5545,35
Непосредственно учитываемые расходы	$C_{нр}$	0
Прочие расходы	$C_{проч}$	9860,81
Итого:		**120733,6**

5.3.9 Прибыль

Прибыль от реализации проекта составляет 20 % от расходов на разработку, т.е. 120733,6· 0,2 = 24146,72 рублей.

5.3.10 Расчет НДС

НДС составляет 18% от суммы затрат на разработку и прибыли. В данном случае это (120733,6+ 24146,72) · 0,18 = 26078,45 рублей.

5.3.11 Цена разработки ВКР

Цена разработки равна сумме полной себестоимости, прибыли и НДС. В данном случае $Ц_{ВКР(КР)}$ = 120733,6+ 26078,45 + 24146,72 = 170958,77 рублей.

5.4 Оценка экономической эффективности проекта

Автоматизированная система оплаты проезда(АСОП) предназначена для организации безналичной оплаты проезда и создания технологической основы для реализации новых разнообразных схем обслуживания пассажиров. Система позволяет перевести расчеты за проезд в безналичную форму, большой объем собранных данных о проездах дает возможность их последующего анализа, а в дальнейшем оптимизации работы транспорта, при этом учесть потребности пассажиров и транспортников. АСОП переводит работу всех участников в электронный вид, придает в совокупности с другими электронными системами (глобального позиционирования, систем составления расписания, систем безопасности) больший эффект и современный вид.

Количественная оценка экономической эффективности проекта является недостижимой в рамках выполнения данной работы.

5.4.1 Оценка научно-технического уровня ВКР

Научно-технический уровень характеризует влияние проекта на уровень и динамику обеспечения научно-технического прогресса в данной области. Для оценки научной ценности, технической значимости и эффективности, планируемых и выполняемых ВКР воспользуемся методом бальных оценок:

$$K_{НТУ} = \sum_{i=1}^{3} R_i \cdot n_i \,,$$

где $I_{НТУ}$ – интегральный индекс научно-технического уровня;

Ri – весовой коэффициент i-го признака научно-технического эффекта;

n_i – количественная оценка i-го признака научно-технического эффекта, в баллах.

Таблица 9. Оценки научно-технического уровня ВКР

Фактор НТУ	**Значимость**	**Уровень фактора**	**Выбранный балл**	**Обоснование выбранного балла**
Уровень новизны	0,4	Новая	7	Автоматизированная система оплаты проезда(АСОП) предназначена для организации безналичной оплаты проезда и создания технологической основы для реализации новых разнообразных схем обслуживания пассажиров
Теоретический уровень	0,1	Анализ связи между факторами	6	Данная модель системы дает возможность проводить статистический анализ пассажиропотока населенного пункта.
Возможность реализации	0,5	В течение первых лет	10	Полная реализация в течение одного года

Интегральный показатель научно-технического уровня для данного проекта составляет:

$0{,}4 \cdot 7 + 0{,}1 \cdot 2 + 0{,}5 \cdot 10 = 8$

Исходя из полученного значения можно сделать вывод, что данный проект имеет высокий уровень научно-технического эффекта.

5.5 SWOT-анализ.

На основе принятых технических решений и анализа рынка необходимо составить матрицу SWOT-анализа, в которой показаны сильные и слабые стороны проекта, возможности и угрозы при разработке. Матрицы SWOT представлена в приложении А.

Вывод: Проект должен реализовываться как можно более наукоемким, чтобы в дальнейшем его можно было продвигать на различных международных выставках и конференциях.

5.6 Ресурсоэффективность

Исходя из предварительного анализа технического задания, разработанного вышестоящим отделом, можно судить, что предлагаемый вариант является оптимальным и ресурсоэффективным. Вариантная проработка проводилась вышестоящим отделом. Необходимости в дальнейшем анализе эффективности нет.

	Сильные стороны: С1. Большой реализуемый потенциал. С2. Уникальность разработки в пределах ТПУ. С3. Привлечение молодых специалистов в область технологий беспроводной передачи данных	**Слабые стороны:** Сл1. Участники проекта не имеют большого опыта участия в подобных проектах. Сл2. Отсутствие финансирования новых научных разработок.
Возможности: В1. Оптимизация внутренних составляющих. В2. Использование финансирования научной деятельности ТПУ	**Направления развития:** Н1. Привлечение финансирование ТПУ за счет наукоемкости и открытости разработки. Н2. Популяризация тематики беспроводных технологий среди молодых специалистов	**Сдерживающие факторы:** Сд1. Отсутствие опыта может сказаться на оптимизации проекта. Сд2. Отсутствие финансирования научных разработок приведет к использованию уже существующих наработок, которые могут оказаться не совсем подходящими.
Угрозы: У1. Санкции со стороны других государств	**Угрозы развития:** Уг1. Санкции со стороны других государств могут	**Уязвимости:** Уя1. Отсутствие опыта создания проектов на

У2. Прекращение финансирования и поддержки проекта. У3. Не оправдание возложенных функций.	привести к закрытию источников поставки компонентов. Уг2. Прекращение финансирования ведет к закрытию проекта.	данную тему может привести к провалу проекта. Уя2. Отсутствие финансирования могут привести к прекращению поддержки руководителей разработки.

6. СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

Аннотация

Представление о понятии «Социальная ответственность» будущий специалист может получить из международного стандарта IC CSR-08260008000: 2011 «Социальная ответственность организации».

В настоящем стандарте используются термины и определения, такие как: **социальная ответственность** (social responsibility) - ответственность организации за воздействие ее решений и деятельности на общество и окружающую среду через прозрачное и этичное поведение, которое [22]:

- содействует устойчивому развитию, включая здоровье и благосостояние общества;
- учитывает ожидания заинтересованных сторон;
- соответствует применяемому законодательству и согласуется с международными нормами поведения;
- интегрировано в деятельность всей организации и применяется в ее взаимоотношениях.

Введение

Объектом дипломной работы являются работы, направленные на исследование беспроводных технологий передачи данных по радиочастотному каналу, а именно:

- изучение литературы по проектированию устройств беспроводной передачи данных;
- изучение применяемых технологий;
- применение технологий для решения задач предметной области;
- постановка компьютерного эксперимента;

Описанные выше работы проводятся в помещении, далее офис, находящемся на территории предприятия ООО «СТК» по адресу Красноармейская 101А, оф. 413.

Объект исследования - система бесконтактной оплаты проезда в общественном транспорте с функцией сбора статистики.

Согласно техническому заданию (ТЗ) планируется спроектировать систему бесконтактной оплаты проезда в общественном транспорте с функцией сбора статистики. Готовое устройство должно проводить сбор статистики пассажиропотока и отправлять данные на WEB сервер по средствам сети Internet, либо GPRS, либо Wi-Fi.

Под системой бесконтактной оплаты планируется использование многоразовых радиочастотных карт с занесенной на них информацией о владельце, текущем балансе карты, а также служебной информацией. Для выполнения требований к ТЗ необходимо спроектировать систему с использованием программируемого контроллера, создать рабочее место оператора (РМО) посредствам установки персонального компьютера (ПК) и подключения его к сети Интернет.

В разделе будут рассмотрены опасные и вредные факторы, оказывающие влияние на производственную деятельность технологического персонала, работающего с системой, рассмотрены воздействия разрабатываемой системы на окружающую среду, правовые и организационные вопросы, а также мероприятия в чрезвычайных ситуациях [23].

6.1 Производственная безопасность

6.1.1 Анализ вредных и опасных факторов, которые может создать объект исследования

Согласно номенклатуре, опасные и вредные факторы по ГОСТ 12.0.003-74 делятся на следующие группы:

- физические;
- химические;
- психофизиологические;
- биологические.

Перечень опасных и вредных факторов, влияющих на персонал в заданных условиях деятельности, представлен в таблице 10.

Таблица 10. Перечень опасных и вредных факторов

Источник фактора, наименование видов работ	Факторы		Нормативные документы
	Вредные	Опасные	
Работа с ПК; Выполнение визуальных осмотров всех основных и вспомогательных механизмов до начала их использования	Температура; Напряженность зрения; Напряженность труда в течение смены; Естественное и искусственное освещение;	Электрический ток.	Гигиенические требования к микроклимату производственных помещений СанПиН 2.2.4-548-96; Нормы естественного и искусственного освещения

при выполнении работ; Монтаж и пуско-наладка системы.	Электромагнитные излучения; Шум.		предприятий, СНиП 23-05-95; Допустимые уровни шумов в производственных помещениях. ГОСТ 12.1.003-83. ССБТ; Гигиенические требования к персональным электронно-вычислительным машинам и организации работы, СанПиН 2.2.2/2.4.1340-03; Защитное заземление, зануление, ГОСТ 12.1.030–81 ССБТ.

Эти факторы могут влиять на состояние здоровья, привести к травмоопасной или аварийной ситуации, поэтому следует установить эффективный контроль за соблюдением норм и требований, предъявленных к их параметрам.

6.1.2 Анализ вредных и опасных факторов, которые могут возникнуть на производстве при внедрении объекта исследования

В условиях современного интенсивного использования ЭВМ важное значение имеет изучение психофизиологических особенностей и возможностей человека с целью создания вычислительной техники, обеспечивающей максимальную производительность труда и сохранение здоровья людей. Игнорирование эргономики может привести к довольно серьезным последствиям.

При внедрении системы бесконтактной оплаты проезда в общественном транспорте с функцией сбора статистики важную роль играет планировка рабочего места оператора сбора данных. Она должна соответствовать правилам охраны труда и удовлетворять требованиям удобства выполнения работы, экономии энергии и времени оператора.

Основным документом, определяющим условия труда на персональных ЭВМ, являются «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы». Санитарные нормы и правила СанПиН 2.2.2/2.4.1340-03, которые были введены 30 июня 2003 года.

6.1.3 Электрический ток

Основным опасным фактором является опасность поражения электрическим током. Исходя из анализа состояния помещения, по степени опасности поражения электрическим током можно отнести к классу помещений без повышенной опасности (согласно ПУЭ).

Основным опасным производственным фактором на рабочем месте оператора поста управления является высокое напряжение в сети, от которой запитана система управления.

Электробезопасность должна обеспечиваться:

- конструкцией электроустановок;

- техническими способами и средствами защиты;
- организационными и техническими мероприятиями.

Электроустановки и их части должны быть выполнены таким образом, чтобы работающие не подвергались опасным и вредным воздействиям электрического тока и электромагнитных полей, и соответствовать требованиям электробезопасности.

Для обеспечения защиты от случайного прикосновения к токоведущим частям необходимо применять следующие технические способы и средства [24,25]:

- защитные оболочки;
- защитные ограждения (временные или стационарные);
- безопасное расположение токоведущих частей;
- изоляция токоведущих частей (рабочая, дополнительная, усиленная, двойная);
- изоляция рабочего места;
- малое напряжение;
- защитное отключение;
- заземление;
- предупредительная сигнализация, блокировка, знаки безопасности.

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

Перед началом работы следует убедиться в отсутствии свешивающихся со стола или висящих под столом проводов электропитания, в целостности вилки и

провода электропитания, в отсутствии видимых повреждений аппаратуры и рабочей мебели, в отсутствии повреждений и наличии заземления приэкранного фильтра.

Токи статического электричества, наведенные в процессе работы компьютера на корпусах монитора, системного блока и клавиатуры, могут приводить к разрядам при прикосновении к этим элементам. Такие разряды опасности для человека не представляют, но могут привести к выходу из строя компьютера. Для снижения величин токов статического электричества используются нейтрализаторы, местное и общее увлажнение воздуха, использование покрытия полов с антистатической пропиткой.

6.1.4 Микроклимат рабочего помещения.

Микроклимат производственных (рабочих) помещений – климат внутренней среды этих помещений, который определяется действующими на организм человека сочетаниями температуры, влажности и скорости движения воздуха, а также интенсивности теплового излучения от нагретых поверхностей. Влажность воздуха – содержание в воздухе водяного пара. Абсолютная влажность W – масса водяного пара в 1 м3 воздуха. Максимальная влажность F – масса водяного пара, который может насытить 1 м3 воздуха при данной температуре. Относительная влажность R – это отношение абсолютной влажности к максимальной. Указанные параметры – каждый в отдельности и в совокупности – оказывают значительное влияние на работоспособность человека, его самочувствие и здоровье. При определенных их значениях человек испытывает состояние теплового комфорта, что способствует повышению производительности труда, предупреждению простудных заболеваний. И, наоборот, неблагоприятные значения микроклиматических показателей могут стать причиной снижения производственных показателей в работе, привести к таким заболеваниям работающих как различные формы простуды, радикулит, хронический бронхит, тонзиллит и др.

Мероприятия по доведению микроклиматических показателей до нормативных значений включаются в комплексные планы предприятий по охране труда. Для создания благоприятных условий работы, соответствующих физиологическим потребностям человеческого организма, санитарные нормы устанавливают оптимальные и допустимые метеорологические условия в рабочей зоне помещения (таблица 11, 12) [6]. Также нормы учитывают категорию работ (легкая, средней тяжести, тяжёлая). В данном случае работа относится к категории **легкая** (1б).

Таблица 11. Оптимальные величины показателей микроклимата на рабочих местах производственных помещений (СанПиН 2.2.4.548-96)

Период года	Температура воздуха, C^0	Температура поверхностей, C^0	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	21 - 23	20 – 24	60-40	0,1
Теплый	23-25	22-26	60-40	0,1

Таблица 12. Допустимые величины показателей микроклимата на рабочих местах производственных помещений (СанПиН 2.2.4.548-96)

Период года	Температура воздуха, °С		Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с	
	диапазон ниже оптимальных величин	диапазон выше оптимальных величин			для диапазона температур воздуха ниже оптимальных величин, не более	для диапазона температур воздуха выше оптимальных величин, не более**
Холодный	19,0-20,9	23,1 - 24,0	18,0 - 25,0	15 - 75	0,1	0,2
Теплый	20,0 - 21,9	24,1 - 28,0	19,0 - 29,0	15 - 75	0,1	0,3

Для обеспечения оптимальных показателей микроклимата на рабочем месте, в холодное время года используются пассивные радиаторы отопления, в теплое время года используется система кондиционирования воздуха.

6.1.5. Производственное освещение

Освещение – получение, распределение и использование световой энергии для обеспечения благоприятных условий видения предметов и объектов. Оно влияет на настроение и самочувствие, определяет эффективность труда [26]. Рациональное освещение помещений и рабочих мест – одно из важнейших условий создания благоприятных и безопасных условий труда. Около 80 % из

общего объема информации человек получает через зрительный аппарат. Качество получаемой информации во многом зависит от освещения: неудовлетворительное в количественном или качественном отношении освещение не только утомляет зрение, но и вызывает утомление организма в целом. Нерационально организованное освещение может явиться причиной травматизма: плохо освещенные опасные зоны, слепящие источники света и блики от них, резкие тени и пульсации освещенности ухудшают видимость и могут вызвать неадекватное восприятие наблюдаемого объекта. Поэтому рациональное освещение помещений и рабочих мест – одно из важнейших условий для создания благоприятных и безопасных условий труда.

Искусственное освещение предусматривается в помещениях, в которых испытывается недостаток естественного света, а также для освещения помещения в те часы суток, когда естественная освещенность отсутствует. По принципу организации искусственное освещение можно разделить на два вида: общее и комбинированное [27].

Общее освещение предназначено для освещения всего помещения, оно может быть равномерным или локализованным. Общее равномерное освещение создает условия для выполнения работ в любом месте освещаемого пространства. При общем локализованном освещении светильники размещают в соответствии с расположением оборудования, что позволяет создавать повышенную освещенность на рабочих местах [27]. *Комбинированное* освещение состоит из общего и местного. Его целесообразно устраивать при работах высокой точности, а также при необходимости создания в процессе работы определенной направленности светового потока.

Местное освещение предназначено для освещения только рабочих поверхностей и не создает необходимой освещенности на прилегающих к ним участкам. Оно может быть стационарным и переносным [27].

Размещение светильников в помещении определяется следующими размерами, м:

H – высота помещения;

hc – расстояние светильников от перекрытия (свес);

hn = H - hc – высота светильника над полом, высота подвеса;

hp – высота рабочей поверхности над полом;

h =hn – hp – расчётная высота, высота светильника над рабочей поверхностью.

В данном случае высота помещения H = 3.5 м. Высота рабочей поверхности $h_{рп}$ =0,7м.

L – расстояние между соседними светильниками или рядами [28].

l – расстояние от крайних светильников или рядов до стены. Оптимальное расстояние l от крайнего ряда светильников до стены рекомендуется принимать равным L/3 [28].

При равномерном размещении люминесцентных светильников последние располагаются обычно рядами – параллельно рядам оборудования. При высоких уровнях нормированной освещённости люминисцентные светильники обычно располагаются непрерывными рядами, для чего светильники сочленяются друг с другом торцами.

Интегральным критерием оптимальности расположения светильников является величина $\lambda = L/h$, уменьшение которой удорожает устройство и обслуживание освещения, а чрезмерное увеличение ведёт к резкой неравномерности освещённости. В данном случае значение $\lambda = 1.1$ [28].

Выбираем светильник типа ОД 2-30, характеристика которого приведены в таблице 13.

Таблица 13. Характеристика светильника ОД 2-30

Мощность, Вт	Размеры, мм			Световой поток, лм
	Длина	Ширина	Высота	
2 х 30	933	204	156	1800

Таким образом, в данном случае:

hc = 0,156, H = 3,5,hp = 0,7

h =hn – hp = H – hc – hp = 3,5 - 0,156 - 0,7 = 2,6 м

Расстояние между светильниками L определяется как:

$$L = \lambda \cdot h$$

Таким образом, расстояние в данном случае определяется, как

L = 1.1 * 2,6 = 2,9 м.

Соответственно рекомендуемое расстояние от стен до крайнего ряда светильников определяется как l = 2,6/3 = 0.9 м

На рисунке 23 представлен план размещения общего освещения относительно рабочего места с соответствующими размерами (в метрах).

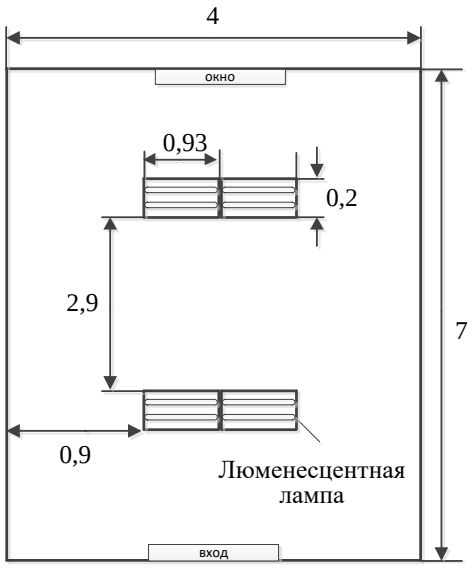


Рисунок 23. План размещения общего освещения (вид сверху)

Согласно СНиП 23-05-95 [27] норма освещённости для рассматриваемого рабочего места составляет 150 Лк.

Расчёт общего равномерного искусственного освещения горизонтальной рабочей поверхности выполняется методом коэффициента светового потока, учитывающим световой поток, отражённый от потолка и стен.

Световой поток лампы накаливания или группы люминесцентных ламп светильника определяется по формуле:

$$Ф = E_н \cdot S \cdot K_з \cdot Z *100/ (n \cdot \eta),$$

где $E_н$ – нормируемая минимальная освещённость по СНиП 23-05-95, лк;

S – площадь освещаемого помещения, $м^2$;

$K_з$ – коэффициент запаса, учитывающий загрязнение светильника (источника света, светотехнической арматуры, стен и пр., т.е. отражающих поверхностей), (наличие в атмосфере цеха дыма), пыли;

Z – коэффициент неравномерности освещения, отношение $E_{ср.}/E_{min}$. Для люминесцентных ламп при расчётах берётся равным 1,1;

n – число светильников;

η - коэффициент использования светового потока, %.

Коэффициент использования светового потока показывает, какая часть светового потока ламп попадает на рабочую поверхность. Он зависит от индекса помещения i, типа светильника, высоты светильников над рабочей поверхностью h и коэффициентов отражения стен ρ_c и потолка ρ_n.

Индекс помещения определяется по формуле

$$i = S/ h(A+B) ,$$

где h - допустимая высота подвеса светильников с люминесцентными лампами;

A – ширина;

В – длина.

Помещение имеет длину А= 4м, ширина В=7м, высота h= 2,6 м. Требуется создать освещение Е=150 лк. Коэффициент отражения светлых стен ρ_c = 50%, светлого потолка $\rho_п$ =70%. Коэффициент запаса $K_з$=1,5, коэффициент неравномерности Z = 1,1 [28].

В каждом ряду можно установить 2 светильника типа ОД 2-30 мощностью 30 Вт [7]. Учитывая, что в каждом светильнике установлено 2 лампы, общее число ламп в помещении N=8.

Находим индекс помещения

S = 28, h = 2,6, A = 4, B = 7

i = 28/2,6 *(4+7) = 0,97

Определяем коэффициент использования светового потока [28]:

η=0,49.

$Ф = \frac{150*28*1,5*1,1}{8*0,49}$= 1767 Лм.

Определяем потребный световой поток ламп в каждом из рядов:

Выбираем стандартную лампу ОД 30 Вт с потоком 1800 лм (таблица 5.3). Делаем проверку выполнения условия:

$-10\% \leq \frac{Ф_{л.станд} - Ф_{л.расч}}{Ф_{с.станд}} 100\% \leq \pm 20\%$ = -10%≤15%≤±20%

Условие выполняется.

Определяем электрическую мощность осветительной установки

P = 8*30 = 240 Вт.

6.1.6. Производственные шумы

Шум - это совокупность различных звуков, возникающих в процессе производства и неблагоприятно воздействующих на организм. Это понятие

обычно рассматривается с точки зрения экологии и медицины, то есть как угрозу жизнедеятельности, а не как фактор, мешающий работе, потому что постоянное его воздействие может принести непоправимый вред здоровью. Традиционно, рабочий шум был постоянной опасностью для работников, занятых в сфере тяжёлой промышленности и ассоциировался только с ухудшением слуха. Современные понятия охраны труда рассматривают шум как угрозу безопасности и здоровью работников многих профессий по различным причинам.

Шум может привести к нарушениям слуха (в случае постоянного нахождения при шуме более 85 децибел(dB)), может являться фактором стресса и повысить систолическое кровяное давление.

Дополнительно, он может способствовать несчастным случаям, маскируя предупреждающие сигналы и мешая сконцентрироваться.

Нормативным документом, регламентирующим уровни шума для различных категорий рабочих мест служебных помещений, является ГОСТ 12.1.003-83 «ССБТ. Шум. Общие требования безопасности» [29].

Помещения, в которых для работы используются ПК не должны граничить с помещениями, в которых уровни шума превышают нормируемые значения.

В помещениях, оборудованных ПК, которые являются основным источником шума при выполнении данных видов работ, уровень шума на рабочем месте не должен превышать 50 дБ [29].

При разработке технологических процессов, проектировании, изготовлении и эксплуатации машин, производственных зданий и сооружений, а также при организации рабочего места следует принимать все необходимые меры по снижению шума, воздействующего на человека на рабочих местах:

- применение шумобезопасной техники;
- использование средств и методов коллективной защиты по ГОСТ 12.1.029 - 80;

- применением средств индивидуальной защиты по ГОСТ 12.4.051-78.
- зоны с уровнем звука или эквивалентным уровнем звука выше 85 дБ *А* должны быть обозначены знаками безопасности по ГОСТ 12.4.026—76. Работающих в этих зонах администрация обязана снабжать средствами индивидуальной защиты по ГОСТ 12.4.051—78.
- На предприятиях, в организациях и учреждениях должен быть обеспечен контроль уровней шума на рабочих местах не реже одного раза в год.

6.1.7. Электромагнитные поля

Ионизирующее излучение – поток микрочастиц, способных ионизировать вещество. Электромагнитное излучение, создаваемое персональным компьютером, имеет сложный спектральный состав в диапазоне частот от 0 Гц до 1000 МГц: электрическую (Е) и магнитную (Н) составляющие.

Основным источником электромагнитных излучений от мониторов ПЭВМ (ПК) является трансформатор высокой частоты строчной развертки.

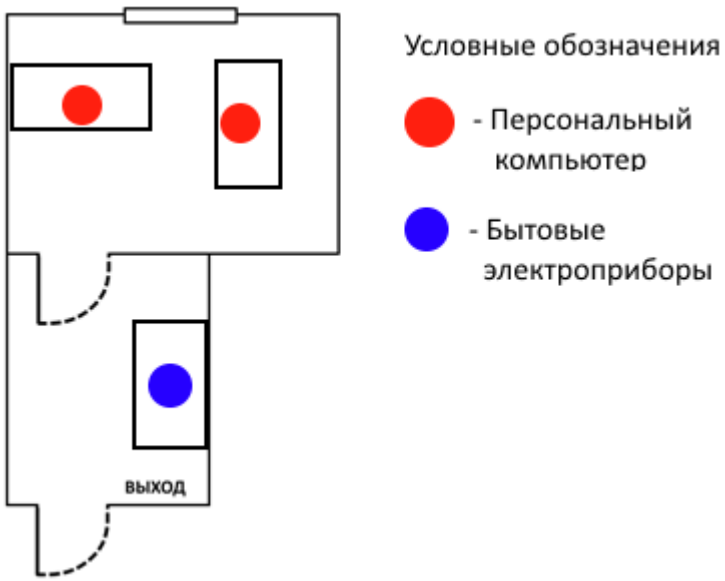


Рисунок 24. Основные источники ЭМП

В соответствии с СанПиНом 2.2.4.1191-03 [9] нормы допустимых уровней напряженности электрических полей зависят от времени пребывания человека в контролируемой зоне. Время допустимого пребывания в рабочей зоне в часах

составляет Т=50/Е–2. Работа в условиях облучения электрическим полем с напряженностью 20–25 кВ/м продолжается не более 10 минут. При напряженности не выше 5 кВ/м присутствие людей в рабочей зоне разрешается в течение 8 часов.

Конструкция монитора ПЭВМ должна обеспечивать мощность экспозиционной дозы рентгеновского излучения в любой точке на расстоянии 0,05 м от экрана и корпуса монитора ПК при любых положениях регулирующих устройств и не должна превышать 7,74 х 10 А/кт, что соответствует эквивалентной дозе, равной 0,1 мбэр/час (100 мкр/час).

Далее в таблице 14 представлены предельно-допустимые уровни напряженности на рабочих местах [30].

Таблица 14**.** Предельно-допустимые уровни напряженности на рабочих местах

Время воздействия за рабочий день, мин	Условия воздействия			
	Общее		локальное	
	ПДУ напряженности кА/м	ПДУ магнитной индукции мТл	ПДУ напряженности кА/м	ПДУ магнитной индукции мТл
0 - 10	24	30	40	50
11 - 60	16	20	24	30
61 - 480	8	10	12	15

Мероприятия по снижению излучений включают:

- мероприятия по сертификации ПЭВМ (ПК) и аттестации рабочих мест;

- применение экранов и фильтров;

- организационно-технические мероприятия;

- применение средств индивидуальной защиты путем экранирования пользователя ПЭВМ (ПК) целиком или отдельных зон его тела;

- использование и применение профилактических напитков;

- использование иных технических средств защиты от патогенных излучений.

6.1.7. Пожарная безопасность

Пожарная безопасность – комплекс организационных и технических мероприятий, направленных на обеспечение безопасности людей, на предотвращение пожара, ограничение его распространения, а также на создание условий для успешного тушения пожара [31].

Рабочее помещение, в котором производится работа по выполнению ВКР по пожарной и взрывной опасности относят к категории Г (умеренная пожароопасность).

К противопожарным мероприятиям в помещении относят следующие мероприятия:

1) помещение должно быть оборудовано: средствами тушения пожара (огнетушителями, ящиком с песком, стендом с противопожарным инвентарем); средствами связи; должна быть исправна электрическая проводка осветительных приборов и электрооборудования.

2) каждый сотрудник должен знать место нахождения средств пожаротушения и средств связи; помнить номера телефонов для сообщения о пожаре; уметь пользоваться средствами пожаротушения.

Помещение обеспечено средствами пожаротушения в соответствии с нормами [10]:

1) пенный огнетушитель ОП-10 – 1 шт.

2) углекислотный огнетушитель ОУ-5 – 1 шт.

При невозможности самостоятельно потушить пожар необходимо вызвать пожарную команду, после чего поставить в известность о случившемся инженера по техники безопасности.

Вынужденная эвакуация при пожаре протекает в условиях нарастающего действия опасных факторов пожара. Кратковременность процесса вынужденной эвакуации достигается устройством эвакуационных путей и выходов, число, размеры и конструктивно-планоровачные решения которых регламентированы строительными нормами СНиП 2.01.02-85.

Помещение и этаж оборудованы следующими средствами оповещения:

- световая индикация в коридорах этажа;
- звуковая индикация в виде громкоговорителя;
- пассивными датчиками задымленности.

Пути эвакуации указаны на рисунках 25 и 26.

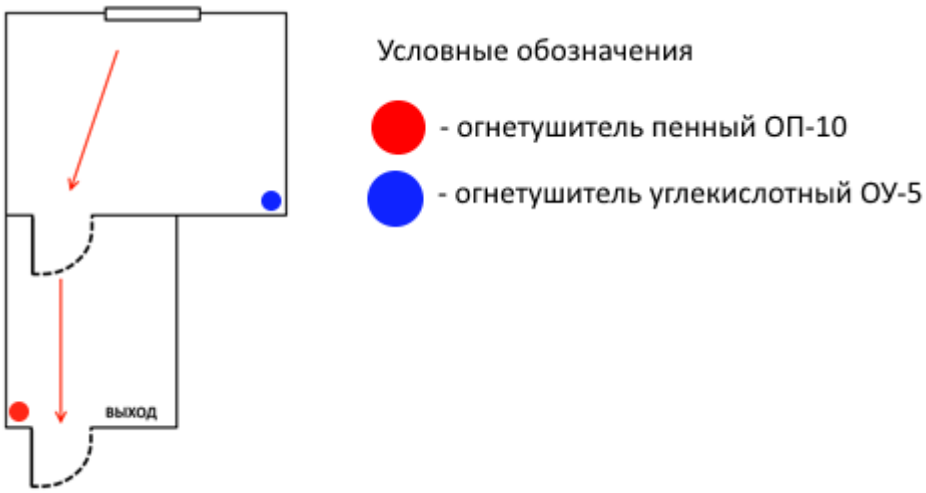


Рисунок 25. План эвакуации

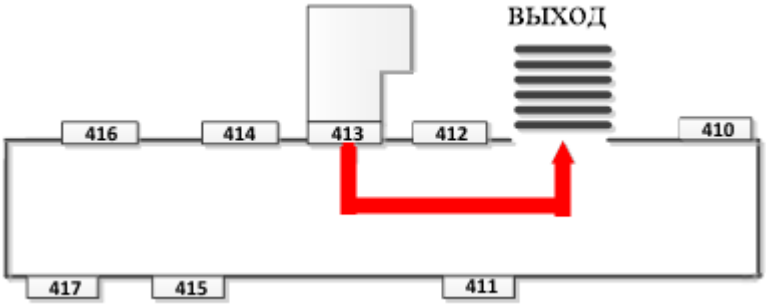


Рисунок 26. План эвакуации

6.2 Экологическая безопасность

Охрана окружающей среды сводится к устранению отходов бытового мусора и отходам жизнедеятельности человека. В случае выхода из строя ПК, они списываются и отправляются на специальный склад, который при необходимости принимает меры по утилизации списанной техники и комплектующих [32].

На сегодняшний день одним из самых распространенных источников ртутного загрязнения являются вышедшие из эксплуатации люминесцентные лампы. Каждая такая лампа, кроме стекла и алюминия, содержит около 60 мг ртути. Поэтому отслужившие свой срок люминесцентные лампы, а также другие приборы, содержащие ртуть, представляют собой опасный источник токсичных веществ.

В целом, утилизация ламп предполагает передачу использованных ламп предприятиям – переработчикам, которые с помощью специального оборудования перерабатывают вредные лампы в безвредное сырье – сорбент, которое в последующем используют в качестве материала для производства, например, тротуарной плитки.

Под хранением отходов понимается временное размещение их в специально отведённых для этого местах или объектах до их утилизации. Отработанные люминесцентные лампы, согласно Классификатору отходов ДК

005-96, утвержденному приказом Госстандарта № 89 от 29.02.96 г., относятся к отходам, которые сортируются и собираются отдельно, поэтому утилизация люминесцентных ламп и их хранение должны отвечать определенные требованиям.

Хранение и удаление отходов (в данном случае - люминесцентных ламп) осуществляются в соответствии с требованиями экологической безопасности согласно ГСанПин 2.2.7.029-99 наполнения тару с отходами закрывают герметически стальной крышкой, при необходимости заваривают и передают по договору специализированным предприятиям, имеющим лицензию на их утилизацию.

6.3 Защита в чрезвычайных ситуациях

В данном случае на объекте (офис) могут возникать чрезвычайные ситуации (ЧС) следующего характера:

- техногенные;
- экологические;
- природные.

Наиболее типичной ЧС для помещения, котором производится выполнение ВКР, является пожар. Данная ЧС может произойти в случае замыкания электропроводки оборудования, обрыву проводов, не соблюдению мер пожаробезопасности и т.д.

Для того что бы избежать возникновения пожара необходимо проводить следующие профилактические работы, направленные на устранение возможных источников возникновения пожара:

- периодическая проверка проводки;
- отключение оборудования при покидании рабочего места;
- проведение инструктажа работников о пожаробезопасности.

Для того что бы увеличить устойчивость офисного помещения к ЧС необходимо устанавливать системы противопожарной сигнализации, реагирующие на дым и другие продукты горения, установка огнетушителей, обеспечить офис и проинструктировать рабочих о плане эвакуации из офиса, а также назначить ответственных за эти мероприятия. Два раза в год (в летний и зимний период) проводить учебные тревоги для отработки действий при пожаре.

В ходе осмотра офисного помещения были выявлены системы, сигнализирующие о наличие пожара или задымленности помещения и наличие огнетушителей.

В случае возникновения ЧС как пожар, необходимо предпринять меры по эвакуации персонала из офисного помещения в соответствии с планом эвакуации (рисунок 25, 26). При отсутствии прямых угроз здоровью и жизни произвести попытку тушения возникшего возгорания огнетушителем. В случае потери контроля над пожаром, необходимо эвакуироваться вслед за сотрудниками по плану эвакуации и ждать приезда специалистов, пожарников. При возникновении пожара должна сработать система пожаротушения, издав предупредительные сигналы, и передав на пункт пожарной станции сигнал о ЧС, в случае если система не сработала, по каким-либо причинам, необходимо самостоятельно произвести вызов пожарной службы по телефону 101, сообщить место возникновения ЧС и ожидать приезда специалистов.

6.4 Правовые и организационные вопросы обеспечения безопасности

В Правилах указаны основные требования к помещениям, микроклимату, шуму и вибрации, освещению помещений и рабочих мест, организации и оборудованию рабочих мест:

- Рабочее место должно быть организовано с учетом эргономических требований согласно ГОСТ 12.2.032-78 «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования» [23] и ГОСТ

12.2.061-81 «ССБТ. Оборудование производственное. Общие требования безопасности к рабочим местам» [24];

- Конструкция рабочей мебели (рабочий стол, кресло, подставка для ног) должна обеспечивать возможность индивидуальной регулировки соответственно росту пользователя и создавать удобную позу для работы. Вокруг ПК должно быть обеспечено свободное пространство не менее 60-120см;

На рисунке 27 схематично представлены требования к рабочему месту

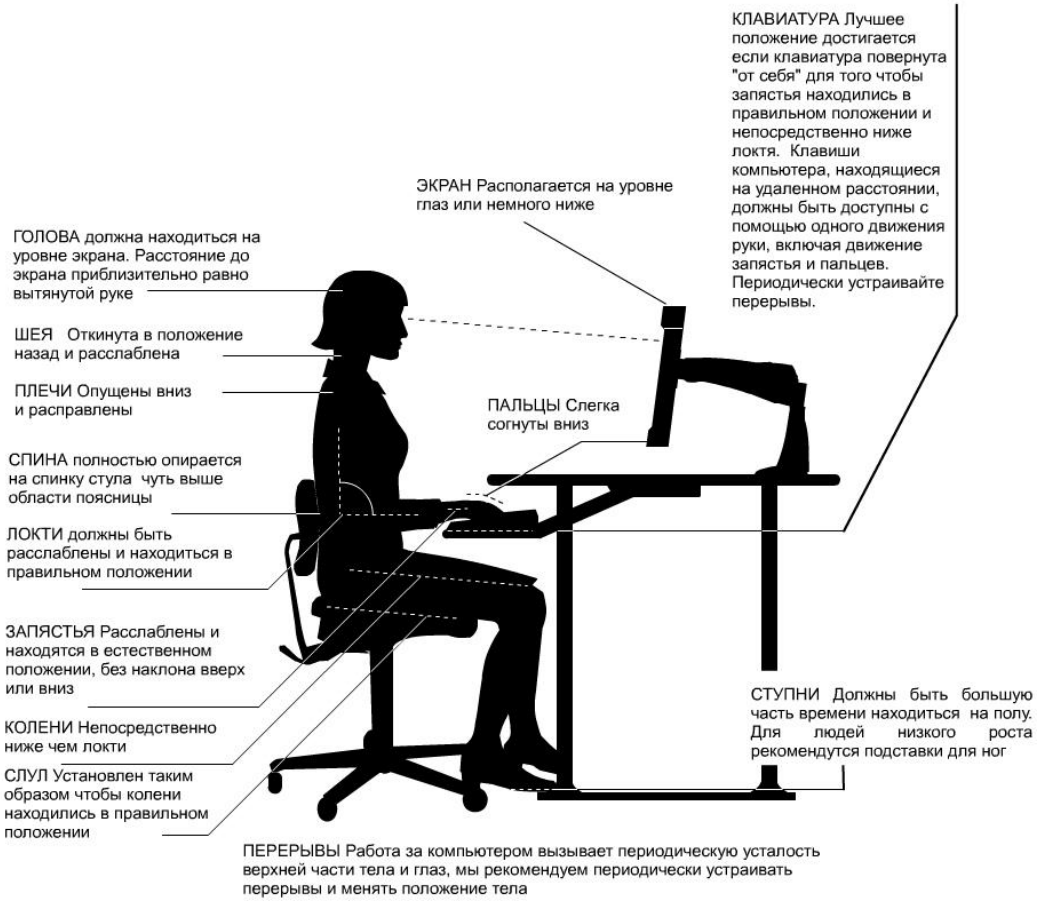


Рисунок 27. Организация рабочего места

В соответствии с трудовым кодексом РФ и правовыми нормами обеспечения безопасности, указанных выше, предусмотрена рациональная организация труда в течение смены, которая предусматривает:

- длительность рабочей смены не более 8 часов;
- установление двух регламентируемых перерывов (не менее 20 минут после 1-2 часов работы, не менее 30 минут после 2 часов работы);
- обеденный перерыв не менее 40 минут.

Обязательно предусмотрен предварительный медосмотр при приеме на работу и периодические медосмотры.

Каждый сотрудник должен пройти инструктаж по технике безопасности перед приемом на работу и в дальнейшем, должен быть пройден инструктаж по электробезопасности и охране труда.

ЗАКЛЮЧЕНИЕ

В ходе выполнения дипломной работы были изучены транспортные платежные системы, существующие на данный момент. Были выявлены недостатки существующих систем, которые были учтены в проектируемой системе.

В связи с тем, что данный проект охватывает различные предметные области, были изучены: способы бесконтактной передачи данных в различных исполнениях, устройство и принципы работы RFID технологий, изучен и применен в работе ресурс API Яндекс. Карт, изучены принципы построения баз данных и web – серверов, проанализированы существующие алгоритмы защиты передаваемых данных, написана программа, шифрующая информацию алгоритмом DES, спроектированы компоненты системы, разработаны схемы алгоритмов работы устройств, изучены физические принципы работы плоских антенн, проведен обзор и подбор компонентов устройств системы, реализован функционирующий макет, позволяющий тестировать возможности RFID-карт.

В дальнейшем планируется доработка системы, а именно реализация системы в виде стенда, отладка взаимодействия компонентов системы, доработка программной и аппаратной части. Разработка мобильного приложения с привязкой проездного билета к мобильному телефону для проведения платежей с помощью последнего. Также требует более детальной проработки устройство считывания данных с пользовательских карт. Требуется провести исследования по существующим реальным системам сбора статистики, усовершенствовать текущую модель, для наглядного отображения работы проекта в условиях, приближенных к действительным.

СПИСОК ИСТОЧНИКОВ

1. Новости в Томске: Заммэра Томска: перевозчики не могут найти кондукторов для работы в маршрутках [Электронный ресурс]. – Режим доступа: https://news.vtomske.ru/news/135909-zammera-tomska-perevozchiki-ne-mogut-naiti-konduktorov-dlya-raboty-v-marshrutkah (дата обращения 28.02.2017)

2. TOMSKRU городской портал: Власти: томичи не хотят работать кондукторами в маршрутках [Электронный ресурс]. – Режим доступа: http://www.tomsk.ru/news/view/121578 (дата обращения 28.02.2017)

3. Википедия: Екарта [Электронный ресурс]. – Режим доступа: https://goo.gl/DIXRnQ (Дата обращения 12.03.2017)

4. Википедия: Тройка (транспортная карта) [Электронный ресурс]. – Режим доступа: https://goo.gl/Oj5F6w (Дата обращения 12.03.2017)

5. ИНТУИТ: общие понятия безопасности персональных данных [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/680 (Дата обращения 15.03.2017)

6. Википедия: шифрование [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki (Дата обращения 17.03.2017)

7. Википедия: криптосистема с открытым ключем [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki (Дата обращения 23.03.2017)

8. Architect: типы алгоритмов, симметричное шифрование [Электронный ресурс]. – Режим доступа: http://students.uni-vologda.ac.ru/pages/pm00/kan (Дата обращения 12.02.2017)

9. Хабрахабр: LW-криптография: шифры для RFID-систем [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/119700/ (Дата обращения 23.03.2017)

10. cryptowiki: криптография в технологии RFID [Электронный ресурс]. – Режим доступа: http://cryptowiki.net/index.php?title= _RFID (Дата обращения 11.03.2017)

11. SlideShare: легковесная криптография [Электронный ресурс]. – Режим доступа: https://www.slideshare.net/phdays/ss-13376519 (Дата обращения 20.03.2017)

12. Allbest: RFID-технологии [Электронный ресурс]. – Режим доступа: http://otherreferats.allbest.ru/radio/00306444_0.html (Дата обращения 7.03.2017)

13. Studfiles: моделирование процессов шифрования, дешифрования с помощью криптографического алгоритма замены [Электронный ресурс]. – Режим доступа: http://www.studfiles.ru/preview/3563960/page:2/ (Дата обращения 9.03.2017)

14. Mindhalls: реализация и криптоанализ шифра простой замены [Электронный ресурс]. – Режим доступа: http://mindhalls.ru/exchange-code/ (Дата обращения 9.03.2017)

15. Хабрахабр: RFID-системы [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/194908/ (Дата обращения 5.04.2017)

16. Crypto: алгоритм DES и его варианты [Электронный ресурс]. – Режим доступа: http://crypto.pp.ua/2010/12/algoritm-des-i-ego-varianty/ (Дата обращения 25.02.2017)

17. Википедия: сеть Фейстеля [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/ (Дата обращения 30.03.2017)

18. Lifeexample: PHP работа с базой данных [Электронный ресурс]. – Режим доступа: http://lifeexample.ru/php-primeryi-skriptov/php-rabota-s-bazoy-dannyih-chast-1.html (Дата обращения 17.05.2017)

19. MySQL: справочное руководство по MySQL [Электронный ресурс]. – Режим доступа: http://www.mysql.ru/docs/man/Database_use.html (Дата обращения 31.04.2017)

20. API Яндекс.Карт: набор сервисов, которые позволяют использовать картографические данные [Электронный ресурс]. – Режим доступа: https://tech.yandex.ru/maps/ (Дата обращения 18.04.2017)

21. Международный стандарт «Социальная ответственность организации. Требования». 2011. URL: http://www.trud22.ru/partner/socotvrab/standart/ (дата обращения 11.03.2015)

22. ГОСТ 12.2.032-78 «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования»

23. ГОСТ 12.2.061-81 «ССБТ. Оборудование производственное. Общие требования безопасности к рабочим местам»

24. ГОСТ 12.1.009-76 «Электробезопасность. Термины и определения»

25. ГОСТ 12.1.019-79 ССБТ «Электробезопасность. Общие требования и номенклатура видов защиты».

26. СНиП 23-05-95. «Естественное и искусственное освещение».

27. Расчёт искусственного освещения. Методические указания к выполнению индивидуальных заданий для студентов дневного и заочного обучения всех специальностей. Томск. 2008 г. 12 с.

28. ГОСТ 12.1.003-83 «ССБТ. Шум. Общие требования безопасности».

29. СанПиН 2.2.4.1191-03. «Электромагнитные поля в производственных условиях».

30. СНиП 21-01-97. «Пожарная безопасность зданий и сооружений».

31. ГОСТ 17.4.3.04-85. «Охрана природы. Почвы. Общие требования к контролю и охране от загрязнения».

32. СанПиН 2.2.4.548-96. «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

ПРИЛОЖЕНИЕ А

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Diagnostics;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace protect_inf_LR1
{
    public partial class Form1 : Form
    {
        private const int sizeOfBlock = 128; //в DES размер блока 64 бит, но
поскольку в unicode символ в два раза длинее, то увеличим блок тоже в два раза
        private const int sizeOfChar = 16; //размер одного символа (in Unicode 16
bit)

        private const int shiftKey = 2; //сдвиг ключа

        private const int quantityOfRounds = 16; //количество раундов

        string[] Blocks; //сами блоки в двоичном формате

        public Form1()
        {
            InitializeComponent();
        }

        //зашифровать
        private void buttonEncrypt_Click(object sender, EventArgs e)
        {
            if (textBoxEncodeKeyWord.Text.Length > 0)
            {
                string s = "";

                string key = textBoxEncodeKeyWord.Text;

                StreamReader sr = new StreamReader("in.txt");

                while (!sr.EndOfStream)
                {
                    s += sr.ReadLine();
                }

                sr.Close();

                s = StringToRightLength(s);

                CutStringIntoBlocks(s);

                key = CorrectKeyWord(key, s.Length / (2 * Blocks.Length));
                textBoxEncodeKeyWord.Text = key;
                key = StringToBinaryFormat(key);

                for (int j = 0; j < quantityOfRounds; j++)
                {
                    for (int i = 0; i < Blocks.Length; i++)
                        Blocks[i] = EncodeDES_One_Round(Blocks[i], key);

                    key = KeyToNextRound(key);
                }

                key = KeyToPrevRound(key);
```

```
            textBoxDecodeKeyWord.Text = StringFromBinaryToNormalFormat(key);

            string result = "";

            for (int i = 0; i < Blocks.Length; i++)
                    result += Blocks[i];

            StreamWriter sw = new StreamWriter("out1.txt");
            sw.WriteLine(StringFromBinaryToNormalFormat(result));
            sw.Close();

            Process.Start("out1.txt");
        }
        else
            MessageBox.Show("Введите ключевое слово!");
    }

    //расшифровать
    private void buttonDecipher_Click(object sender, EventArgs e)
    {
        if (textBoxDecodeKeyWord.Text.Length > 0)
        {
            string s = "";

            string key = StringToBinaryFormat(textBoxDecodeKeyWord.Text);

            StreamReader sr = new StreamReader("out1.txt");

            while (!sr.EndOfStream)
            {
                s += sr.ReadLine();
            }

            sr.Close();

            s = StringToBinaryFormat(s);

            CutBinaryStringIntoBlocks(s);

            for (int j = 0; j < quantityOfRounds; j++)
            {
                for (int i = 0; i < Blocks.Length; i++)
                    Blocks[i] = DecodeDES_One_Round(Blocks[i], key);

                key = KeyToPrevRound(key);
            }

            key = KeyToNextRound(key);

            textBoxEncodeKeyWord.Text = StringFromBinaryToNormalFormat(key);

            string result = "";

            for (int i = 0; i < Blocks.Length; i++)
                result += Blocks[i];

            StreamWriter sw = new StreamWriter("out2.txt");
            sw.WriteLine(StringFromBinaryToNormalFormat(result));
            sw.Close();

            Process.Start("out2.txt");
        }
        else
            MessageBox.Show("Введите ключевое слово!");
    }

    //доводим строку до размера, чтобы делилась на sizeOfBlock
    private string StringToRightLength(string input)
    {
```

```
            while (((input.Length * sizeOfChar) % sizeOfBlock) != 0)
                input += "#";

            return input;
        }

        //разбиение обычной строки на блоки
        private void CutStringIntoBlocks(string input)
        {
            Blocks = new string[(input.Length * sizeOfChar) / sizeOfBlock];

            int lengthOfBlock = input.Length / Blocks.Length;

            for (int i = 0; i < Blocks.Length; i++)
            {
                Blocks[i] = input.Substring(i * lengthOfBlock, lengthOfBlock);
                Blocks[i] = StringToBinaryFormat(Blocks[i]);
            }
        }

        //разбиение двоичной строки на блоки
        private void CutBinaryStringIntoBlocks(string input)
        {
            Blocks = new string[input.Length / sizeOfBlock];

            int lengthOfBlock = input.Length / Blocks.Length;

            for (int i = 0; i < Blocks.Length; i++)
                Blocks[i] = input.Substring(i * lengthOfBlock, lengthOfBlock);
        }

        //перевод строки в двоичный формат
        private string StringToBinaryFormat(string input)
        {
            string output = "";

            for (int i = 0; i < input.Length; i++)
            {
                string char_binary = Convert.ToString(input[i], 2);

                while (char_binary.Length < sizeOfChar)
                    char_binary = "0" + char_binary;

                output += char_binary;
            }

            return output;
        }

        //доводим длину ключа до нужной
        private string CorrectKeyWord(string input, int lengthKey)
        {
            if (input.Length > lengthKey)
                input = input.Substring(0, lengthKey);
            else
                while (input.Length < lengthKey)
                    input = "0" + input;

            return input;
        }

        //шифрование DES один раунд
        private string EncodeDES_One_Round(string input, string key)
        {
            string L = input.Substring(0, input.Length / 2);
            string R = input.Substring(input.Length / 2, input.Length / 2);

            return (R + XOR(L, f(R, key)));
        }
        //расшифровка DES один раунд
```

```
        private string DecodeDES_One_Round(string input, string key)
        {
            string L = input.Substring(0, input.Length / 2);
            string R = input.Substring(input.Length / 2, input.Length / 2);

            return (XOR(f(L, key), R) + L);
        }

        //XOR двух строк с двоичными данными
        private string XOR(string s1, string s2)
        {
            string result = "";

            for (int i = 0; i < s1.Length; i++)
            {
                bool a = Convert.ToBoolean(Convert.ToInt32(s1[i].ToString()));
                bool b = Convert.ToBoolean(Convert.ToInt32(s2[i].ToString()));

                if (a ^ b)
                    result += "1";
                else
                    result += "0";
            }
            return result;
        }

        //шифрующая функция f. в данном случае это XOR
        private string f(string s1, string s2)
        {
            return XOR(s1, s2);
        }
        //вычисление ключа для следующего раунда шифрования. циклический сдвиг >> 2
        private string KeyToNextRound(string key)
        {
            for (int i = 0; i < shiftKey; i++)
            {
                key = key[key.Length - 1] + key;
                key = key.Remove(key.Length - 1);
            }

            return key;
        }

        //вычисление ключа для следующего раунда расшифровки. циклический сдвиг << 2
        private string KeyToPrevRound(string key)
        {
            for (int i = 0; i < shiftKey; i++)
            {
                key = key + key[0];
                key = key.Remove(0, 1);
            }

            return key;
        }

        //переводим строку с двоичными данными в символьный формат
        private string StringFromBinaryToNormalFormat(string input)
        {
            string output = "";

            while (input.Length > 0)
            {
                string char_binary = input.Substring(0, sizeOfChar);
                input = input.Remove(0, sizeOfChar);

                int a = 0;
                int degree = char_binary.Length - 1;

                foreach (char c in char_binary)
                    a += Convert.ToInt32(c.ToString()) * (int)Math.Pow(2, degree--);
```

```
                output += ((char)a).ToString();
            }

            return output;
        }
    }
}
```

ПРИЛОЖЕНИЕ Б

ПРИЛОЖЕНИЕ В. ЧАСТЬ ВКР НА АНГЛИЙСКОМ ЯЗЫКЕ

Подраздел 1. REVIEW OF ANALOGUES

Подраздел 2.DATA PROTECTION METHODS

Подраздел 3. STRUCTURAL SCHEMES OF ALGORITHMS OF WORK OF DEVICES

Студент:

Группа	ФИО	Подпись	Дата
8ВМ5А	Россамахин Дмитрий Игоревич		

Консультант кафедры ИСТ:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Мирошниченко Евгений Александрович	к.т.н.		

Консультант – лингвист кафедры ИЯИК:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
старший преподаватель	Рыбушкина Светлана Владимировна	-		

1. Review OF ANALOGIES

The main systems used in the Russian Federation:

• ECARTA (Ekaterinburg)

• TROIKA (Moscow)

Main information on these systems:

EKAPTA - electronic payment system for public transport in Ekaterinburg, as well as a plastic RFID card used in this system. It operates in Ekaterinburg tram, trolleybus, subway and bus (all municipal and most commercial routes). The operator of the system is the company "I-Network" (JSC "Information Network") [2].

The experiment on the introduction of ECARTA was launched in the Ekaterinburg subway on July 15, 2009. The experiment was attended by 200 volunteers, selected by the organizers of the project by random sampling. From July 15 to August 2, they made almost 2.5 thousand trips to the subway. The sale of ECART started in the metro on December 1. The issuance of registered social ECART began on December 7 in all branches of the Unified Settlement Center. The system operation in land transport and personal card management began on January 1, 2010. 12 rubles for social card holders and 14 rubles for ordinary passengers. It is also possible to use EKARTU as a single travel ticket for 4 types of transport, a tariff component of 300 rubles for holders of the social card and 1500 for the rest and having no analogues in the form of paper travel cards [3].

Pros of the system:

• System versatility

• Massiveness of the system

Cons of the system:

• It possible to make a copy of the card

• For payment it is necessary to bring the card to the validator

• Necessity of participation of the conductor at payment

TROIKA - is a contactless plastic card Mifare Plus X 2k, designed to store money for payment on the transport; Essentially it is a transport electronic wallet.

It was introduced after the change of the tariff system for the use of municipal transport in Moscow on April 2, 2013.

On the "Troika" card it is possible to "fix" travel tickets for a certain number of TAT, "Bus", "uniform" and "90 minutes" trips, without limit "United", "Bus" and TAT and subscriptions for suburban railway service.

Before registering a TAT ticket and / or subscription to the train, the owner is required, if the card was purchased before September 20, 2013, to update the media program (card) by replenishing the account through the Moscow Metro ticket machine, except for ticket machines, Equipped with MasterCard PayPass technology.

If there is an updated card, the owner can "record" the required ticket through the cashier. But the "Troika" transport card cannot use the money to pay for the ticket, the money already put into the account. For this reason, despite the fact that there may be enough money on the card in the account, the owner cannot spend it on buying a ticket. At the same time, due to this feature of the card, the passenger always has the opportunity to pay the fare by the card, even if the trips on the "recorded" ticket have expired or the validity period has expired [4].

Pros of the system:

• System versatility

• Adequacy of technology

• Global network for collecting statistics (in the metro)

• High degree of system security (in metro)

Cons of the system:

• Ability to make a copy of the map (ground transportation)

• For payment it is necessary to bring the card to the validator

2.DATA PROTECTION METHODS

One of the important aspects of the operation of any system related to the transfer and storage of data is their protection from intentional access and change. The system developed in this work is the most vulnerable, since there is both a remote transfer of data from device to device (dynamic state) and a web server on which a large amount of information (static state) will be stored.

Protection of static information at this level of the system is not a priority, since in the future each user will have his own version of the equipment for storing information and software for managing static information processes.

The most important is to protect the transmitted information, avoid leaks and other harmful effects. In this regard, it is necessary to understand the general principle of stealing dynamic data, as well as ways to protect them.

The principle of theft of dynamic data is the principle that there is a data sender, a data receiver, a data channel. An attacker tries to steal data at the same time when the data is in the process of flowing through the data transmission channel. Figure 1 shows a schematic representation of the dynamic data theft:

Figure 1. Schematic representation of dynamic data theft

As can be seen from the figure, the hacker interacts directly only with the data transfer channel, the attacker does not interact with the sender or recipient of the data. Interact with the data transmission channel it can in many ways - both with the help of various software, and with the help of physical devices [5].

The most common way to protect information from any type of interception is data encryption.

Data encryption is a reversible transformation of information for the purpose of hiding from unauthorized persons, with the provision, at the same time, to authorized users of access to it [6].

2.1 Encryption Algorithms

Encryption algorithms are divided into two large classes: symmetric (AES, GOST, Blowfish, CAST, DES) and asymmetric (RSA, El-Gamal). Symmetric encryption algorithms use the same key for encrypting information and for decrypting it, and asymmetric algorithms use two keys - one for encrypting, the other for decryption.

In asymmetric systems, you need to use long keys (512 bits or more). A long key dramatically increases the encryption time. In addition, the generation of keys is very long. But you can distribute keys on unprotected channels [7].

Symmetric algorithms using shorter keys, so encryption is faster. But in such systems it is difficult to distribute the keys [8].

Because in this system the speed of the system's work is important, Namely the processing time of the data from the card, we will consider only symmetric algorithms of encryption.

2.2 Algorithms LW (low weight)

LW cryptography - the section of cryptography aims to develop algorithms for use in devices that are not able to provide most of the existing ciphers with sufficient resources for operation.

It is clear that creating a new cipher without certain flaws is a rather difficult task, but the existing algorithms show good results and, possibly, will find their application in cryptosystems providing RFID security [9].

There are both block and streamlined LW algorithms. At the moment, only three described LW-cipher streams are known that have relatively acceptable characteristics. These are the algorithms MICKEY, Trivium and GRAIN. However, these ciphers are not applicable in passive RFID systems due to the individual characteristics of each of them. For example, Trivium requires an area on the chip that exceeds the permissible limit by more than 1.5 times (3488GE with a limit of 2000GE). The current version of the GRAIN cipher can be successfully attacked on related keys. As for MICKEY, developers have tested its resistance only to some attacks, but this is not enough to ensure confidence in its reliability [10].

Thus, we can conclude that at the moment there is no algorithm among the stream ciphers that satisfies the basic requirements of RFID systems.

In the section of block ciphers, the situation is somewhat better. Let us consider in more detail some block LW-algorithms.

In Table 2 shows the comparative characteristics of the algorithms.

Algorithm	Key size	Block size	Cycle/blocks	Speed, kbs	Amount of GE
DESL	56	64	144	44.4	1848
KATAN32	80	32	256	12.5	812
KATAN64	80	64	255	25.1	1027
PRESENT-80	80	64	547	11.7	1075
PRESENT-128	128	64	559	11.45	1391
Trivium	80	1	1	100	2599
Grain	80	1	1	100	1294

For optimal using of DES in RFID systems, it was modified. First of all, permutations of IP and IP-1 were excluded, which do not affect the stability, but take place on the diagram. Then, eight original S-boxes were replaced by one, repeated eight times. The authors proved that this change does not affect the stability of the algorithm to the main attacks, such as linear and difference cryptanalysis. The received code is called DESL. Its main disadvantage is the small size of the key - 56 bits. Although for its disclosure a full search requires months of work of a cluster of several dozen computers, on a supercomputer this task is solved in just three days. Therefore, such an algorithm should be used only where short-term protection is required, or where the importance of the protected data is relatively small. To implement the algorithm, you need 1848GE, which is an acceptable requirement for the LW-cipher [11].

The next block LW-algorithm that meets all the requirements of RFID-systems is PRESENT.

In difference DESL, this cipher uses a key with a length of 80 bits, which greatly improves its reliability. Developers have investigated the vulnerability of this

algorithm to linear and difference analysis, algebraic attack and some other types of attacks. The shown PRESENT durability is an excellent result for the cipher, created from scratch. At the moment, no successful attack on the full-round version of the algorithm is known.

There are various implementations of PRESENT. The most compact of them requires only 1000GE, which is one of the best results for LW-ciphers.

In addition to ensuring the security of transmitted data in RFID systems, some PRESENT modifications have found application in other resource-dependent devices. For example, H-PRESENT-128 is the most compact of known hash functions. In addition, it is possible to use the algorithm as a pseudo-random number generator for the crypto-GPS scheme.

Also among the LW-ciphers can be identified families of algorithms KATAN and KTANTAN.

Each of the families consists of three ciphers, differing in the number of rounds of encryption: 32, 48 or 64. All ciphers have an 80-bit key. The difference between KTANTAN and KATAN is that the first ones require less resources due to the fact that the encryption key is "stitched" into the device and cannot be changed. In the description of ciphers, developers show resistance to such attacks as difference and linear analysis, attack on related keys and algebraic attack.

Hardware implementations of representatives of KTANTAN show the best results in this area of cryptography. So, for example, the KTANTAN48 algorithm can be implemented using only 588GE, which is almost half that of the most compact implementation of PRESENT [12].

However, despite all the advantages of the block ciphers described above, and for them there are certain threats that do not allow them to be used everywhere. As already mentioned, the DESL algorithm uses a relatively short key, which makes its use in devices, the security of which must be ensured at a high level, impossible.

Algorithms PRESENT and KTANTAN, despite the many studies conducted over the past few years, may carry critical vulnerabilities that will negate all current merits.

There are many more block LW-algorithms. However, they have certain drawbacks. For example, MIBS and TWIS show good results, both in terms of speed and economy, but they have not been sufficiently researched, which, like with flow algorithms, does not allow one to judge with certainty their reliability. Other ciphers, such as HIGHT or mCrypton, require too much space on the chip for hardware implementation.

Thus, summarizing all of the above, we can conclude that the task of creating both a streaming and a block encryption algorithm for passive RFID tags is still relevant and requires a solution

2.3 The DES algorithm

This section provides a more complete description of the DES algorithm.

DES (data encryption standard) is an algorithm for symmetric encryption developed by IBM and approved by the US government in 1977 as the official standard (FIPS 46-3). The block size for DES is 64 bits. The algorithm is based on a Feistel network with 16 cycles (rounds) and a key having a length of 56 bits [13].

The main advantages of the DES algorithm:

• only one 56-bit key is used

• Encrypting a message with one packet, you can use any other package to decrypt it

• Relative simplicity of the algorithm ensures high speed of information processing

• sufficiently high stability of the algorithm

DES encrypts 64-bit data blocks using a 56-bit key. Decryption in DES is an operation of reverse encryption and is performed by repeating the encryption operations in the reverse order.

The encryption process consists of the initial permutation of the bits of the 64-bit block, sixteen encryption cycles, and finally, the reverse bit rearrangement.

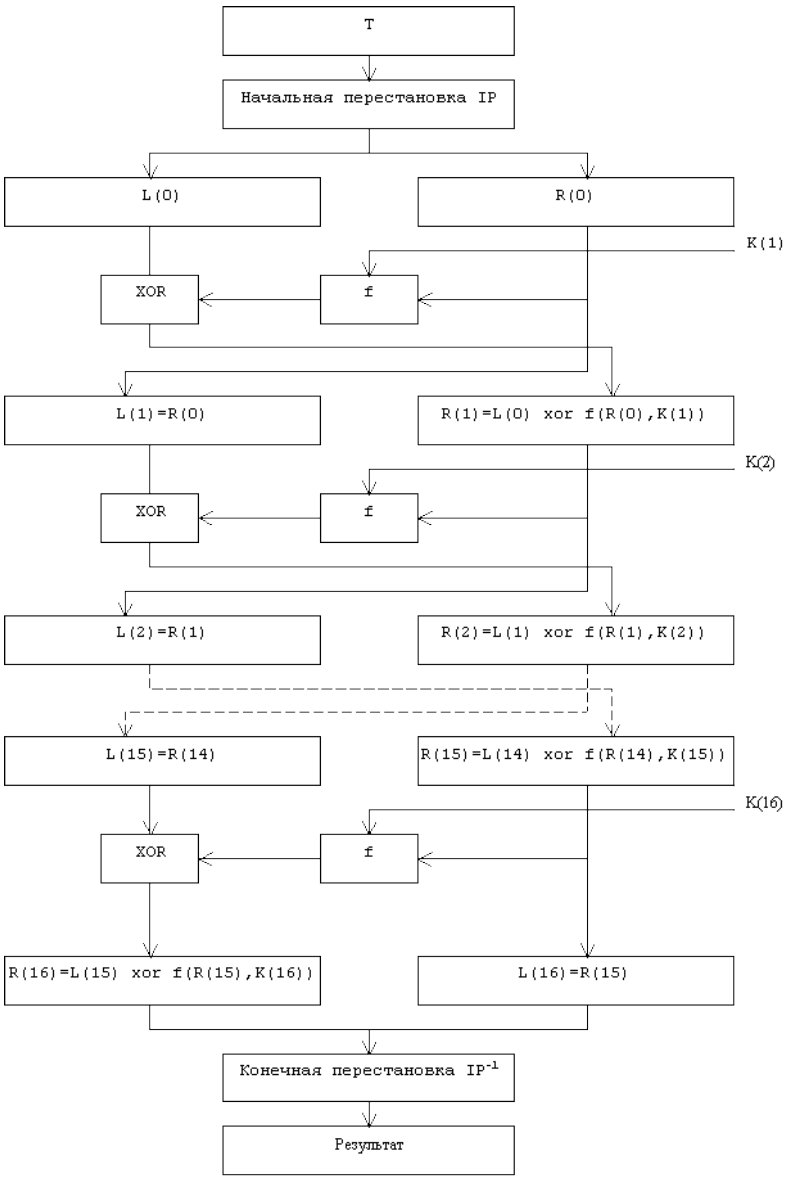


Figure 2. A detailed scheme for encryption of the DES algorithm.

The function fi is called a cyclic function, and the key Ki used to obtain the function fi is called a cyclic key. As you can see, with the cyclic function only the left half is added, and the right half is unchanged. Then both halves change places. This transformation is scrolled several times (several cycles) and the output of the cipher is the pair (l, r) obtained at the end [14].

Map data structure:

Сектор	Блок	Номер байта в блоке																Описание
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
15	3	Ключ А						Биты доступа				Ключ В						Сектор трайлер 15
	2																	Данные
	1																	Данные
	0																	Данные
14	3	Ключ А						Биты доступа				Ключ В						Сектор трайлер 14
	2																	Данные
	1																	Данные
	0																	Данные
(сектора со 2 по 13)																		
1	3	Ключ А						Биты доступа				Ключ В						Сектор трайлер 1
	2																	Данные
	1																	Данные
	0																	Данные
0	3	Ключ А						Биты доступа				Ключ В						Сектор трайлер 0
	2																	Данные
	1																	Данные
	0																	Блок производителя

Figure 3. A detailed scheme for encryption of the DES algorithm.

The entire memory of the card is divided into 16 equal-sized sectors of 64 bytes each. In turn, each sector is divided into 4 blocks, with the last block of each sector containing keys and rules for access to the sector, which allows using the map in 16 different disjoint applications. Due to the fact that each application "knows" only its access keys, other sectors of the map are inaccessible to it. The assignment of keys for each sector determines the access bits, which allows you to separate the rights to read and write to different entities even within the same application. Data blocks can be of two types - standard data blocks and so-called value - blocks that have a fixed format and are intended to use the sector as an "electronic purse". The zeroth sector differs from the others in that it contains only two data blocks. The zero block of the zero sector contains the service information recorded during production - the serial number of the card (4 bytes) and the manufacturer's data. Access to the zero block is always open for reading, while all other blocks require access key knowledge [even for reading] [15].

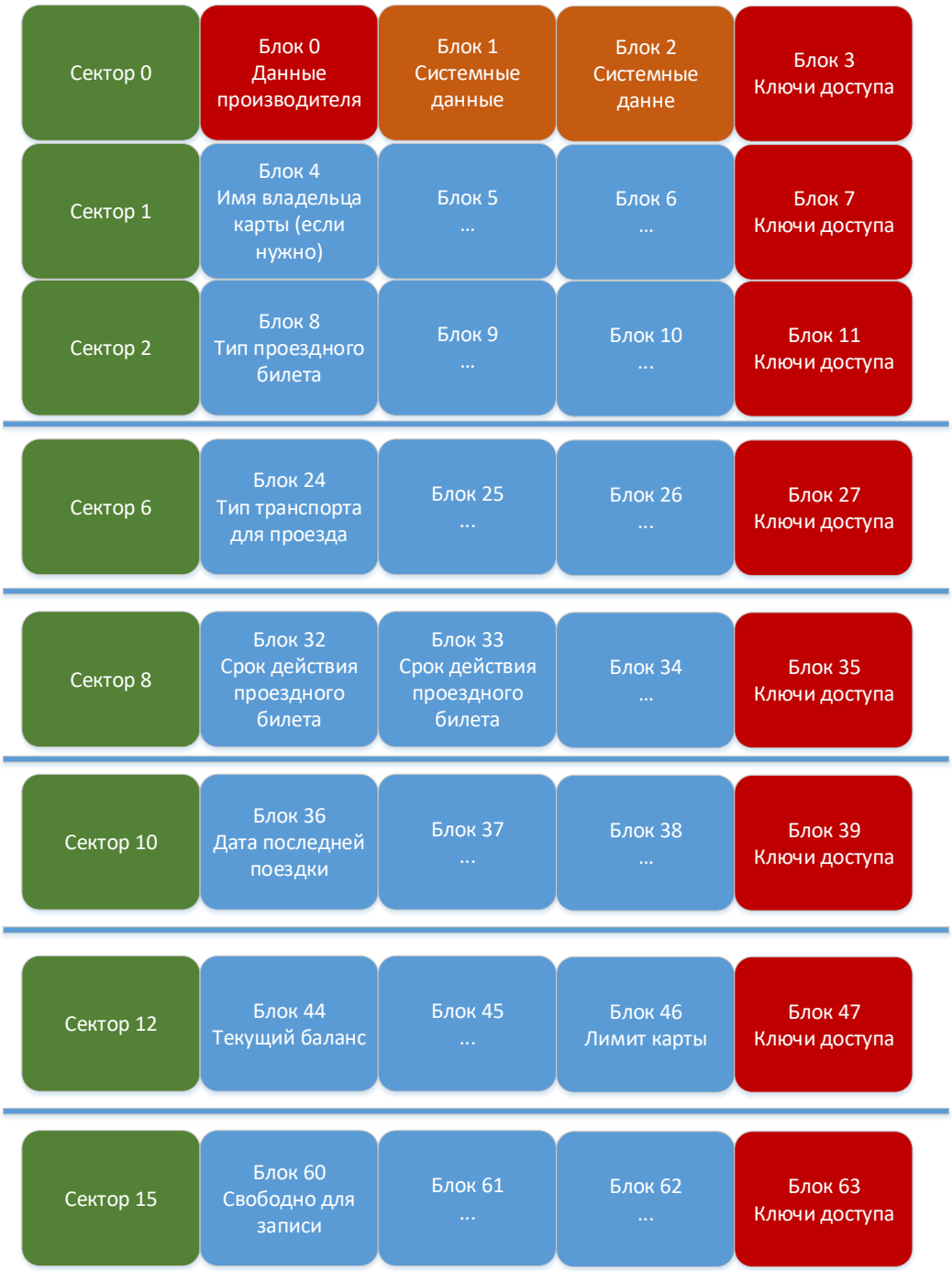


Figure 4. Sectors and memory blocks with information

3 STRUCTURAL SCHEMES OF ALGORITHMS OF WORK OF DEVICES

In this chapter will present the structural diagrams of the algorithms for the operation of the devices of the components that make up the system.

3.1 Block diagram of the algorithm for the control device

Figure 6 is a block diagram of the algorithm for operating a control device with a travel card.

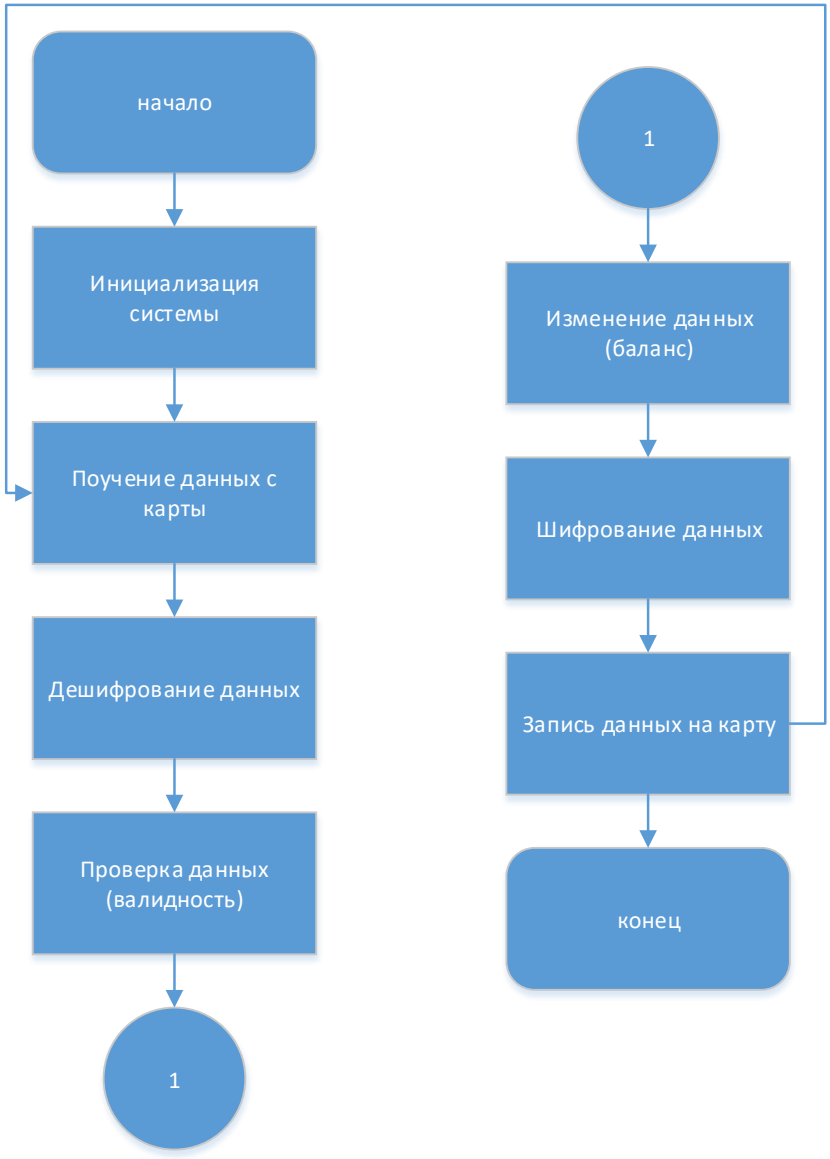


Figure 6. Schematical algorithm of card working

Description of the block diagrams of the algorithm for working with the travel card:

• System initialization - at this stage, all system devices are initialized, data input /output ports are set, communication with the server is established.

• Receiving data from the card - reading data from user cards

• Decrypting data - the information on the card is stored in an encrypted form, its decoding needs to be decrypted.
• Data validation - after decryption, the cards are verified according to the balance sheet and by the service life.

• Data modification - in case of correctness of user card data, it is possible to change them, namely, trip writing.

• Data encryption - for data write back, data information is again encrypted.

• Write data to the card - after all data operations, they are written to the card.

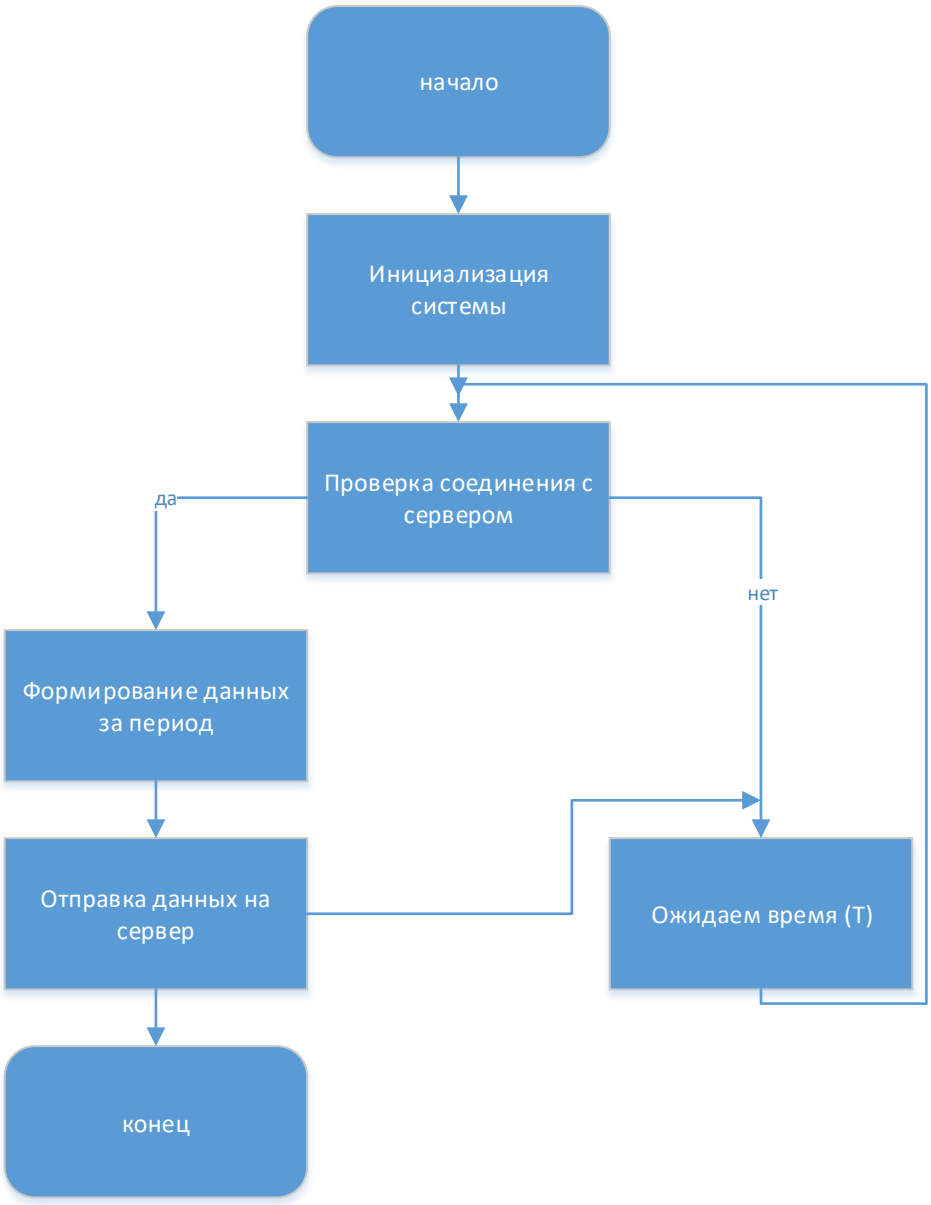


Figure 7. Schematical algorithm of server working

Description of the block diagrams of the algorithm for working with the server:

• System initialization - at this stage, all system devices are initialized, data input / output ports are set, communication with the server is established.

• Check the connection of the control device to the server. If the connection is not established, the device goes into the waiting state until the next data transfer session.

• At the stage of data generation over the period, information collected from the system is generated. Parameters such as the UID of the involved cards are transferred in the

period, the activation time of the map and the coordinates (latitude, longitude) of the interaction of the user card with the system.

• After the data is generated, it is uploaded to the server. From the information received, the general statistics on traffic congestion are compiled.