Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Институт естественных и точных наук
Факультет математики, механики и компьютерных технологий
Кафедра прикладной математики и программирования
Направление подготовки: 09.04.04 Программная инженерия

РАБОТА ПРОВЕРЕНА
Рецензент, генеральный директор
ООО «Трио Плюс»
_____ И.В. Свистунов
«____»_____2019 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой, д.ф.-м.н.,
доцент
_____/А.А. Замышляева
«____»_____ 2019 г.

Разработка системы сбора, обработки и передачи данных «Global Wizard»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ–09.04.04.2019.110.ПЗ ВКР

Консультант, директор по развитию
ООО «Трио Плюс»
_____ А.Н. Витт
«____»_____2019 г.

Руководитель работы, д.ф.-м.н.,
доцент
_____/А.А. Замышляева
«____»_____2019 г.

Автор работы,
студент группы ЕТ-225
_____/С.В. Смольников
«____»_____2019 г.

Нормоконтролер, ассистент
_____/Н.С. Мидоночева
«____»_____2019 г.

Челябинск
2019

АННОТАЦИЯ

Смольников С.В. Разработка системы сбора, обработки и передачи данных «Global Wizard». – Челябинск: ЮУрГУ, ЕТ-225, 59 с., 28 ил., 10 табл., библиогр. список – 21 наим., 2 прил.

В работе представлен процесс разработки системы сбора, обработки и передачи данных энергоресурсов с различных видов объектов, а также организация защиты данных, на различных уровнях передачи, которыми система оперирует.

Целью работы является создание системы сбора, обработки и передачи данных об энергоресурсах.

Перед принятием решения о реализации данной работы были исследованы разработки отечественных и зарубежных организаций в данной области и сделан вывод, что данные системы находятся на начальном уровне своего развития, и не соответствует требованиям автоматизированного контроля и регулирования ресурсов. В ходе разработки была построена структурная и функциональная схема с учетом всех участников системы. Разработаны протоколы обмена между функциональными блоками и написано программное обеспечение для модуля сбора и обработки данных, и модуля передачи. Для взаимодействия с пользователями был реализован web-интерфейс. Перед установкой на объект определены уязвимые места и внедрены современные методы защиты.

Данная система с подобным функционалом единственная на рынке аналогичных изделий и выполняет полный спектр по автоматизации услуг в области энергетики.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время в современном обществе все большее значение приобретает внедрение современных технологий во все области жизни. Только путь модернизации и использования автоматизированного учета потребления энергоресурсов и их рационального использования снижает участие человека на всех этапах, начиная от измерения и заканчивая передачей данных поставщику. С целью измерения, сбора, обработки и передачи данных, потребители и поставщики создают автоматизированные системы для учета и контроля энергоресурсов. При внедрении подобных систем организация сама контролирует свои расходы и может строить выгодные отношения с поставщиками, минимизируя свои затраты.

Большинство людей под давлением различных факторов в поисках пути перехода на новые системы, которые позволят занять лидирующие позиции на рынке, экономить и получать прибыль в сфере энергетики.

В выпускной квалификационной работе рассмотрен процесс разработки системы сбора, обработки и передачи данных энергоресурсов «Global Wizard» с полным контролем со стороны пользователя. Данная система обладает беспроводной передачей и осуществляет полный автоматизированный контроль.

Система создается с целью снижения эксплуатационных затрат за счет оптимального процесса энергоснабжения, а именно:

– сделать процесс использования ресурсов открытым и контролируемым;

– замена устаревшего оборудования;

– обеспечение безопасности функционирования объектов;

– снижение затрат человеческого труда;

– улучшения качества взаимодействия с потребителями.

Для достижения поставленных целей были выделены следующие задачи:

– разработать структуру и определить функционал системы;

– разработать программное обеспечение для элементов непосредственно отвечающих за сбор, хранение и обработку данных;

– создать интерфейс для взаимодействия клиентов с системой;

– исследовать систему на уязвимые места, выбрать и внедрить современные методы обеспечения безопасности;

– провести тестирование блоков и ввести в тестовую эксплуатацию на объект.

В рамках поставленных задач предоставляет:

– централизованный контроль, измерение и передачу технологических параметров (токи, напряжения, мощности, уровни освещенности, режимы и время работы);

– удаленное управление объектами структуры;

– формирование данных для предоставления пользователям и разработчикам системы.

1 БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ УЧЕТА РЕСУРСОВ

Целью данного этапа является исследование текущего состояния выбранной области. Обзор характеристик предмета исследования, обоснование найденных недостатков существующих аналогов. Описание преимуществ, которые может предоставить разрабатываемая система в сравнении с конкурентами.

Внедрение системы «Global Wizard» должно дать возможность организациям и управляющим компаниям выстроить налаженный учет ресурсов, избежать потерь и получить полную картину работы организаций и городов в режиме реального времени.

1.1 Технико-экономическая характеристика предметной области

Россия, как и многие другие страны, располагает гигантским потенциалом в области развития энергосбережения. Наравне с другими энергетическими ресурсами этот параметр не менее важен при обеспечении экономического роста страны.

Из-за отсутствия эффективной государственной политики в сфере энергосбережения, на фоне увеличения спроса на энергоресурсы внутри страны, принятые ранее меры по снижению энергоемкости страны оказались малоэффективны. И хотя страна богата такими ископаемыми как нефть и газ, увеличение объема их добычи и развитие транспортной сети требует больших вложений, да и сами ресурсы не бесконечны.

До недавнего времени развитие энергосбережения и энергоэффективности в стране сдерживали следующие факторы:

– низкая мотивация;

– малая осведомленность в данной области;

– отсутствие опыта финансирования, организации и координации.

Эффективное использование энергоресурсов предполагает тотальный контроль их потребления с помощью современных средств, которые позволяют:

– применять дифференцированный учет по зонам за различные периоды времени;

– автоматизировать контроль и учет любых ресурсов по требованию заказчика.

В конечном итоге внедрение подобных технологий экономит до 70% затрат.

1.2 Системы контроля и регулирования расхода ресурсов

На текущий момент нет четкой правительственной программы по контролю и учету. Большинство потребителей пользуются оборудованием тридцатилетней давности, а данные попадают в компании методом самостоятельного съема показаний. Учитываю ситуацию сложно точно предсказать эффект от внедрения современных технологий, но он точно будет положительным.

Разрабатываемая, в рамках выпускной квалификационной работы, система позволит осуществлять точный сбор затрачиваемых ресурсов, а также контролировать их качество путем обработки полученных данных, передавать с любого объекта вне зависимости от его удаленности на единый сервер. Позволит более рационально использовать электроэнергию в зависимости от времени суток или от текущего уровня освещенности. Предоставит всю необходимую информацию в удобном виде за любой период.

Подобные технологии на рынке предоставляют пара десятков компаний, но наиболее близких к разрабатываемой системе всего несколько, а именно:

– ООО «Технология энергоучета»;

– «Эмис-Электра»;

– АРК «Энергосервис»;

– «Евромобайл».

Все перечисленные выше компании имеют в своем арсенале системы передачи данных и контроля ресурсов с возможностью удаленного просмотра, реализованные разными методами. Но если говорить об оптимальности, функционалу и соотношении «цена-качество», то ни одна из них не подойдет по данному критерию [5]. Ниже представлена сравнительная таблица 1 данных компаний.

Таблица 1 – Сравнительная таблица аналогов

Функционал	Компании				
	Ивелси	ООО «Технологии энергоучета»	«Эмис-Электра»	АРК «Энергосервис»	«Евро-мобайл»
Работа в экстремальных условиях	+	-	-	+	-
Современные методы защиты данных	+	-	+	+	-
Многообразие контролируемых параметров	+	+	+	-	-
Цена-качество	+	-	-	-	-
Развитый функционал	+	-	-	+	-
Возможности web-интерфейса	+	-	-	+	-

Как видно из таблицы ни одна из представленных компаний не может предоставить полный набор функций, которыми должна обладать полностью доработанная система.

У всех компаний есть один большой минус – это соотношение «цена-качество», их технические решения предполагают внедрение устройств передачи данных непосредственно внутрь измерительный устройств, что

сразу сказывается на цене оборудования. Так если бы им пришлось контролировать расходы энергоресурсов крупного города, то для получения первой прибыли пройдет не одна тройка лет, что не выгодно никому. Также недостатком я считаю отсутствие возможности работы в экстремальных погодных условиях, столбики термометров большинства городов России во время зимы опускаются ниже тридцати градусов, а во время обзора комплектующих было выявлено, что у большей части устройств рабочая температура не достигает и минус двадцати.

Не в каждом устройстве были внедрены методы защиты данных требуемого уровня, многие решили ограничиться простым паролем. Измерения данных проводиться только при наличии определенного соответствующего датчика, так если будет запрос на получение данных, для которых измерительное устройство отсутствует, организации необходимо будет его создать, что уже не целесообразно.

Последним выявленным недостатком считается, возможности web-интерфейса, функционал ограничивается таблицей без возможности смены вида и минимальным периодом в один день. Считаем такой функционал неприемлемым для конечного пользователя и никак не помогающим контролировать затраты и расходы.

1.3 Технологии для беспроводной передачи данных

Для реализации системы необходимо провести анализ характеристик существующих технологий передачи данных, которые используются в системах автоматизированного контроля. На сегодняшний день к таким можно отнести: проводные и беспроводные средства.

К проводным технологиям относят самый старый вид построения сети, который уходит в прошлое, и сейчас встречается только в промышленном секторе. «Выделяют два подвида проводной технологии PLC: PLC-I и PLC-II. В качестве коммуникаций при построении системы PLC применяются непосредственно силовые линии электроснабжения. Упрощенно эту

технологию можно представить системой взаимосвязанных между собой электросчетчиков абонентов в рамках многоквартирного дома или коттеджного поселка [6].

Устройства связаны посредством линий 0,4 кВ с концентраторами, расположенными в трансформаторной подстанции (ТП) и передающими диспетчеру информацию о потребляемой электроэнергии через GSM-шлюзы.

Счетчики и концентраторы используют интерфейс RS-485 – международный стандарт, описывающий характеристики дифференциальных линий связи (тип «общая шина»), который позволяет беспрепятственно загрузить необходимую информацию, просто подключив ноутбук» [12].

Беспроводные системы имеют большой выбор технологий, позволяющих передавать информацию без проводов, основными из них считаются:

– GSM/GPRS;

– технологии для «умных домов» ZigBee, Z-Wave, M-Bus;

– LPWAN.

«ZigBee работает в диапазоне частот 2,4 ГГц, но при этом ZigBee не ограничена одним каналом. Z-Wave использует диапазон частот до 1 ГГц, что делает ее более защищенной от помех. Обе технологии оптимизированы для передачи небольших команд включить/выключить, прибавить или снизить яркость освещения и т. п. Технология передачи данных M-Bus тоже считается беспроводной, но с некоторыми оговорками – все приборы учета соединяются шиной m-bus, посредством которой коммутируется оборудование и передаются данные. К несомненным преимуществам всех трех технологий можно отнести умеренные затраты на монтаж и низкое энергопотребление. Однако до сих пор эти технологии продолжают быть применимы, главным образом, для европейского формата» [12].

«LPWAN – технология беспроводной передачи данных с низким потреблением энергии и охватывающая большие площади. LPWAN отличается высоким уровнем проникновения сигнала. По сравнению

с модемами GSM/GPRS, устройства на базе LPWAN продолжают передавать данные даже в условиях подземной прокладки коммуникаций, но обременены в размеры передаваемой информации» [13].

Любые существующие беспроводные технологии передачи данных обладают такими характеристиками как дальность, скорость и энергоэффективность, причем одновременно можно соответствовать лишь 2-м из 3-х [7].

Сравнительная таблица технологий передачи представлена в таблице 2.

Таблица 2 – Сравнение технологий передачи данных

Параметр	Модем	ZigBee	LPWAN
Диапазон, МГц	850/900/1800/1900	2400…2483,5 МГц, 15 каналов с полосой 5 МГц	2,4/868/915/433/169
Скорость передачи, Кбит/с	До 85.6	До 250	Несколько сотен бит
Рабочий диапазон температур, °С	-40 ~ +85	-30 ~ +65	-30 ~ +75
Тип передаваемой информации	Данные	Данные	Данные
Мощность передатчика, мВт	40	63	10
Дальность, км	Зависит от качества сигнала	до 1.8	10–15
Потребление Tx/Rx, мВт	Не более 400, не более 1 Вт	Не более 500, не более 1.4 Вт	Не более 300, не более 800
Цена, руб	От 400	От 3000	От 1500

Также необходимо уточнить, что при выборе данной технологии нужно помнить о законе распределения эффективности систем передачи данных, данный закон графически представлен на рисунке 1.1.

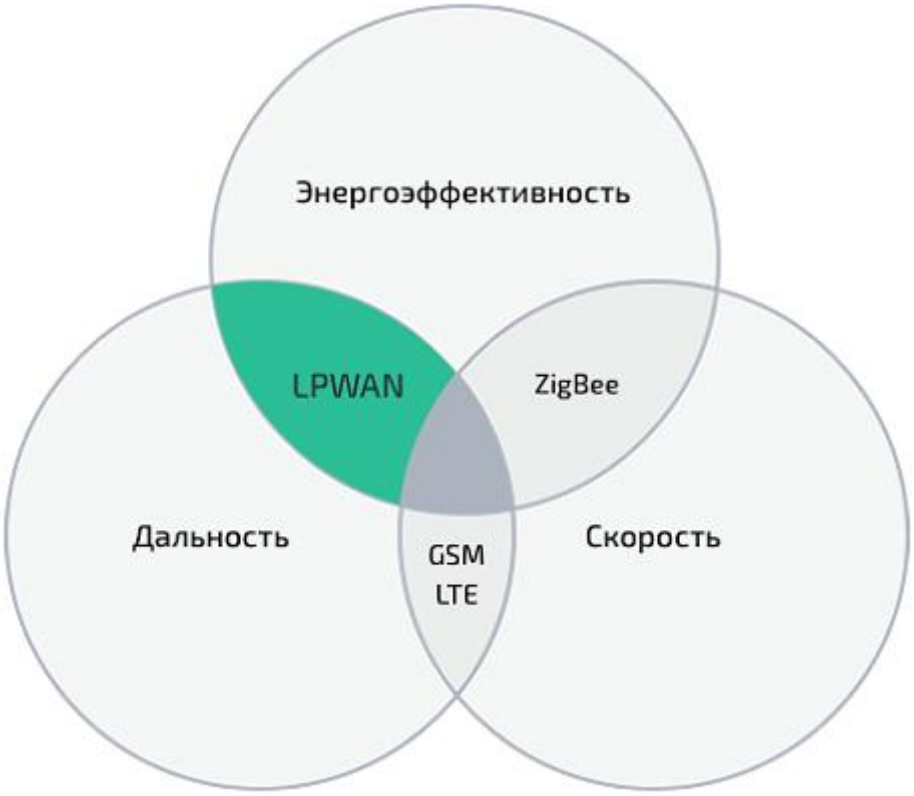

Рисунок 1.1 – Распределение эффективности
систем передачи данных

В конечном итоге, если брать за основу проводные системы, то они будут дешевле аналогов при построении сети, но являются не слишком надежными и могут обернуться дорогим обслуживанием. Наиболее современные беспроводные технологии, такие как LPWAN подойдут только для небольших систем с маленьким объемом передаваемых данных, а это лишает систему возможности развития, что приведет к росту расходов на переоборудование в будущем. Системы на базе GSM/GPRS с учетом грамотно построенной структуры и определенными функциями позволят сократить затраты и повысить надежность, а скорость передачи данных позволит передавать большое количество данных с запасом, что в будущем позволит расширить и модернизировать систему без перехода на более дорогие технологии [8].

1.4 Выводы по разделу

Исходя из проведенного анализа подобных систем, становится очевидна необходимость создания системы контроля и регулирования расходов энергоресурсов, так как не один из аналогов не обладает достаточным функционалом и возможностями. Существующие технологии передачи данных, рассмотренные в разделе, и оборудование позволяют разработать наиболее законченную систему, удовлетворяющую потребности самого привередливого пользователя.

Для написания программного обеспечения оборудования для системы «Global Wizard » был выбран язык программирования C++, а среда Atmel Studio, наиболее подходящая для работы с микроконтроллерами. Интерфейс будет реализован в среде NetBeans на языке Java при помощи фреймворка Vaadin.

2 ПРОЕКТИРОВАНИЕ СИСТЕМЫ «GLOBAL WIZARD»

2.1 Разработка структуры системы

Первоначальным этапом разработки системы является выявление её структурных частей и определение управляющих взаимосвязей между ними, что позволит в дальнейшем перейти к определению функционала [11].

В ходе работы были выявлены следующие структурные элементы:

– контроллер;

– базы PLC;

– модем;

– счетчики и датчики;

– светильники, включающие в себя:

а) PLC-приемник;

б) LED-драйвер;

в) светодиодную плату;

– преобразователь интерфейса PRC100;

– панель управления;

– сервер;

– любое устройство с доступом в интернет.

Структурная схема системы представлена на рисунке 2.1. На данном рисунке можно увидеть, как связаны между собой все структурные элементы, напряжение питающей сети, соединения. В зависимости от используемого оборудования можно составлять различные конфигурации для внедрения в разные объекты, которые будут актуальны для заказчика. Можно заметить, что связь с системой поддерживается с помощью разнообразных устройств, у которых в наличии есть возможность выхода интернет.

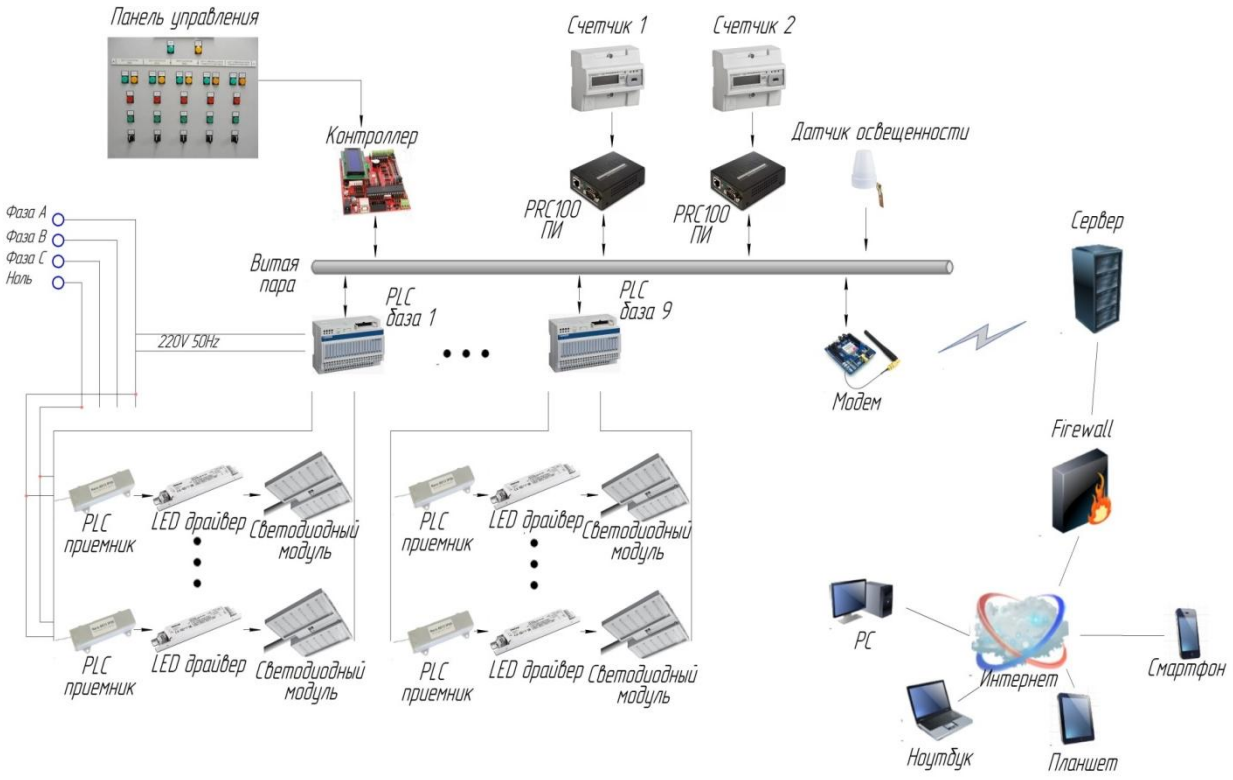

Рисунок 2.1 – Структурная схема системы

2.2 Разработка функциональной схемы

Функциональная схема определяет функциональные связи между структурными единицами и демонстрирует оснащенность объекта средствами автоматизации: измерительными приборами, преобразователями и механизмами. Также схема определяет взаимодействие элементов контуров управления и направление передачи управляющих сигналов [11].

После полного изучения объекта, определения функций, изучения статических и динамических характеристик, параметров контроля и управления, разработана функциональная схема, представленная на рисунке 2.2, имеющая следующие функциональные блоки:

– блок измерительных устройств;

– блок исполнительных устройств;

– блок ручного управления;

– блок сбора и обработки данных на нижнем уровне;

– блок передачи данных;

– блок обработки данных на верхнем уровне;

– блок клиентов.

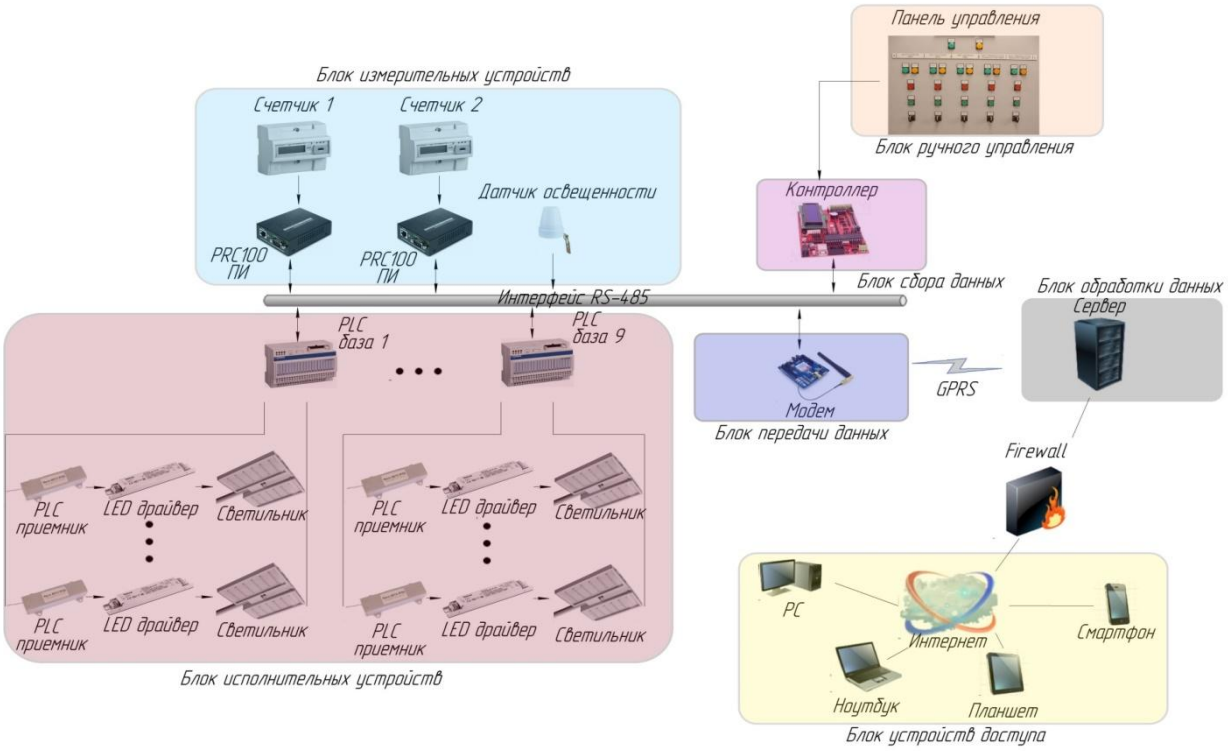

Рисунок 2.2 – Функциональная схема системы

2.3 Разработка протоколов обмена

После определения функциональных частей системы необходимо подумать о налаживании связи между ними для этого используются протоколы передачи данных различных уровней. Протоколы передачи данных – это наборы соглашений или же стандарты, которые задают то, как будет происходить обмен данными между устройствами. Главный смысл протокола – это упорядочить передачу и сделать независимой от используемого оборудования. Нельзя путать протокол с интерфейсом и приравнивать к физическому уровню, т. к. он является логическим уровнем.

Наиболее распространенным и простым промышленным протоколом является Modbus. Также используются Ethernet, CAN, HART, PROFIBUS, они необходимы для связи нижнего и верхнего уровней автоматизированных систем. Но так как описание всех этих протоколов находится в свободном

доступе, что снижает безопасность данных и любой сможет извлечь посылку и обработать полученную информацию, было принято разработать свой собственный протокол обмена для интерфейса RS-485.

Разработанный протокол работает по принципу один master(ведущий) и множество slave(ведомый). Передачу может инициировать только ведущий, ведомый только отвечает на запросы. Скорость передачи варьируется от 1200 бит/с до 921600 бит/с.

Формат запроса в общем виде представлен в таблице 3.

Таблица 3 – Формат запроса

Адрес объекта	Номер функции	Параметры	CRC8

Формат ответа в общем виде представлен в таблице 4.

Таблица 4 – Формат ответа

Адрес объекта	Номер функции/ошибка	Ответ	CRC8

Были разработаны уникальные коды функций, которые определяли длину посылки, неверная передача повлечет за собой ошибки чтения.

На данный момент существует четыре кода, которые выполняют требуемые функции:

– запрос типа объекта;

– запрос значения параметров;

– синхронизация времени;

– установка значения параметра.

При выявлении ошибочных запросов подготовлены специальные функции, информирующие об ошибке.

Разработанный протокол применяется для обмена данными между блоком сбора и обработки данных на нижнем уровне с блоками исполнительных и измерительных устройств, и блоком передачи данных.

Блок передачи данных общается с блоком обработки данных на верхнем уровне с помощью AT-команд.

AT-команды – это специальные команды языка AT, разработанные компанией Hayes в 1970-е годы. Практически каждый модем знает эти

команды и содержит много своих собственных основанных на тех же принципах. Для того чтобы модем понял эти команды, они записываются в специальной форме, в определенных последовательностях с заданными задержками.

Командами настраивается соединение, формируется посылка и передается на сервер. Также AT-командами настраиваются и другие внутренние параметры работы блока передачи данных [14].

Обмен данными между клиентами и сервером происходит по принципам технологии JSON Web Token.

2.4 Выводы по разделу

В результате проделанной работы в проектной части была разработана структурная и функциональная схема, которые дают общее представление о работе системы в целом и объясняют ее функционал.

Также для всех выявленных функциональных блоков были определены интерфейсы и разработаны уникальные протоколы обмена данными, которые позволяют выполнять функции запроса, передачи и установки значений. Все эти команды позволяют обеспечить полный набор функции для создания эффективной экосистемы общения оборудования.

3 РЕАЛИЗАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ «GLOBAL WIZARD»

Программное обеспечение разрабатывалось для двух функциональных блоков, а именно: для блока сбора и обработки данных на нижнем уровне и блока передачи.

Языком программирования был выбран C++, среда программирования Atmel Studio 7.

Закономерный вопрос: почему был выбран не язык Си или ассемблер?

C++ декларирует поддержку различных устоявшихся парадигм программирования – процедурное, объектно-ориентированное, обобщенное, что очень сильно расширяет возможности программы и дает много преимуществ, также для некоторых моментов был использован язык Си, так как он специализирован под низкоуровневое программирование. Единственная возможная проблема – это ограниченная память небольших микроконтроллеров, но для нашей системы это проблемой не является, памяти в выбранных нами контроллерах достаточно, даже для реализации улучшений, и есть поле для экспериментов.

Выбранная среда программирования была выпущена разработчиками AVR и ARM контроллеров Atmel и поддерживает все свои контроллеры, а также предоставляет все необходимые инструменты и библиотеки на языках C/C++ и идеально подходит под наши нужды.

3.1 Функциональность программного обеспечения

В конечном итоге блок сбора и обработки данных на нижнем уровне выполняет следующие функции:

– сбор данных с датчиком (CO_2, температура, освещенность);

– сбор данных со счетчиков (мощность, напряжение, ток);

– отправка управляющих воздействий на исполнительные устройства (светильники, реле);

– обработка полученных данных в вид для отправки блоку передачи.

А блок передачи данных:

– преобразует полученные данные в вид (URL + № передатчика + пароль + данные);

– настройка параметры для передачи (установка GPRS связи, получений IP адреса, связь с оператором);

– отправка посылки на сервер;

– прием команд управления с сервера;

– передача команды управления контроллеру.

Так как разработанное программное обеспечение является собственностью фирмы, т. е. конфиденциально, нет возможности предоставить листинг программы, справка о конфиденциальности находится в ПРИЛОЖЕНИИ 1.

3.2 Выводы по разделу

Было разработано программное обеспечение для основы системы. Блок сбора, обработки, управляемый контроллером, обрабатывает любые данные, поучаемые с подключенных к линии связи устройств, раздает управляющие команды исполнительным механизмам и оформляет данные в удобные посылки, формируемые по протоколу. Блок передачи под управлением модема после получения посылки превращает ее в пакет для сервера, предварительно шифруя, а также передает команды управления с сервера контроллеру, предоставляя удаленное администрирование. Таким образом, определенные на этапе проектирования части объединились в единую сеть.

4 ОРГАНИЗАЦИЯ БАЗЫ ДАННЫХ СЕРВЕРА И РАЗРАБОТКА WEB-ИНТЕРФЕЙСА

Тщательное проектирование базы данных очень важный этап при создании идеально работающего приложения. При создании базы данных необходимо придерживаться определенных правил проектирования, чтобы обеспечить целостность и простоту обслуживания.

Базы данных создаются для хранения информации и получения при необходимости.

4.1 Разработка базы данных

Для разработки была выбрана реляционная база данных – MySQL. Отличительная особенность реляционных систем – возможность располагать данные не в одной таблице. Данные, которые связаны, объединяются по одному общему ключу [15].

Далее необходимо подумать о нормализации, т. е. о взаимоотношении и организации данных, типах связи, резервных копиях и восстановлении.

Спроектированная база данных представляет собой последовательность взаимодействия пользователя с web-интерфейсом системы от аутентификации и до мониторинга параметров.

Также необходимо обозначить связи между таблицами, прежде всего это для разработчиков, чтобы поддерживать целостность базы данных. Правильно настроенные связи дают уверенность в том, что ничего не потеряется.

С учетом всех описанных выше принципов, после выделения ключевых полей и элементов для взаимодействия пользователя с сервером, была разработана база данных системы «Global Wizard», ее структура представлена на рисунке 4.1.

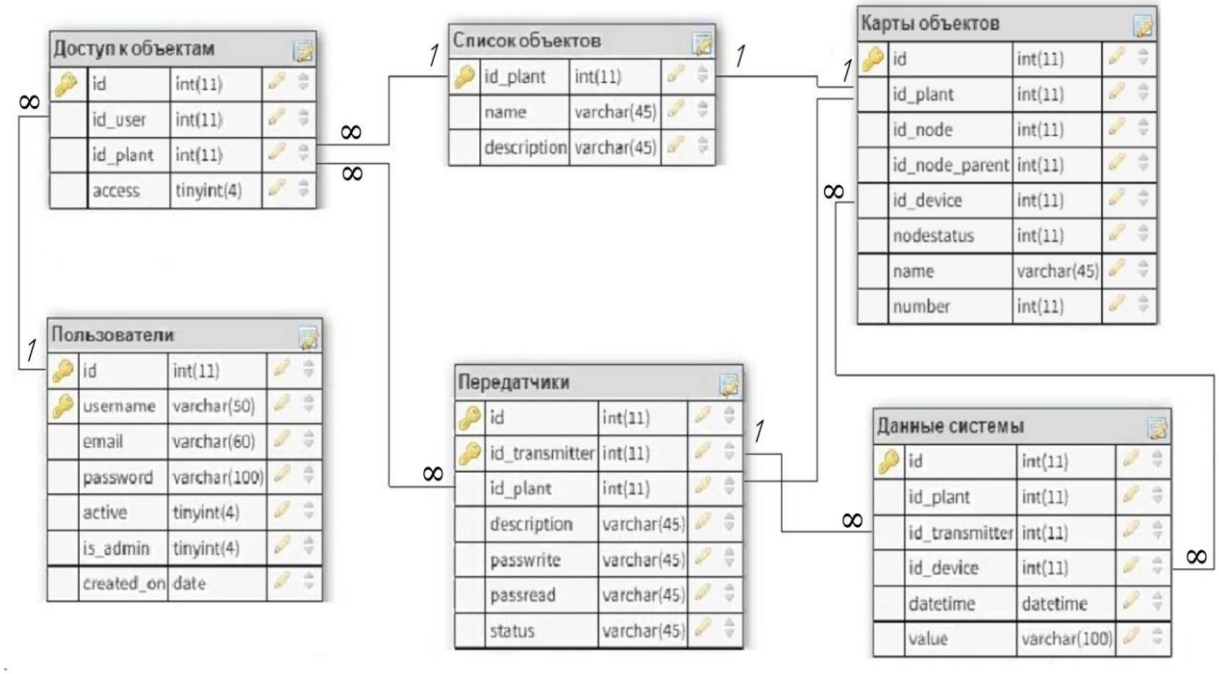

Рисунок 4.1 – Структура базы данных

Для понимания того, как пользователь взаимодействует с приложением, была разработана структура хранения объектов, представленная на рисунке 4.2. По ней пошагово можно отследить то, как получить доступ к любому интересующему нас объекту.

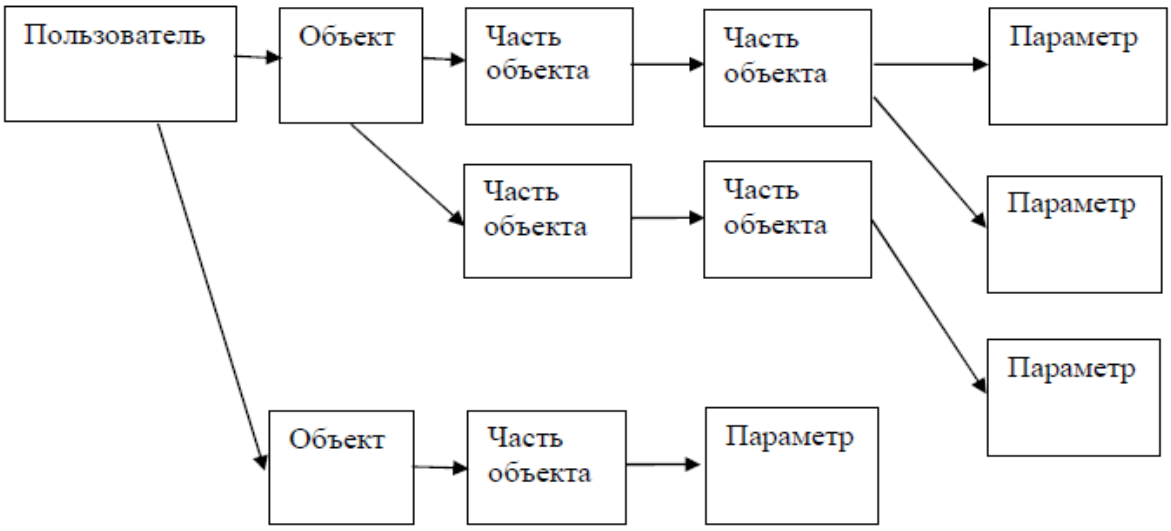

Рисунок 4.2 – Структура хранения объектов

Большая часть существующих организаций и практически каждый пользователь сети интернет имеет свой web-сайт для того, чтобы иметь

возможность предоставить информацию о себе, своих разработках, продуктах и иметь возможность наладить тесный контакт с потребителем путем взаимодействия через интернет.

Чтобы пользователи нашей системы не беспокоились о сохранности и расходах своих ресурсов, о технологическом обслуживании оборудования. Чтобы каждый потребитель мог сам следить за тем, как современные методы автоматизации, экономят его время и деньги, было принято разработать удобный, а самое главное информативный web-интерфейс системы.

После того как данные были направлены на сервер их надо отформатировать, рассортировать по категориям, представить в приятном для пользователя виде.

4.2 Разработка web-интерфейса

Для разработки web-интерфейса был выбран язык программирования Java, а среда программирования NetBeans.

Язык Java является одним из самых популярных объектно-ориентированных языков. Его главное особенность независимость от платформы и схожесть с языком C++, но при этом он лишен его недостатков.

Средой разработки был выбран NetBeans не просто так, во-первых, она является бесплатной, а во-вторых, имеет все необходимые, а именно:

– полностью настраиваемая рабочая область;

– расширенный многоязыковой редактор;

– проверка синтаксиса;

– генератор стандартных фрагментов;

– визуальный редактор – Swing GUI Builder для разработки профессиональных приложений на Java;

– поддержка Java EE 6 для разработки сервлетов, веб-страниц, веб-сервисов и пр.;

– расширение функциональности с помощью подключаемых модулей и др. не менее полезные функции.

Так как сама Java не предлагает подходящих средств для создания web-интерфейса, был выбран фреймворк Vaadin, который поддерживает все современные браузеры [15]. Разработка ведется непосредственно на Java, который выполняется на сервере, а клиенту будет доступен чистый JavaScript. Он идеально подходит для создания приложений, где есть большой функционал, который постоянно дорабатывается и меняется.

В конечном итоге с использованием всех приведенных выше средств был разработан web-интерфейс для взаимодействия с клиентами, показанный ниже.

Первое, что пользователь увидит при обращении к ресурсу это окно аутентификации, изображенное на рисунке 4.3, каждому абоненту будет выдан его личный логин и пароль для получения доступа. Т. о. обеспечивается разграничение доступа, что способствует безопасности системы.

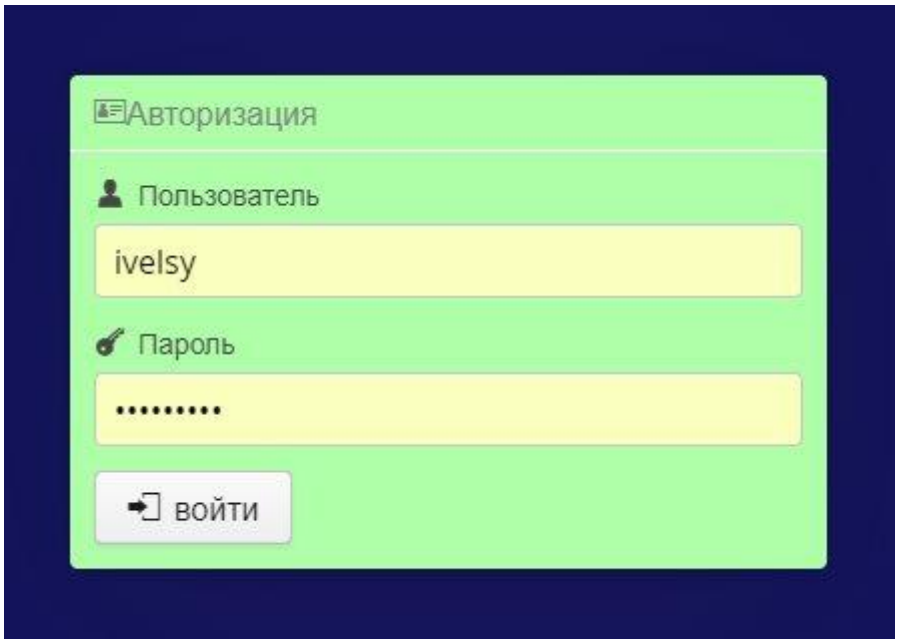

Рисунок 4.3 – Окно аутентификации пользователя

После входа в систему мы попадаем в главное окно, представленное на рисунке 4.4, на нем каждый пользователь будет видеть объект, которые доступны только ему.

Так как мы вошли под логином разработчика, нам для обзора доступны все объекты, подключенные к системе. Разработчик или администратор

может выбрать любую организацию и провести все манипуляции, что и пользователь, но помимо этого он может просмотреть уведомления об ошибках и провести наладку в разделе настроек, от клиента данные разделы скрыты.

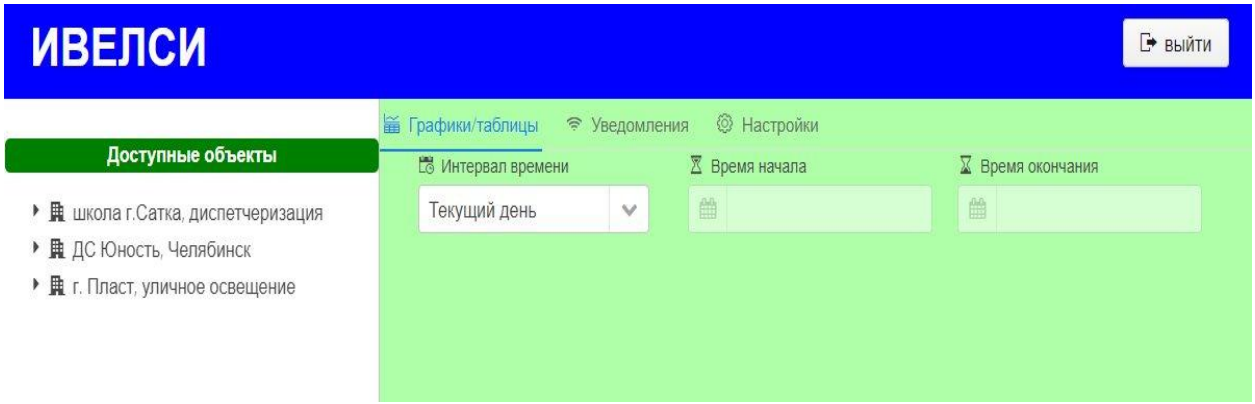

Рисунок 4.4 – Основной экран

После нажатия на объект раскрывается дерево подчиненных пунктов, изображенное на рисунке 4.5, и в каждом можно выбрать для отслеживания параметры, которые в данный момент контролируются в указанном месте. К примеру, если абонент подключил систему в школе, подчиненными объектами будут классы, в каждом классе может быть по несколько кабинетов, а в них установлены следующие датчики для сбора данных:

– контроля температуры;

– освещенности;

– уровня CO_2.

Для сбора этих данных на всю школу достаточно установить лишь один шкаф управления с разработанной системой.

Любой из параметров, заданный в системе, или указанный к добавлению по требованию заказчика в дальнейшем можно выбрать и отследить, без какой-либо посторонней помощи и вмешательства.

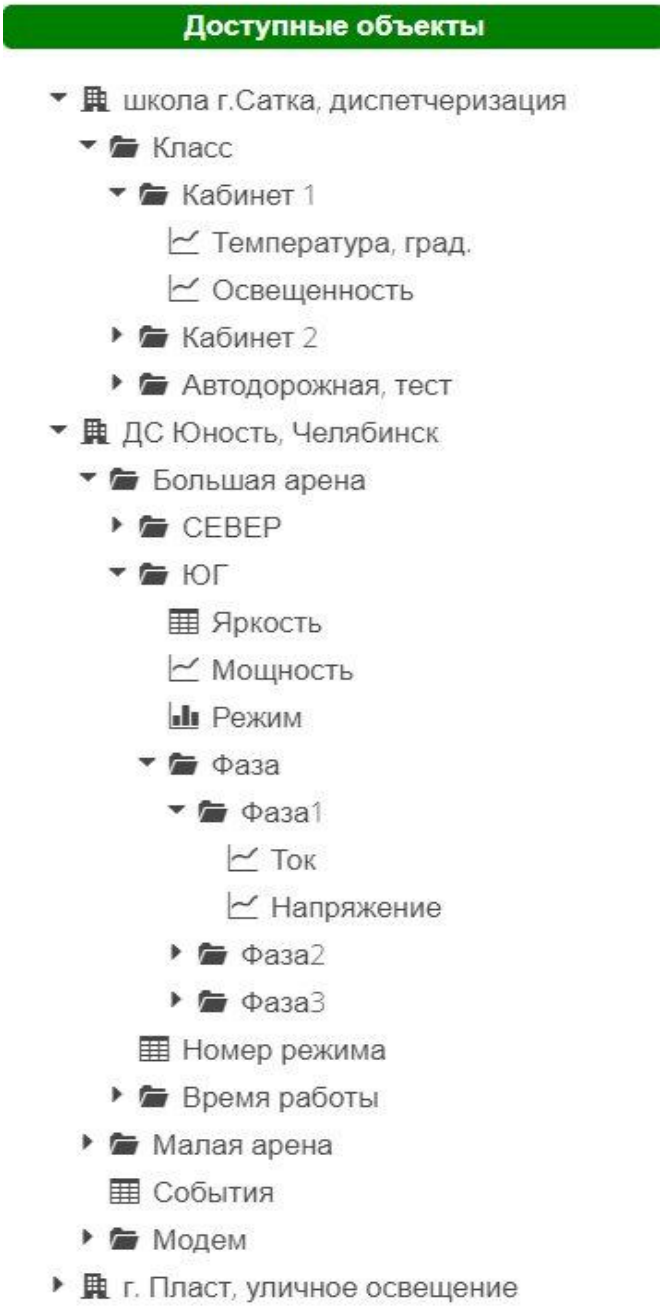

Рисунок 4.5 – Структура объекта

При выборе какого-либо контролируемого параметра в свободной области справа открываются данные в наиболее удобном виде для представления. К примеру, на объекте дворец спорта «Юность», при отслеживании уровня яркости освещения в различных режимах, открывается таблица с данными, изображенная на рисунке 4.6, собираемыми раз в час.

В таблице отображается дата сбора данных, номер режима, в котором система работала во время снятия показаний, а также уровень яркости в тот момент.

Мы можем задать в строке параметра номер режима, чтобы узнать, какая освещенность была именно при работе в этом пункте, а также условие – значение освещенности, больше, меньше или равное, или требуемое значение в поле значение и отследить есть какие-либо нарушения в работе системы.

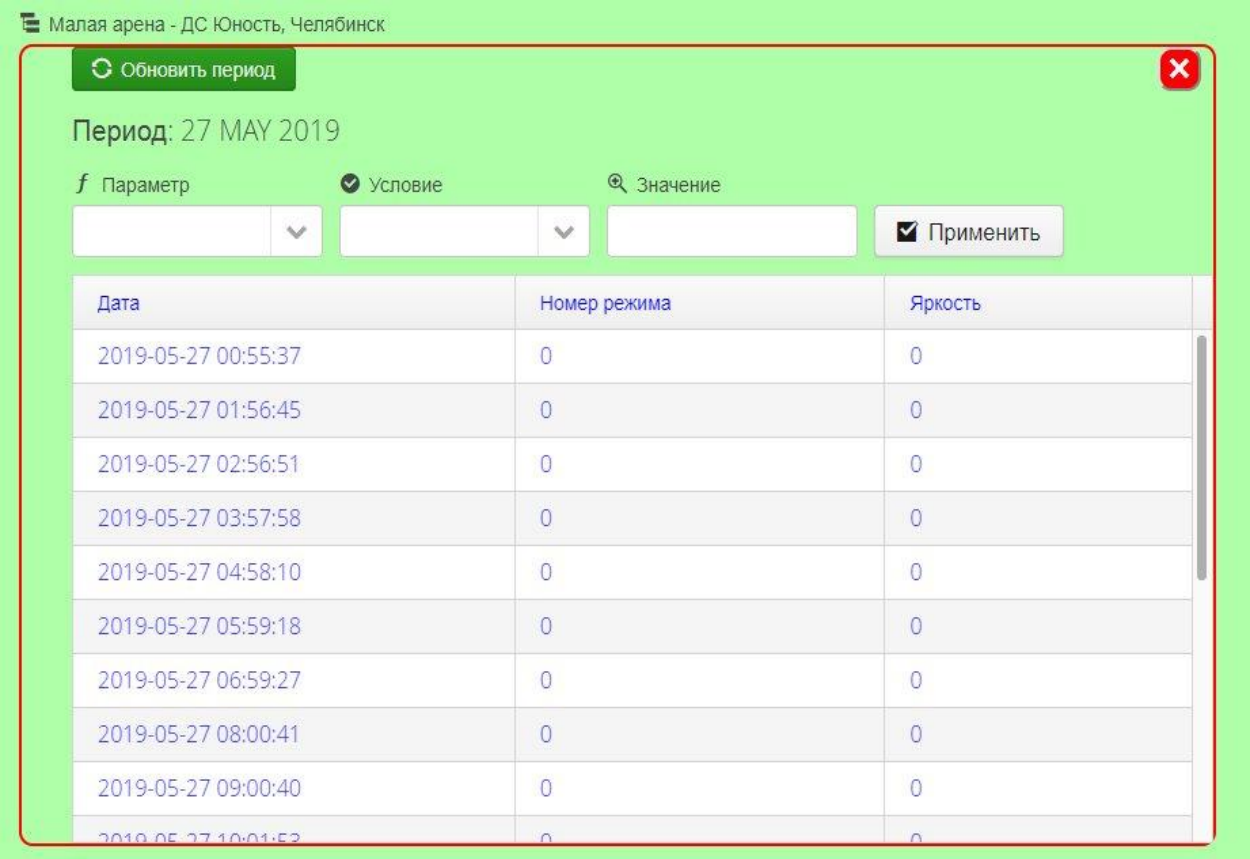

Рисунок 4.6 – Отслеживание параметров в таблице

При выборе другого параметра, например температуры, нам открывается окно с графиком изменения данного параметра, изображенное на рисунке 4.7, также мы можем увидеть текущее значение и выбрать период для мониторинга.

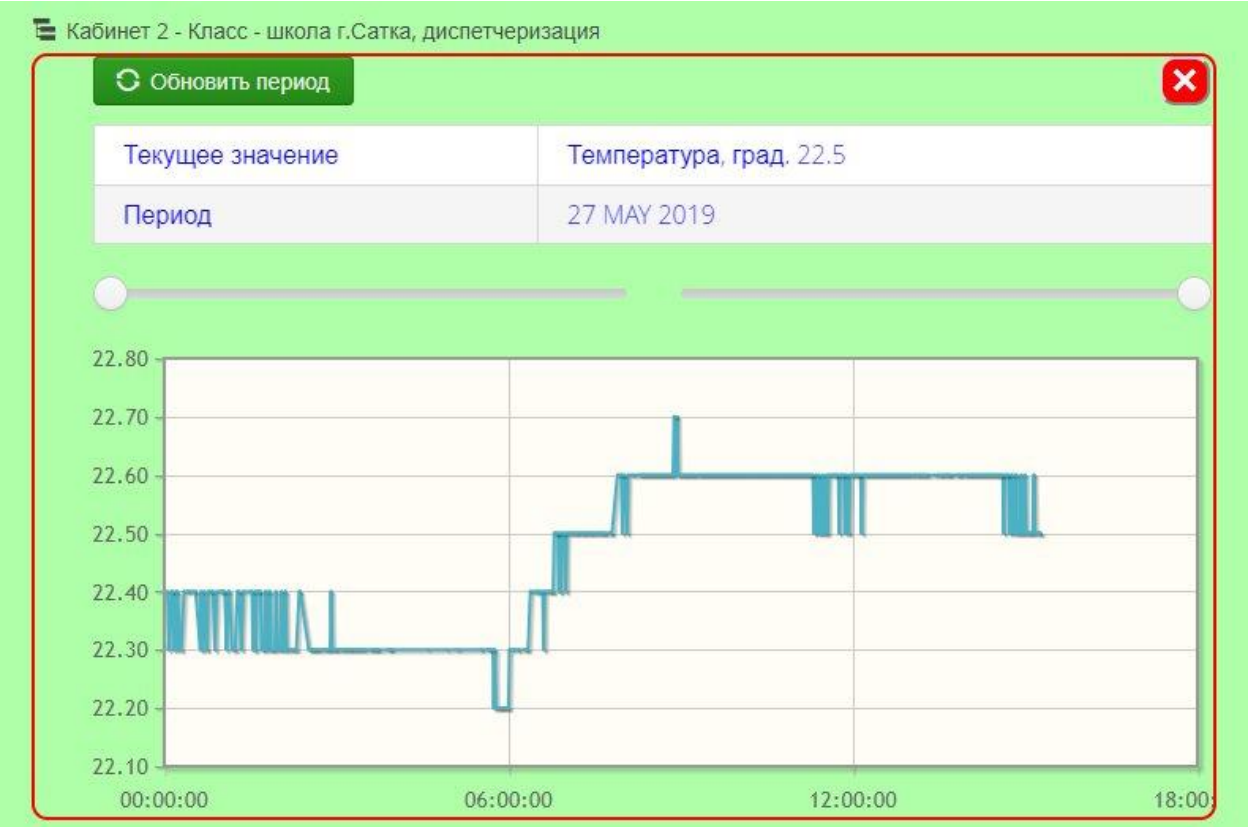

Рисунок 4.7 – График отслеживания изменений температуры

По такому же принципу при выборе отслеживания затрат мощности высвечивается график, представленный на рисунке 4.8. На этом графике можно не только посмотреть изменение затраченных ресурсов, но и отследить время работы в различных режимах освещения, а также, сколько мощности потребляет при работе в данном режиме система и за какое время.

Обзором только этих параметров система не ограничивается, пользователь может запросить графики затрат тока на линии, изменение уровней напряжения питания.

Отследить какой режим работы оказался наиболее полезным и продуктивным. Проверить с помощью карты, где установлено оборудование, какие участки оно контролирует, это будет очень полезным при возникновении неполадок на объекте, не придется тратить время на поиск места поломки и устранение неисправностей.

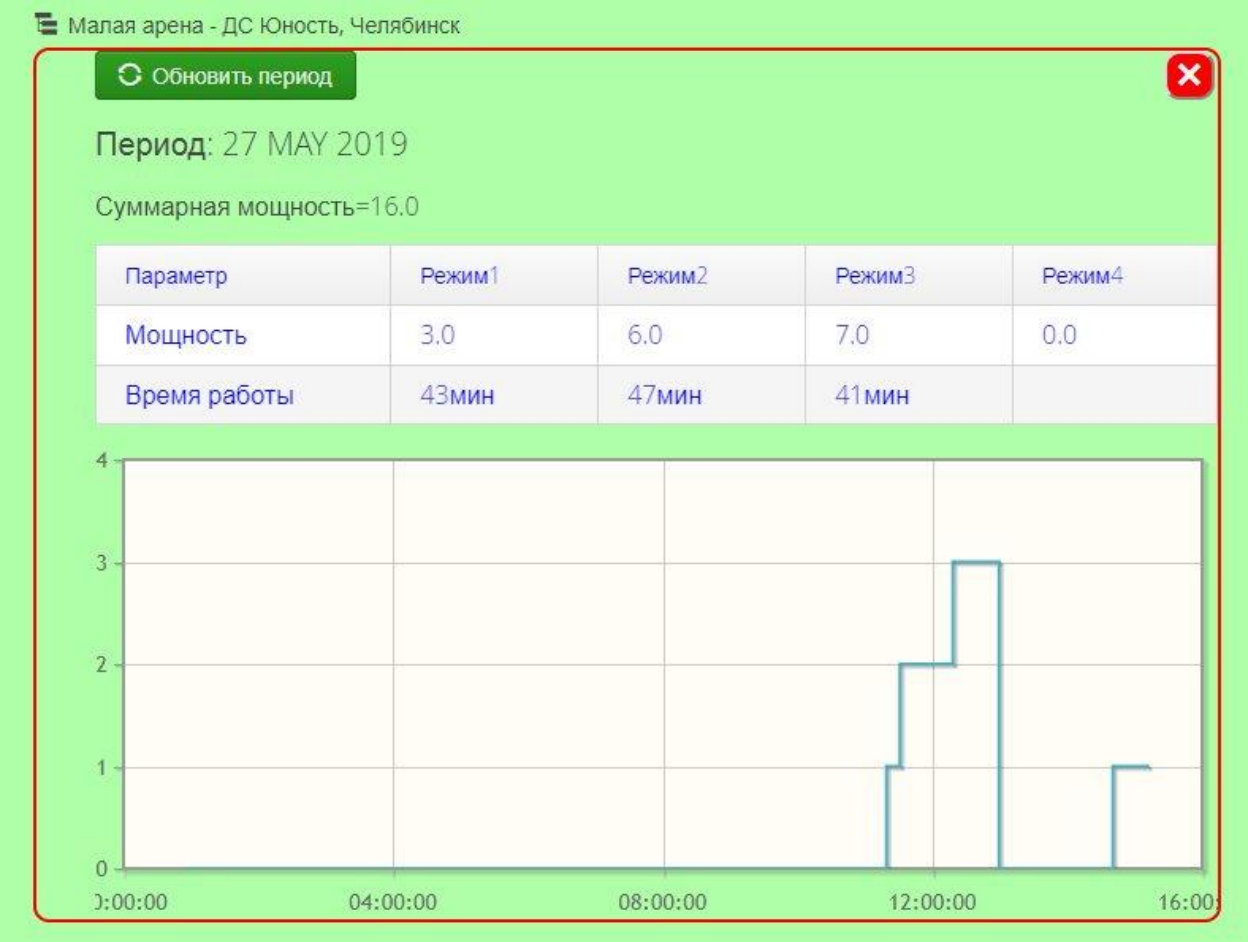

Рисунок 4.8 – Таблица и график по затратам мощности

Также в системе предусмотрен режим работы для разработчиков или администратора. Данный режим предусматривает мониторинг работы самих устройств, выявление причин неполадок, а также настройки системы. При входе в систему администратор видит все объекты, а также в каждом появляются дополнительные пункты, представленные на рисунке 4.9. Первый пункт – это события, которые были заранее разработаны с учетом устанавливаемого оборудования и позволяют понять, что не работает в системе или выявить неправильную эксплуатацию. Этот раздел будет доступен и потребителю для устранения неисправностей. Предусмотрены следующие варианты событий:

– не отвечает PLC база;

– падение амплитуды ниже критического значения;

– не отвечает счетчик;

– неверный запрос;

– превышение значения тока;

– снижение значения тока;

– превышение значения напряжения;

– снижение значения напряжения.

Второй пункт – модем, позволяет наблюдать за качеством сигнала, напряжением питания, качеством передачи, числом перезапусков устройства и временем работы. Также будет предусмотрен вариант удаленного управления с целью улучшения качества обслуживания, это позволит при возникновении неисправностей, переключаться на другие режимы работы и сохранять работоспособность системы.

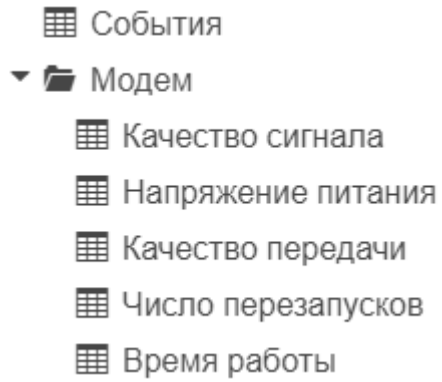

Рисунок 4.9 – Объекты контроля администратора

4.3 Выводы по разделу

В описанном выше разделе разработана база данных системы для приведения всей информации в упорядоченный вид и отражения структуры взаимодействия клиента с данными.

Разработан web-интерфейс, позволяющий пользователю выполнять полный спектр функций по контролю и регулированию затраченных ресурсов.

5 ОПРЕДЕЛЕНИЕ КОНЦЕПЦИИ И ВНЕДРЕНИЕ СОВРЕМЕННОЙ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ

Самый важный этап всей разработки – это выявление уязвимостей и внедрение современных средств защиты для предотвращения угроз.

Существует ряд важный особенностей перед постановкой задачи защиты информации [10]:

– в связи с увеличением числа угроз и мошенников, внедрение комплексной системы защиты становится более актуальным;

– защита информации требуется не только государственным организациям, но и небольшим негосударственным предприятиям;

– сильно растет разнообразие информации, которую необходимо защищать.

Мероприятия по защите информации проводятся повсеместно специалистами различного уровня, но успех подобных действий зависит не только от людей, но и от хороших методов и средств решения задач. Чтобы защита системы действительно была комплексной нужно знать принципы, методы и подходы построения оптимальных защитных процессов и уметь управлять ими в ходе их функционирования [10].

При построении комплексной системы защиты требуется придерживаться следующих принципов [20]:

– принцип законности, а именно соответствие тех мер защиты, которые будут применены, текущему действующему законодательству;

– принцип полноты защищаемой информации, защите должна подвергаться любая информация, утрата который может нанести какой-либо вред ее владельцу, таким образом поддерживается сохранность интеллектуальной собственности;

– принцип обоснованности защиты информации, это соответствие методов защиты информации их целесообразности в данной ситуации;

– принцип участия, любое лицо которое имеет доступ к какой-либо конфиденциальной информации, несет ответственность за ее сохранность;

– принцип персональной ответственности, информация доверенная человеку лично, должна быть им защищена любыми средствами;

– принцип наличия и использования всех необходимых сил и средств для защиты, использование специального персонала, организационных мероприятий и материально-технических ресурсов обязательно требуется для комплексной защиты данных;

– принцип превентивности принимаемых мер, система создается с учетом заблаговременного предупреждения возможных угроз.

Чтобы создать действительно комплексную систему защиты необходимо использовать совокупность всех описанных принципов.

Перед внедрением средств защиты необходимо определить уязвимые в системе места, определиться с иерархией и выделить приоритетные уровни, также нужно обосновать выбор тех или иных технологий, а именно от каких угроз и неполадок они будут защищать данные.

Для разрабатываемой автоматизированной системы были выделены три условных уровня безопасности:

– начальный, который обеспечивает безопасность данных при обмене в RS-485;

– достаточный для защиты при передаче модем-сервер;

– высокий уровень, предоставляет защиту информации на стороне сервера и клиента.

5.1 Защита обмена в интерфейсе RS-485

Беспроводные сети становятся все более популярными с каждым годом, но, несмотря на это в жестких условиях эксплуатации на промышленном производстве наиболее устойчивую связь до сих пор обеспечивает интерфейс RS-485.

Данный стандарт обеспечивает обмен на высокой скорости и на достаточно большие расстояния по одной линии. Сейчас распространено

несколько типов интерфейсов, каждый из которых разработан для конкретных ситуаций, к их числу относят:

– CAN;

– RS-232;

– RS-485/RS-422;

– I^2C;

– I^2S;

– LIN;

– SPI;

– SMBus..

В отличие от RS-422, RS-485 более гибкий, т. к. может использовать несколько master на одной шине и до тридцати двух подключенных устройств.

Стандарт TIA/EIA-485 позволяет достичь дальности до 1200 метров и скорости передачи до 40 Мбит/с. Все это достигается благодаря дифференциальному сигналу. Зависимость скорости обмена от длины линии связи представлена в таблице 5.

Таблица 5 – Зависимость скорости обмена от длины линии

Скорость обмена, бит/с	Длина линии, м
38400	1200
57600	1000
76800	750
115200	500
230400	250
460800	125
921600	62

Интерфейс можно использовать в двух режимах:

– полудуплексный (одна витая пара);

– дуплексный, одновременная передача и прием (две витые пары).

В интерфейсе RS-485 имеется возможность создавать сети, состоящие из различных устройств, подключенных к одному последовательному порту, пример такой сети изображен на рисунке 5.1.

Но, несмотря на большое количество преимуществ, у интерфейса есть ни недостатки [17]:

– сильное влияние электромагнитных помех;

– переходные процессы в сетях;

– разности потенциалов.

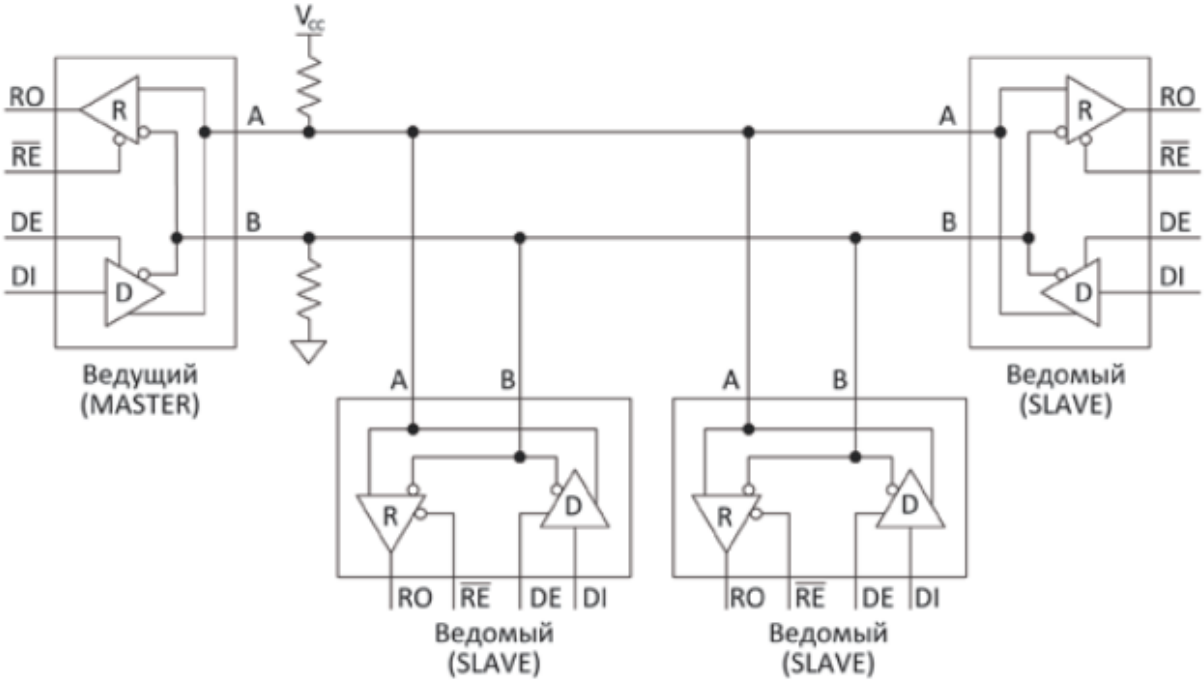

Рисунок 5.1 – Многоточечная полудуплексная приемопередающая система

После выявления слабых мест необходимо рассмотреть существующие методы защиты от данных угроз и внедрить их минимизируя влияние на общие качества всей системы в целом.

Первая угроза, от которой необходимо защитить данные в интерфейсе RS-485, это электромагнитные помехи. Если в передаче используются импульсы с крутыми фронтами, то в сигнале будут проявляться высокие частоты, график измерения сети с высокими частотами представлен на рисунке 5.2.

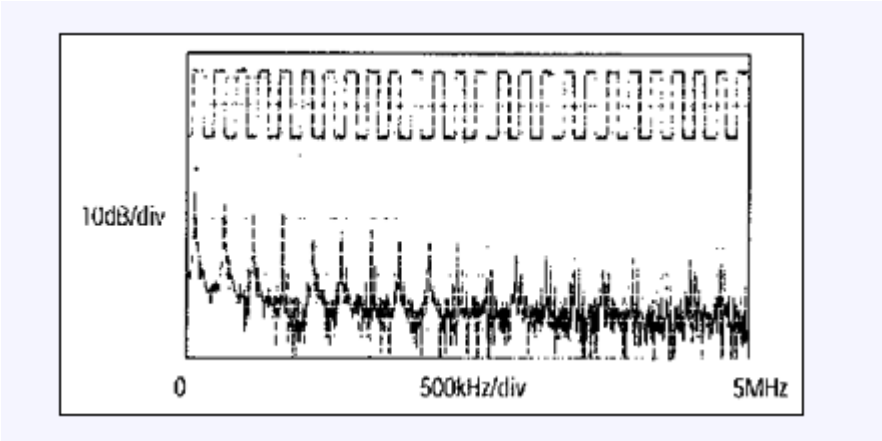

Рисунок 5.2 – Форма сигнала без помех и с помехами

Полученные высокие частоты приводят к возникновению электромагнитных помех. Система, построенная по балансной структуре, помогла бы избежать подобных проблем, но предположение о том, что провода будут иметь одинаковую длину и располагаться в одинаковых точках не даст нам 100% гарантии того, что линия будет защищена. Поэтому будем считать, что линии связи имеют разную длину, тогда линия будет подвержена так называемому эффекту длинных линий из-за распределенных индуктивных и емкостных свойств кабеля. По этой причине сигнал в линии начинает искажаться (резонировать), чтобы подавить эти колебания в конце линии подключается резистор с сопротивлением равным волновому сопротивлению кабеля, благодаря этому колебания снижаются.

Такой резистор называют «согласующим» или «терминирующим», для нашей сети он будет устанавливаться с двух концов линии, пример применения таких резисторов показан на рисунке 5.3.

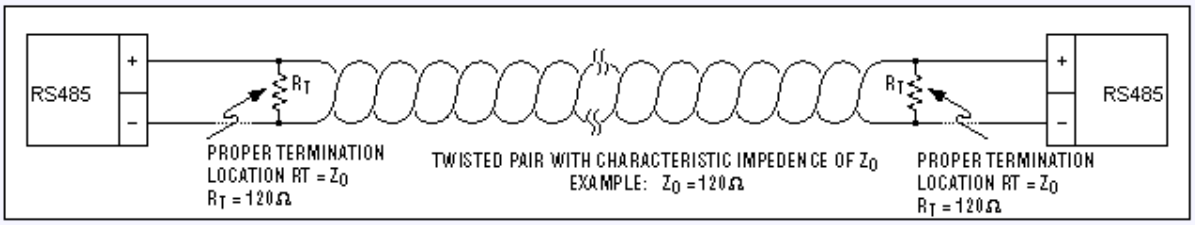

Рисунок 5.3 – Применение согласующих резисторов

Если неправильно подобрать сопротивление, то возникновение расхождений неизбежно, возникновение подобных помех при неправильно подобранном «терминаторе» показано на рисунке 5.4.

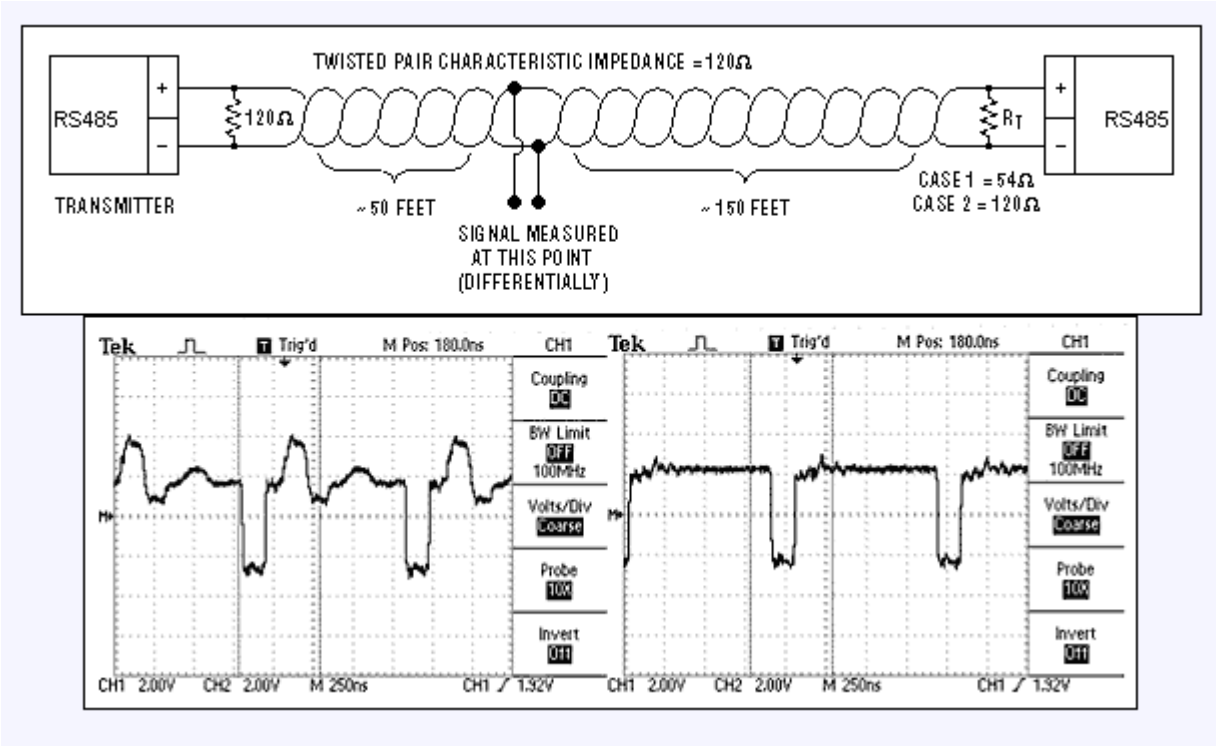

Рисунок 5.4 – Искажение сигнала при неверном терминировании линии

Устанавливать резисторы необходимо на дальних концах кабеля.

Следующая возможная угроза нашим данным это разность потенциалом между «землями», которая ограничена 7–12 В.

При развязке сети, нужно помнить о третьем проводнике – это «земля» и если устройства расположены друг от друга на больших расстояниях, то значительная разность потенциалов, которая возникает между ними, приведет к поломке не только передатчика, но и всего устройства.

Для устранения данной угрозы используется опторазвязка цифровых сигналов с организацией изолированного питания микросхем, тогда дополнительно прокладывается сигнальная «земля», соединенная с землей питания через большое сопротивление не менее сотни килоом. Пример применения такой системы показан на рисунке 5.5.

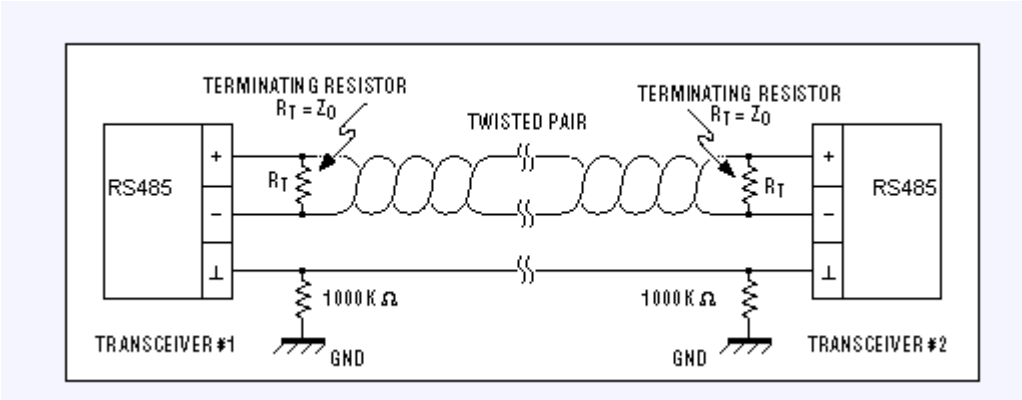

Рисунок 5.5 – Выравнивание потенциала через изолированную «землю»

Другой способ выровнять потенциал – это использование дренажного провода, при таком методе его прокладывают вместе с витой парой для соединения «земли» всех устройств, заземлять его необходимо через резистор 100 Ом и мощностью 0,5 Вт. Пример изображен на рисунке 5.6.

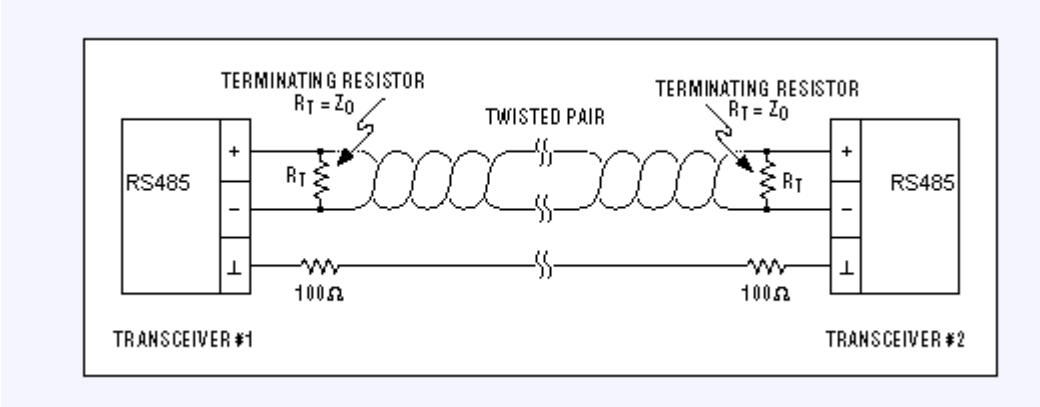

Рисунок 5.6 – Выравнивание потенциала дренажным проводом

Защита линии от перенапряжений, возникающих при замене кабеля или прикосновении каких-либо предметов к портам ввода-вывода. Перенапряжение может привести к выходу из строя проводящей структуры или вывести из строя несколько микросхем. Такие аварии приводят к значительным убыткам из-за повышения расходов на гарантийное обслуживание. Для защиты схем от этой проблемы могут использоваться внешние диоды, но для наших цепей мы будем использовать встроенную защиту, упрощенная схема которой показана на рисунке 5.7.

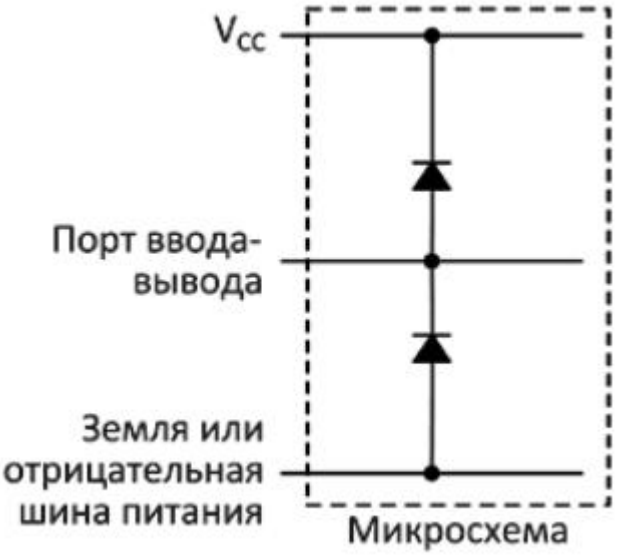

Рисунок 5.7 – Схема защиты от ЭСР

Для упрощения замены вышедшего из строя оборудования будет применена схема с «горячей заменой», которая исключает появление ложных импульсов. При горячей замене плат могут возникать переходные процессы, которые неблагоприятно скажутся на качестве передаче данных. Для устранения подобных проблем будет использоваться схема защиты входов, изображенная на рисунке 5.8.

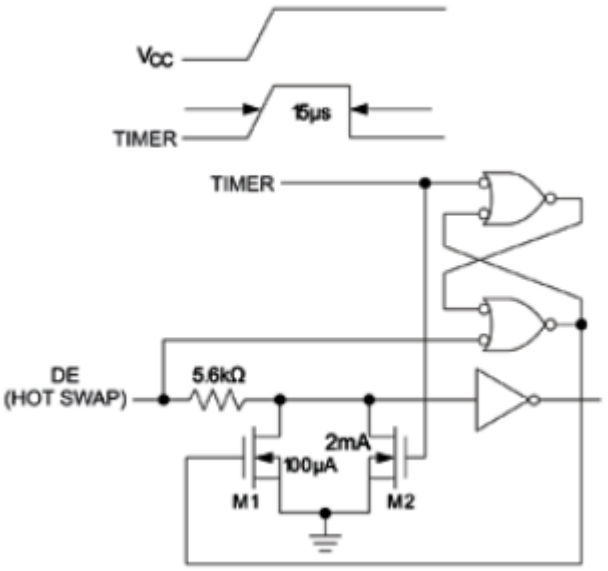

Рисунок 5.8 – Схема защиты входа при горячей замене

Следующий этап защита интерфейса – это экранирование и применение индуктивных фильтров [17]. Применение экранированного кабеля позволяет избавиться от емкостных связей и электромагнитных помех. Экран заземляется только в одной точке, чтобы избежать возникновения тока в сигнальной линии. В случаях, когда помехи все-таки попадают в линию, например при повреждении экрана, их лучше всего устранять с помощью индуктивных фильтров. Они встраиваются возле приемников, применение экранирования и фильтров в линии, изображено на рисунке 5.9.

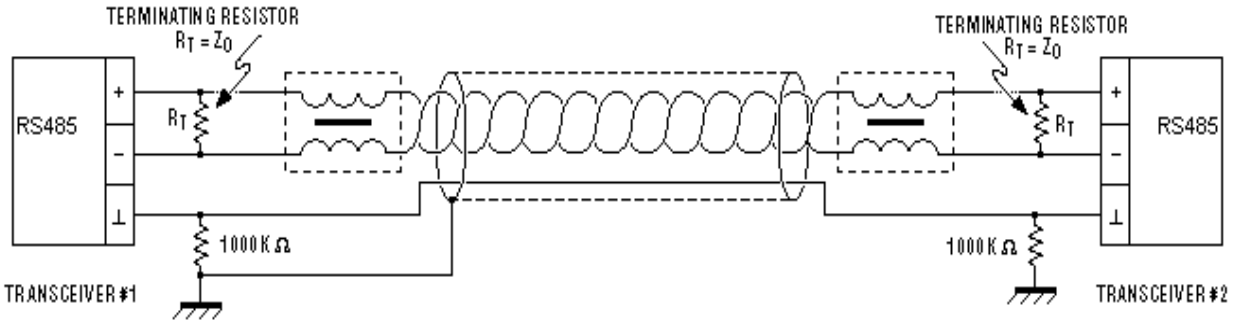

Рисунок 5.9 – Защита линии экраном и фильтрами

Последний этап организации защищенной линии – это разработка уникального протокола обмена между устройствами. Решение разработать собственный протокол, было принято не просто так, есть хорошие промышленные протоколы обмена Profibus, Modbus и другие, но вся документация, принципы организации и их структура находится в интернете в свободном доступе, что дает злоумышленникам шанс с помощью стороннего приемника врезаться в линию передачи, перехватить посылку, обработать и заменить своей. Другая проблема заключается в назначении посылки, если она вдруг окажется управляющей, то преступник сможет испортить работу всей системы в целом.

Чтобы избежать подобных проблем, и был разработан наш протокол. Его суть заключается в том, что если кто-то и ворвется в сеть, то предварительно ему придется расшифровывать то, что пыталось передаваться в посылке, выяснять структуру, какие байты и за что отвечают,

а в случае ошибки посылка просто не будет принята системой. Сверх этого ему придется рассчитывать контрольную сумму отправляемого пакета, которая используется в системе для проверки целостности, что является не менее трудоемкой задачей. Для ее решения надо знать какой вид контрольной суммы используется, через какие алгоритмы он организуется. Таким образом, единственное, что сможет сделать взломщик, это отправить похожую посылку, выполним предварительно все расчеты, на которые уйдет немало времени, и добьется только подмены нужных данных неправильными. Пример команды протокола – установка ручного режима представлен в таблице 6.

Таблица 6 – Установка ручного режима

2 байта	3 бит	5 бит	1 байт	1 байт	1 байт
Адрес объекта	000	01110	Номер переменной	1 – актив-ть 0 – деакт-ть	CRC8

Пример верного ответа на команду представлен в таблице 7.

Таблица 7 – Верный ответ на команду

2 байта	3 бит	5 бит	1 байт
Адрес объекта	000	01110	CRC8

Пример ошибочного ответа на команду представлен в таблице 8.

Таблица 8 – Ответ на команду с ошибкой

2 байта	3 бит	5 бит	1 байт
Адрес объекта	ошибка	01110	CRC8

5.2 Защита данных при передаче модем-сервер

После полноценной организации защиты линий обмена в интерфейсе RS-485 перед нами встала задача защиты данных при отправке с модема на сервер для обработки. Главная проблема в том, что данные уходят в открытом виде, а это недопустимо, так как при организации их обмена будут

использоваться команды управления, а перехват таких команд может привести к глобальным проблемам.

Передача информации осуществляется с помощью технологии GPRS. Развитие технологии началось с 1993 г., и она актуальна для использования до сих пор. Главное достоинство в оплате только объема передаваемой и получаемой информации.

Архитектура GPRS выглядит так, как показано на рисунке 5.10. Она расширяет стандартные компоненты GSM, новыми и измененными компонентами.

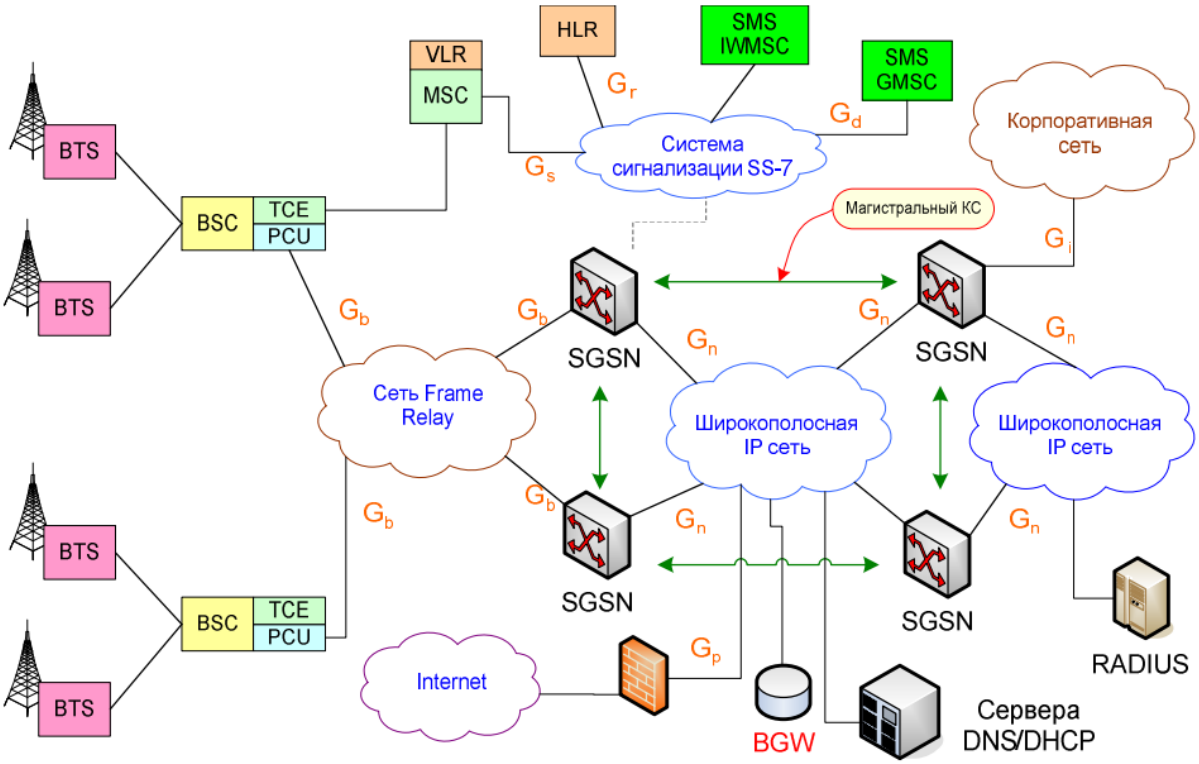

Рисунок 5.10 – Архитектура сети GPRS

В GSM появилось четыре новых узла:

– обслуживающий узел поддержки GPRS – SGSN он принимает информацию пользователя и преобразует их в IP-пакеты для передачи в сеть и обратно;

– шлюзовой узел поддержки GPRS – GGSN отправляет пакеты в сеть и получает ответы;

– мобильная станция MS – устройство для работы в глобальной сети;

– базовая станция BBS – оборудования оператора сотовой связи.

Подразделение на разные интерфейсы обусловлено стандартами ETSI, это позволяет связывать между собой оборудование разных производителей. Так как использование технологии GPRS обусловлено использованием SIM-карт, рассмотрим механизмы безопасности, которые нам предоставляются на базовом уровне.

К первому уровню относится идентификация – подтверждение наше право на использование устройства и аутентификация – подтверждение права работать в сети. Для реализации этого на базовой станции реализован специальный алгоритм A3, это позволяет предотвратить несанкционированный доступ злоумышленников к базовой станции. Схема организации этого процесса на рисунке 5.11.

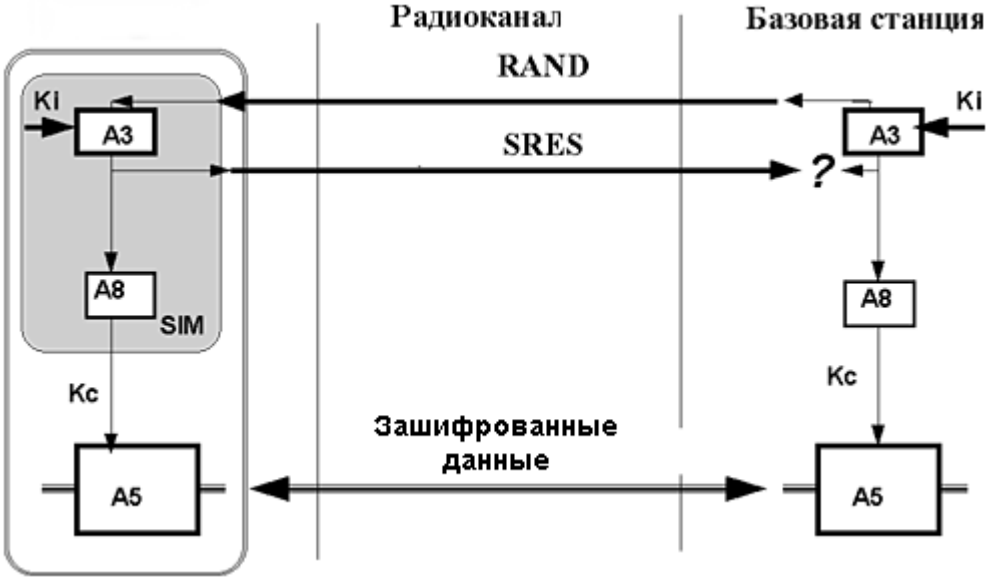

Рисунок 5.11 – Схема аутентификации в сети GPRS

Самым уязвимым местом в сети GPRS является канал радиоэфира, это канал обмена между BS и MS. Любой человек с самодельным приемником может перехватить сигналы, поэтому вся информация, идущая по каналу, шифруется с помощью алгоритмов GEA1, GEA2, GEA3. Атака и перехват данных на таком канале называется интернет-сниффингом.

Передача данных между внутренними узлами защищается протоколом GPT и применением частных IP по стандарту RFC1918. До сих пор

неизвестно еще ни одного случая перехвата информации из внутренних каналов.

Последним этапом остается защита от внешних угроз. Если обратиться к архитектуре сети, то можно заметить, что узел маршрутизации подвержен всем существующим на данный момент атакам, так как он является участником двух сетей. Эта проблема решается хорошим антивирусом и надежным файрволом. Также можно воспользоваться принципом трансляции адресов и для устранения возможности DDoS-атак использовать пограничные шлюзы.

Так как протоколы внутреннего шифрования уже старые, то было принято решение шифровать данные передающиеся на сервер дополнительно, с помощью одного из современных протоколов обмена. Перед этим рассматривались три современных протокола и два старых, но отвечающих всем требованиям криптостойкости:

– AES, первоначальное название Rijndael;

– ГОСТ 28147–89, он же «Магма»;

– ГОСТ Р 34.12-2015 («Кузнечик»);

– DES;

– IDEA.

Важная характеристикой систем шифрования – это способность противостоять криптоанализу.

На данный момент для шифрования используются два вида алгоритмов: симметричные и ассиметричные. Основной недостаток симметричных шифров – это организация процесса передачи ключей, т.к. закрытый ключ должен быть известен и отправителю, и получателю, а для ассиметричных алгоритмов – это низкая скорость выполнения из-за использования пары ключей, невозможность математически доказать криптостойкость и атака с подменой ключей.

Следующий признак классификации – это размер шифруемого сообщения. Различают поточные и блочные системы.

Поточные шифры это те, которые кодируют каждый символ с учетом его расположения:

– A3, A5, A8;

– MUGI;

– PIKE;

– RC4;

– SEAL;

– ORION и др.

Блочные разбивают информацию на блоки определенной длины, а затем шифруют, из-за схожести процедур зашифрования и расшифрования создание устройств шифровки становится проще, т. к. используются аналогичные блоки.

Самые известные блочные шифры [16]:

– ГОСТ 28147-89 – советский и российский стандарт шифрования, также являющийся стандартом СНГ;

– DES (Data Encryption Standard);

– AES (Advanced Encryption Standard) – американские стандарты шифрования, используемые для государственной тайны;

– IDEA (англ. International Data Encryption Algorithm) – международный алгоритм шифрования данных;

– ГОСТ Р 34.12-2015 («Кузнечик»).

Перед выбором шифра проведем их сравнительный анализ по основным параметрам:

– длина ключа;

– число раундов шифрования;

– длина шифруемого блока;

– криптостойкость;

– сложность аппаратной и программной реализации;

– сложность преобразования.

Сравнение значений перечисленных параметров для разных шифров представлено в таблице 9.

Таблица 9 – Сравнительный анализ шифров

Криптоалгоритм	Длина ключа, бит	Длина блока, бит	Число раундов	Число режимов работы
ГОСТ Р 34.12-2015	256	128	9	6
ГОСТ 28147-89	256	64	32	4
AES	128/192/256	128	10/12/14 (зависит от размера ключа)	5
DES	56	64	16	4
IDEA	128	64	8	4

Из анализа следует, что наиболее сильными алгоритмами являются «Кузнечик» и AES. В AES используется несколько режимов работы:

– режим электронной кодовой книги;

– режим сцепления блоков шифротекста;

– режим обратной связи по шифротексту;

– режим обратной связи по выходу;

– режим гаммирования.

ГОСТ Р 34.12-2015 представляет собой SP-сеть (постановочно-перестановочную) – несколько раундов линейного и нелинейного преобразования, а также операция наложения ключа. SP-сеть очень похожа на сеть Фейстеля, отличие в том, что преобразуется блок целиком [16].

Блочные шифры подвержены следующим типам атак:

– полный перебор;

– частотный криптоанализ;

– метод максимального правдоподобия;

– XSL-атака, атака на основе решения алгебраических уравнений;

– атака на основе внесения ошибок в процедуру дешифрования;

– атака на основе использования слабых ключей;

– метод «встречи посередине»;

– линейный криптоанализ;

– дифференциальный криптоанализ.

В итоге при выборе алгоритма для шифрования данных, шифр «Кузнечик» был отброшен как слишком молодой и малоизвестный, а его S-box для подстановок вызывают много вопросов о своем происхождении [16].

Алгоритмы DES, IDEA и «Магма» являются устаревшими и с набором уязвимостей.

Алгоритм AES из всего списка является самым надежным и проверенным, т. к. используется даже для документов государственной важности, поэтому было решено использовать для шифрования именно его.

Перед внедрением алгоритма была изучена его история. Шифр AES пришел на смену устаревшего алгоритма DES. Начиная с 1997 по 2000 гг. во время конкурса NIST, который получил название Advanced Encryption Standart любая группа исследователей или компания могла представить свою разработку в области блочного шифрования. Требования к шифру были следующими:

– должен быть блочный;

– должен иметь длину блока – 128 бит;

– должен поддерживать ключи – 128, 192, 256 бит.

В итоге во второй этап попали 5 шифров, их сравнительные характеристики представлены в таблице 10.

Главным победителем конкурса стал блочный шифр RIJNDAEL, который получил второе название AES. Самое интересное, что в нем впервые была применена особая структура обработки раундов, которая до этого с такой целью нигде не применялась, но, тем не менее, это не снижает заслуг и самих разработчиков, которые смогли внедрить в эту структуру такой большой блок текста с разными размерами ключей.

Таблица 10 – Сравнительные характеристики финалистов AES

Преимущества	Алгоритмы				
	RIJNDAEL	SERPENT	TWOFISH	RC6	MARS
Быстродействие: аппаратная реализация	+	+			
Программная реализация: на слабых ВС, на мощных ВС	+	+		+	
Этап расширения ключа	+		+	+	
Распараллеливаемость	+				
Этап дешифрования			+	+	+
Запас криптостойкости	Оптимум	Завышен	Завышен	Оптимум	Завышен
Кол-во голосов	86	59	31	23	13

Данный шифр использует нетрадиционные KASLT – сети. Шифруемый блок имеет форму прямоугольника с размерами 4x4, 4x6, а затем преобразуется через добавление ключа, табличную перестановку и линейное перемешивание [19].

Одно из главных его достоинств – это быстродействие на всех платформах, возможность распараллеливания, а коэффициент ускорения достигает 6-8 раз, поэтому данный алгоритм лучше всего подходил для наших целей и был более прост в реализации.

Обобщенная структура шифрования алгоритмом AES представлена на рисунке 5.12. Из структуры видно, что на вход подается текст, затем в первом раунде происходит добавление сгенерированного раундового ключа, полученное сообщение проходит четыре этапа модернизации, а затем этот процесс повторяется выбранное число раундов до получения шифрованного сообщения.

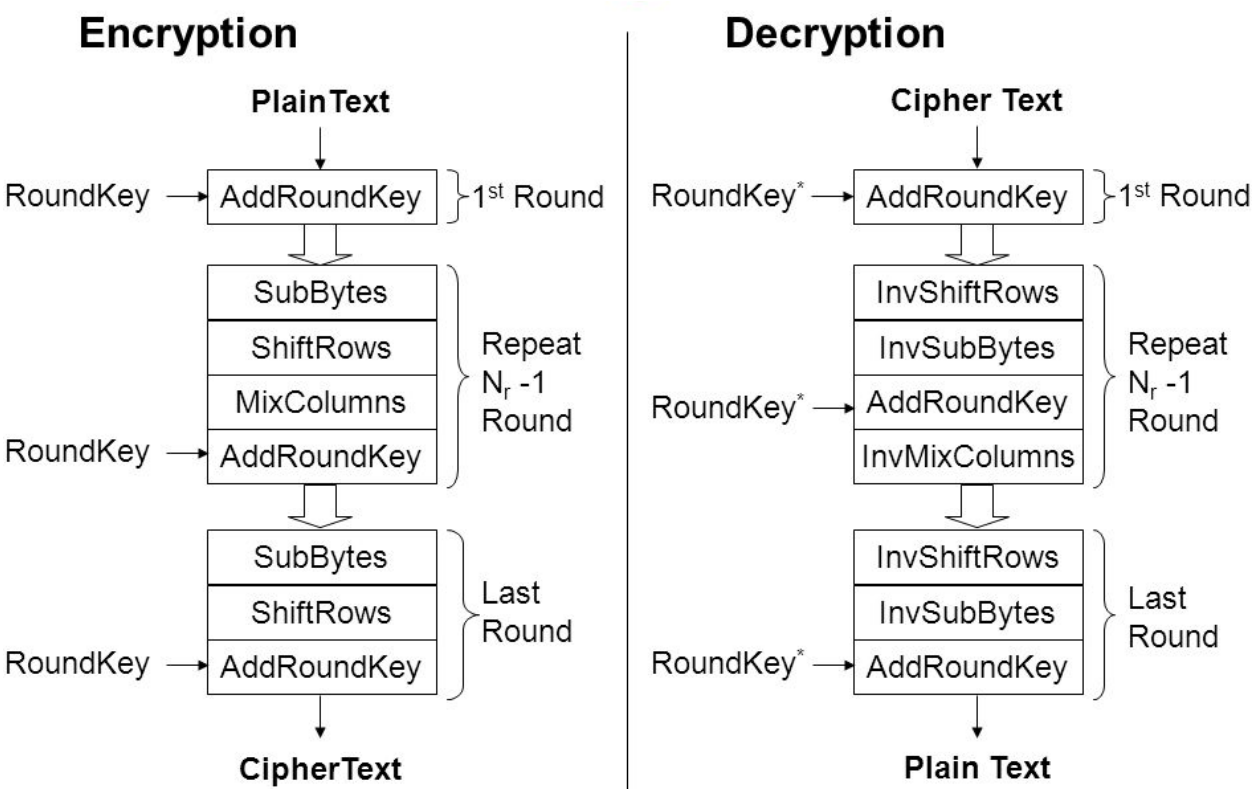

Рисунок 5.12 – Структура шифрования и дешифрования AES

Пример шифрования блока текста при помощи 128 битного ключа представлен на рисунке 5.13.

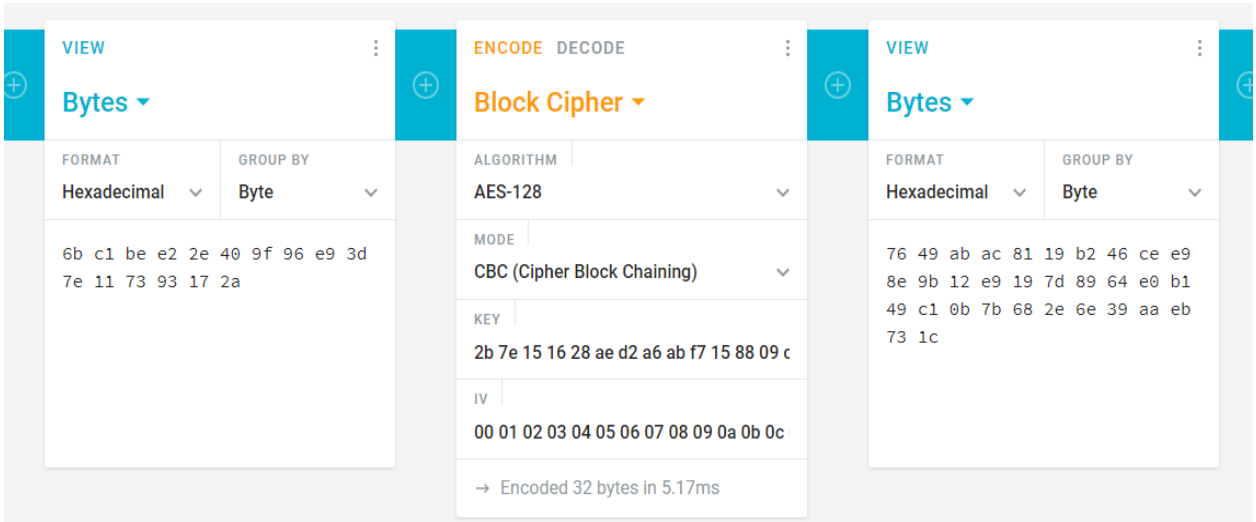

Рисунок 5.13 – Пример шифрования алгоритмов AES

Длина ключа, используемая при шифровании, определяет, сможет ли хакер взломать пароль с помощью полного перебора. По мере увеличения размера ключа количество комбинаций возрастает экспоненциально. К примеру, для взлома 128 битного ключа потребуется 1.02×10^{18} лет [19].

5.3 Защита данных клиент-сервер

В основе общения с сетью Internet лежит технология клиент/сервер. В общем случае это способ создания информационной системы из двух видов подсистем – клиентской и серверной. Клиентская часть инициирует запросы, а серверная обрабатывает и генерирует ответы.

Архитектура подразделяется на классическую и многозвенную. Для классической архитектуры имеется выделенный сервер, который обрабатывает запросы от определенного количества клиентов. Для многозвенной архитектуры выделяется несколько серверов с разными функциями, где каждый из них может быть, как сервером, так и клиентом. Обычно такие сервера называют сервера приложений, т. к. с ними связано прикладное программное обеспечение. Ярким примером многозвенной архитектуры является web-сервер, для присоединения клиентов к базе данных с помощью браузера. Структура клиент-серверного приложения изображена на рисунке 5.14.

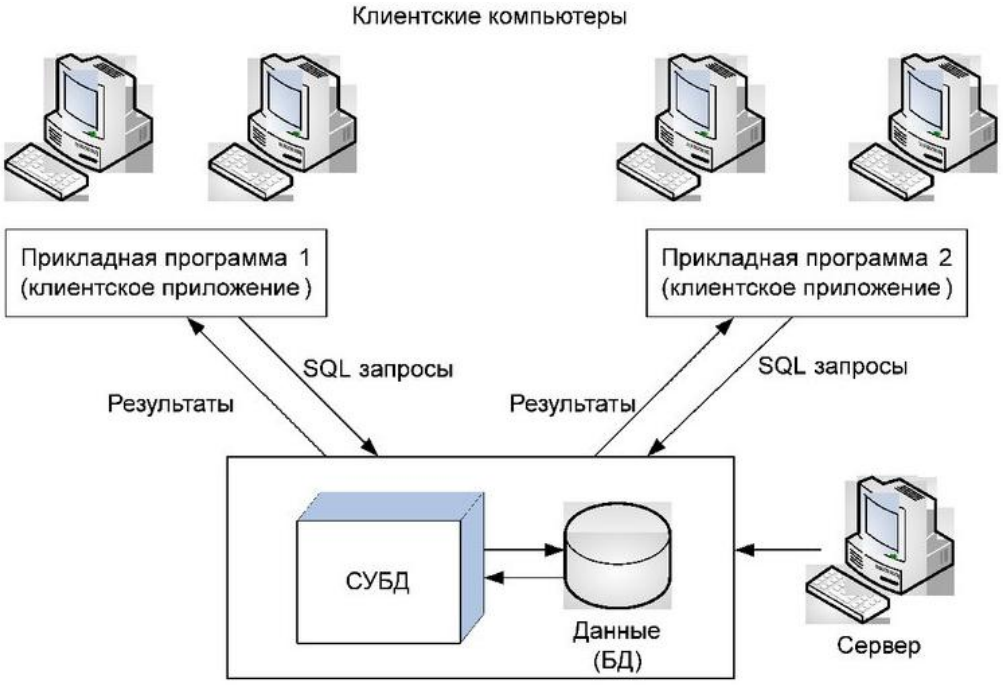

Рисунок 5.14 – Архитектура «клиент-сервер»

Архитектура клиент-сервер имеет следующие очевидные угрозы:

– пассивный перехват передаваемых запросов;

– модификация запросов;

– перехват ответов клиенты;

– модификация ответов клиенту;

– выдача хакером себя за сервер;

– выдача хакером себя за клиента;

– перегрузка сервера запросами;

– случайные сбои и ошибки;

– действия клиентов и др.

Средства безопасности не должны допускать проникновение информации во внешний мир, а также проверять подлинность сервера и клиентов.

Для планирования общей системы защиты необходимо выделить уровни обороны, например, пользователь, чтобы добраться до данных должен попасть в компьютер, затем в сеть, а уже потом на сервер, при этом ему будут доступны только определенные данные в зависимости от его уровня доступа. Защита все системы определяется уровнем защищенности ее самого слабого элемента, поэтому сформируем основные принципы защиты данных в распределенных системах:

– взаимодействие по выделенному физическому каналу;

– моделирование ситуаций перехвата всех сообщений, снижение или устранение отрицательных последствий;

– взаимодействие по виртуальным каналам связи;

– использование криптоалгоритмов с открытым ключом;

– контроль маршрута сообщений для определения отправителя;

– контроль виртуальных соединений;

– избегать алгоритмов удаленного поиска, либо же использовать его на выделенном сервере.

При защите на уровне приложения было решено использовать средства, разработанные внутри организации, чтобы лишить хакеров, хорошо известных им алгоритмов. Поддержка контроля целостности базы данных,

возможность отката до работоспособного состояния. Ведение аудиторского журнала для фиксации ошибок и сообщений от системы.

Информация на сервер защищается с помощью файервола в ОС Linux, которая является самой безопасной из всех систем. Также внедрена IDS система обнаружения вторжений, чтобы знать совершаются ли какие-либо атаки на сервер, и иметь возможность принять меры. Применение сильных паролей, сгенерированных случайным образом. Ограничение учетных записей и проверка привилегий. Применение песочниц и тюрем для запуска приложений.

Обмен данными с сервером происходи по принципам технологии JSON Web Token, основанный на стандарте RFC 7519. Он считается одним из безопасных способов передачи информации между двумя участниками. Для его создания определяется заголовок header с информацией по токену, данные payload, такие как id, его роль, подписи и т. д. [21].

Сервер аутентификации обеспечивает пользователя токеном, с помощью которого он сможет взаимодействовать с приложениями, более подробно принцип взаимодействия представлен на рисунке 5.15.

Приложение использует ОЦЕ для проверки аутентификации пользователя следующим образом:

– вход на сервер с помощью ключа (логин/пароль, либо ключ);

– создание JWT и отправка пользователю;

– при запросе к API, добавление ранее полученного JWT;

– при API запросе, приложение проверяет пользователя.

Хедер содержит информацию о том, как должна вычисляться подпись. Для этого используется HMAC-SHA256 (один ключ) или RS256 (два ключа).

Payload – это данные, которые хранятся внутри (заявки). Существует список стандартных заявок:

– iss – определяет приложение, из которого отправляется токен;

– sub – тема токена;

– exp – время жизни токена.

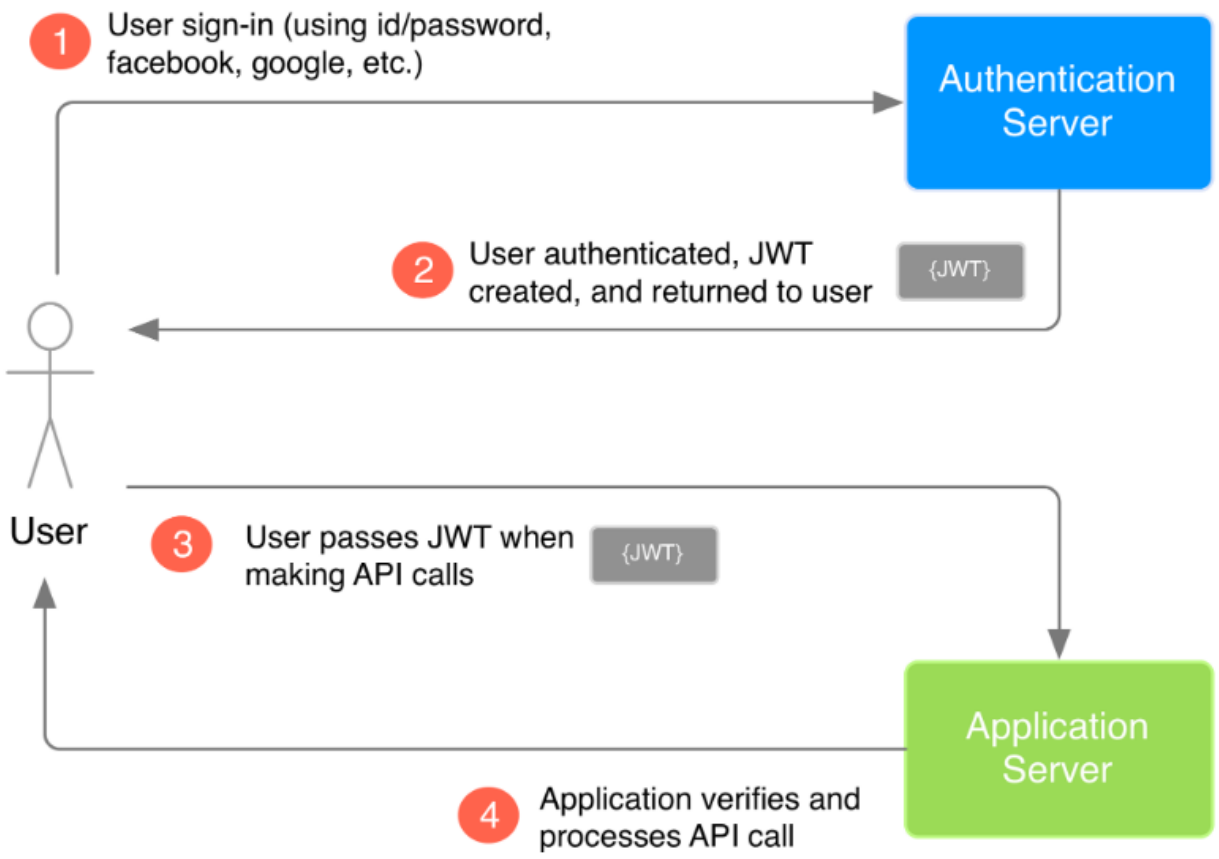

Рисунок 5.15 – Принцип взаимодействия JWT

Подпись вычисляется с использованием псевдо-кода, изображенного на рисунке 5.16.

```
const SECRET_KEY = 'cAtwalkkEy'
const unsignedToken = base64urlEncode(header) + '.' + base64urlEncode(payload)
const signature = HMAC-SHA256(unsignedToken, SECRET_KEY)
```

Рисунок 5.16 – Псевдо-код для вычисления подписи

Алгоритм base64url кодирует хедер и payload, соединяет и хеширует. Затем все компоненты соединяются в строку и отсылаются пользователю.

JWT не скрывает и не маскирует данные, а проверяет, что отправленные данные действительно были переданы авторизованным источником [21].

5.4 Выводы по разделу

В ходе работы над этим разделом была разработана комплексная защита системы. Первоначально были поставлены задачи, которые необходимо реализовать. Выделены три уровня защиты: начальный (RS-485), средний (модем-сервер) и высокий (клиент-сервер). Для каждого уровня защиты выделены актуальные угрозы безопасности данных и внедрены соответствующие средства для их устранения.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы была разработана система сбора, обработки и передачи данных о затратах и использовании энергоресурсов. Для этого первоначально были определены цели и задачи работы, исследованы технико-экономические показатели и проведен анализ аналогичных и похожих систем, применяемых в этой отрасли. Сделано обоснование выбора технологий, которые будут использоваться во время разработки.

На этапе проектирования была разработана структурная и функциональная схема системы, которые в совокупности дают понимание того, как система будет работать и какие функции выполнять. Для наладки связи между функциональными частями системы был разработан уникальный протокол обмена по интерфейсу RS-485.

Затем на языке C++ в среде Atmel Studio было разработано программное обеспечение для блока сбора и обработки, под управлением контроллера, и блока передачи данных, под управлением модема, исходя их требуемой для них функциональности.

С целью организации взаимодействия пользователей с системой была разработана база данных и web-интерфейс.

Последним этапом работы было выявление уязвимостей, выбор средств защиты от них и внедрение комплексной системы защиты в систему.

Разработанная система была введена в эксплуатацию на нескольких объектах и полностью функционирует, согласно, заявленных требований. В будущем планируются мероприятия по модернизации и улучшению системы, добавление новых функций в программное обеспечение и web-интерфейс, постоянная поддержка средств защиты. Система будет внедряться не только в организации, но и в управление освещением и энергетическими ресурсами городов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Мейерс, С. Эффективный и современный C++. Рекомендации по использованию: учебник / С. Мейерс. – М.: Вильямс, 2017. – 304 с.

2 Гамма, Э. Приемы объектно-ориентированного проектирования. Паттерны программирования: учебник / Э. Гамма, Р. Хелм, Р. Джонсон. – СПб.: Питер, 2001. – 344 с.

3 Гранд, М. Шаблоны проектирования в Java: учебник / М. Гранд. – М.: Новое издание, 2004. – 548 с.

4 Коннолли, Т. Базы данных. Проектирование, реализация и сопровождение: учебное пособие / Т. Коннолли, К. Бегг. – М.: Вильямс, 2003. – 1440 с.

5 Технологии автоматизированного учета энергоресурсов. – Дата обновления: 05.06.2015. URL: https://uchetjkh.ru/publikacii/sravnenietehnologiy-askue.html (дата обращения: 20.04.2018).

6 Современные беспроводные системы передачи данных. – Дата обновления: 30.01.2014. URL: https://strij.tech/tehnologiya-strizh (дата обращения: 23.04.2018).

7 Характеристика средств передачи данных и их учета. – Дата обновления: 03.06.2016. URL: https://vuzlit.ru/399423/issledovanie_harakteristik_sredstv_igbee_usloviyah_kvartiry_sovremennogo_mnogokvartirnogo_zhilogo_doma (дата обращения: 10.04.2018).

8 Технология передачи данных GPRS. Преимущества и недостатки. – Дата обновления: 14.08.2014. URL: http://1234g.ru/2g/gprs/struktura-gprs (дата обращения: 11.02.2018).

9 Ерёмина, М. А. Развитие автоматизированных систем коммерческого учета энергоресурсов: научная статья / М.А. Ерёмина. Москва: Изд-во Молодой ученый, 2015. – №3. – С. 135-138.

10 Исследование проблем информационной безопасности АСКУЕ. – Дата обновления: 24.08.2016. URL: http://7universum.com/ru/tech/archive/item/3307 (дата обращения: 11.03.2018).

11 Разработка функциональных схем. – Дата обновления: 28.10.2014. URL: https://studfiles.net/preview/28727867789679/page:2/ (дата обращения: 11.11.2017).

12 Руководство по технологии ZigBee. – Дата обновления: 10.07.2014. URL: http://www.center-proton.ru/files/misc/rukovodstvomodemzigzag.pdf (дата обращения: 23.09.2018).

13 Технология LPWAN. Преимущества и недостатки. – Дата обновления: 15.01.2016. URL: https://ru.wikipedia.org/wiki/LPWAN (дата обращения: 05.12.2018).

14 AT-команды. Описание и возможности. – Дата обновления: 12.02.2013. URL: http://housecomputer.ru/programs/at/at.html (дата обращения: 01.02.2019).

15 Разработка на PHP и MySQL. – Дата обновления: 15.16.2013. URL: https://webshake.ru/php-i-mysql-s-nulya/4 (дата обновления: 25.09.2018).

16 Алгоритм шифрования «Кузнечик». – Дата обновления: 15.10.2015. URL: http://lib.itsec.ru/articles2/crypto/gost-r-chego-ozhidat-ot-novogo-standarta (дата обращения: 03.04.2019).

17 Защита интерфейса RS-485. – Дата обновления: 09.06.2012. URL: http://technology.snauka.ru/2016/01/9292 (дата обращения: 05.05.2019).

18 AES шифрование. История появления. Преимущества. – Дата обновления: 11.08.2010. URL: https://studfiles.net/preview/909637/page:6/ (дата обращения: 07.02.2019).

19 Организация защиты на стороне сервера. – Дата обновления: 17.03.2017. URL: http://www.infocity.kiev.ua/hack/content/hack054.phtml (дата обращения: 02.03.2019).

20 Программно-технические средства обеспечения безопасности компьютерных сетей. – Дата обновления: 26.01.2016. URL: https://3ys.ru/programmno-tekhnicheskie-sredstva-obespecheniya-bezopasnosti-kompyuternykh-setej/zashchita-arkhitektury-klient-server.html (дата обращения: 12.03.2019).

21 JSON Web Token. Описание технологии. – Дата обновления: 09.08.2015. https://medium.com/vandium-software/5-easy-steps-to-understanding-json-web-tokens-jwt-1164c0adfcec (дата обновления: 15.05.2019).

ПРИЛОЖЕНИЕ 1

Справка о конфиденциальности