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

Институт машиностроения
(наименование института полностью)

Кафедра «Промышленная электроника»
(наименование)

11.04.04 «Электроника и наноэлектроника»
(код и наименование направления подготовки, специальности)

«Электронные приборы и устройства»
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Система резервного питания»

Обучающийся Д.С. Шеховцов
(И.О. Фамилия) (личная подпись)

Научный руководитель к.т.н., Е.С. Глибин
(ученая степень, звание, И.О. Фамилия)

Тольятти 2024

Содержание

Введение

В современном мире электроэнергия играет важную роль в повседневной жизни человека. Сегодня невозможно представить общество без электричества, при отключении которого вся привычная инфраструктура останавливается, перестает течь вода в водопроводе, приготовить пищу становиться проблемой, отсутствует связь и интернет, не работают современные гаджеты, смартфоны, ноутбуки и др. Стабильное электроснабжение остаётся актуальной темой для человечества.

С технологическим прогрессом возрастает интерес к использованию электричества как основного источника энергии и сейчас все больше и больше набирают объемы производства и НИОКР в области электроавтомобилей, электросамокатов, электродронов. «Согласно данным, аналитического центра при Правительстве РФ виден росте продаж и значительная поддержка сектора электромобилей: рост инвестиций в электромобили и зарядные станции, субсидирование спроса в большинстве стран, паритет стоимости обслуживания автомобилей с ДВС и электродвигателем. В Китае рост сегмента в 2022 году составил 85%, в США – 88%, в Европе – 28%. При этом в России объем рынка новых электромобилей за прошлый год вырос на 33%. Тем не менее, в целом по стране, на долю электромобилей пока приходится всего 0,5% от общего объема рынка. Нужна соответствующая инфраструктура» [1]. Это обусловлено тем, что цены и объёмы на нефтепродукты и газовую продукцию нестабильны из-за геополитической обстановки в мире и не стабильности курса валют, также использование газа бензина засоряют окружающую среду, в то время как электричество не требует использования продуктов горения, горюче смазочной продукции, соответственно это более экологично.

Из сводного отчета по ЕЭС России «Схема и программа развития электроэнергетических систем России на 2023-2028 годы» можно увидеть, что установленная мощность электростанций ЕЭС России в 2023–2028 годы возрастет по сравнению с 2021 годом на 11972,7 МВт (4,8 %) и составит 258563,6 МВт, рост доли мощности от ВИЭ – возобновляемых источников энергии (ВЭС – ветроэлектрические станции, СЭС – солнечная электростанция) возрастет с 1,6 % до 2,9 %. Для исключения рисков выхода параметров электроэнергетического режима работы энергосистемы за пределы допустимых значений и предотвращение аварийных ситуаций, планируется потратить колоссальные денежные средства на создание понижающих подстанций, устройств фиксации отключения линии, устройств управления отключением нагрузки и др. Потребность в инвестиционных ресурсах на развитие и модернизацию генерирующих мощностей и электрических сетей напряжением 220 кВ и выше в период 2023–2028 годов прогнозируется в размере 2631885,31 млн руб. с НДС [2].

Помимо наращивания объемов электроэнергии необходимо и стабильное качество. Многие сферы производства очень сильно зависят от электричества. От скачков в напряжении и отключения электричества ежегодно умирают тысячи людей по всему миру, а компании несут многомилионным убыткам. К примеру, согласно Постановлению № А55-27714/15 от 20.09.2016 АС Самарской области - 1 минута проста конвейера на АО «АВТОВАЗ» оценивается в 63 000 руб. В текущее время, непрерывность работы оборудования и систем становится все более критической, и резервное питание играет ключевую роль в обеспечении стабильности работы. Решение по установке дизельной электростанции требует: выделение площади, организации приточно-вытяжной вентиляции и системы отвода выхлопных газов, дополнительной шумоизоляции, периодических тестовых запусков [3], становиться не актуальным по сравнению с использованием дистанционной системы резервного питания,

состоящей из аккумуляторов, инвертора, зарядного устройства и системы контроля.

«Изучив статистику рынка источников бесперебойного питания (ИБП) РФ – за последние годы, можно увидеть, что 2022 г., начался на российском рынке ИБП не очень удачно, затем продажи уверенно пошли вниз, начав выравниваться лишь ближе к концу года. Основным драйвером данного снижения был массовый уход зарубежных производителей (работавших в инфраструктурном сегменте), что, без преувеличения, несло прямую угрозу безопасности государства.» [4]. В 2023г. по сравнению с 2022г. можно наблюдать внушительный рост на рекордные 50% в количественном и денежном выражении. По мнению экспертов рынок ИБП еще 2 года будет иметь небольшой рост 1-8%, затем вероятен локальный спад на два года, затем опять возврат рынка к росту. Данные еще раз подтверждают актуальность данной темы.

1 Источник бесперебойного питания – ИБП

1.1 Сущность ИБП и его роль в современном мире

Каждое современные предприятия не может обойтись без сложных электронных устройств и оборудования, но перебои в электроэнергии и скачки напряжения, могут остановить, а иногда и привести к его поломке. Для исключения таких проблем в 40х годах XX века началась работа по созданию приборов, которые при отключении основного источника питания, продолжали бы поставлять энергию.

ИБП (UPS, англ. Uninterruptible Power Supply) или источник бесперебойного питания — это тип системы бесперебойного питания, которая обеспечивает автоматизированное резервное электроснабжение нагрузки при выходе из строя входного источника питания или сети электропитания.

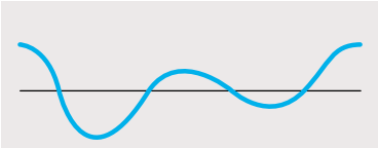
Основные функции ИБП:

1. Сохранить бесперебойную работу подключенного оборудования;
2. Исключить повреждение электронного и электротехнического оборудования от скачков напряжения;
3. Исключить риски повреждения и утери данных во время отключения электроэнергии.

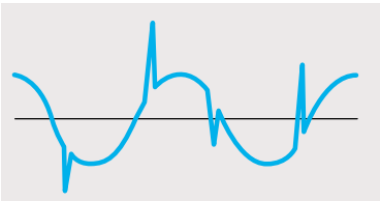
ИБП применяется для обеспечения надёжной работы во многих сферах жизни: IT-оборудование, корпоративные серверов, отопительные газовые и дизельные котлы, медицинское оборудование и др. электробытовые приборы.

ИБП устраняет следующие проблемы электросети, которые приведены в таблице 1.

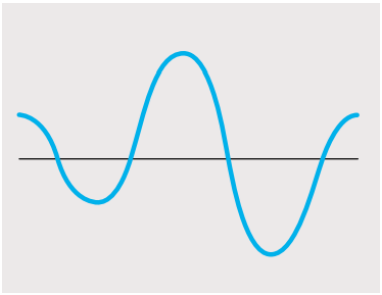
Таблица 1 - Типы неисправностей в электросети

Проблема	Описание	Эффекты
Прова напряжения 	Кратковременное падение уровня напряжения. Это наиболее распространенная неисправность (она даже составляет 87% от всех неисправностей), связанная с электроснабжением и вызванная запуском электрических устройств, таких как двигатели, компрессоры, подъемники и тали.	Снижение энергопотребления, необходимого компьютеру для правильной работы, что приводит к отключению клавиатуры или неожиданному сбою системы, а также к потере или повреждению обрабатываемых данных.

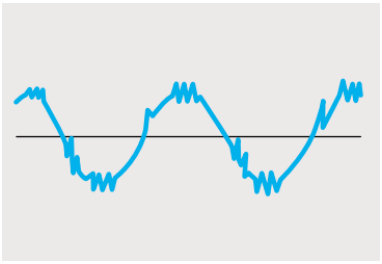
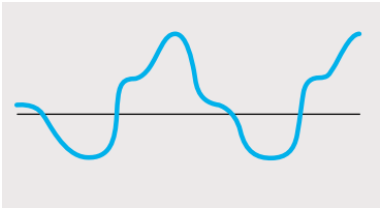
Продолжение таблицы 1

Проблема	Описание	Эффекты
Отключение электроэнергии 	Обесточивание приводит к полной потере электроэнергии. Это может быть вызвано чрезмерным спросом на электроэнергию, грозами, гололедом на линиях, дорожно-транспортными происшествиями, земляными работами, землетрясениями и т.д.	Это может привести к потере данных, нарушению связи, отсутствию освещения, блокировке производственных линий, нарушению деятельности компании, возникновению опасности для людей и т.д.
Скачки напряжения 	Скачки напряжения, как правило, вызваны ударом молнии, а также могут возникать при восстановлении электроснабжения после отключения электроэнергии	Это может повлиять на работу электронного оборудования по всей сети, последовательных линий или телефонных линий, а также может привести к повреждению или полному выходу из строя компонентов и необратимой потере данных.

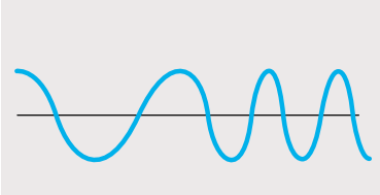
Продолжение таблицы 1

Проблема	Описание	Эффекты
Всплески напряжения 	Это кратковременное повышение напряжения, которое обычно длится 1/120 секунды. Скачок напряжения может быть вызван крупногабаритными электродвигателями, такими как системы кондиционирования воздуха. Любое дополнительное напряжение на линии электропередачи будет рассеяно , когда они отключатся.	Компьютерам и другому высокочувствительному электрическому оборудованию требуется переменное напряжение в пределах определенного допустимого диапазона. Любое значение напряжения, превышающее пиковое значение или эффективные уровни напряжения (последнее можно считать средним напряжением), создает нагрузку на чувствительные компоненты и приводит к преждевременным отказам.

Продолжение таблицы 1

Проблема	Описание	Эффекты
Электромагнитный/ Радиочистотный шум 	Шум от электромагнитных и радиопомех изменяет синусоиду, подаваемую питающей сетью. Он возникает в результате различных факторов и явлений, включая удары молнии, переключение нагрузки, работу генераторов, радиопередатчиков и промышленного оборудования.	Любой шум может быть прерывистым или постоянным и приводить к переходным процессам, ошибкам и неполадкам в компьютерных данных или телекоммуникациях; он также может приводить к неисправностям в различных электрических устройствах.
Паразитные и гармоничные токи 	Они возникают в результате возмущений или атмосферных колебаний, колебаний нагрузки, работы генераторов тока, электромагнитных излучений и промышленных систем.	Эти помехи приводят к ошибкам в выполнении программ, преждевременному выходу из строя компьютеров и любых содержащихся в них данных, а также к неисправностям в различных типах электрооборудования.

Продолжение таблицы 1

Проблема	Описание	Эффекты
Калебания частот 	Как правило, они присутствуют в энергии, вырабатываемой генерирующими установками.	Эти отклонения приводят к ошибкам при выполнении вычислений, трудностям при интерпретации магнитных носителей (дисков, лент и т.д.) и различным проблемам в электромеханических приложениях.

ИБП состоит из:

– аккумуляторная батарея;
– электронный блок управления для включения/отключения и контроля параметров тока;
– байпас для питания нагрузки в обход ИБП, когда параметры тока из сети соответствуют всем требованиям;
– бустер, который передает энергию от батарей к шине постоянного тока. Он повышает напряжение батареи, чтобы обеспечить достаточное напряжение на шине для питания инвертора. Бустер также обеспечивает независимость напряжения на шине постоянного тока от напряжения батареи, которое будет меняться при разрядке;
– инвертор, который преобразует постоянное напряжение шины постоянного тока в переменное напряжение, подаваемое на нагрузку. ИБП последнего поколения включают в себя высокопроизводительные инверторы на основе высокочастотной технологии IGBT, которые способны генерировать идеальные

синусоидальные напряжения даже при сильно искажающих нагрузках, сохраняя при этом высокие показатели эффективности при особенно компактных размерах;

– зарядное устройство для автоматического восстановления заряда в аккумуляторах.

Аккумуляторная батарея является основным элементом в ИБВ, который обеспечивает резервное питание при отлучениях и скачках в напряжении. Существует два основных типа батарей для ИБП: литий-ионные и свинцово-кислотные. Каждый из них имеет свои преимущества и недостатки, что делает их подходящими для разных сценариев.

Литий-ионные батареи на рисунке 1. Литий-ионные батареи, известные своими компактными размерами и длительным сроком службы, отличаются более высокой плотностью энергии, более высокой производительностью, экологичностью, малым весом и меньшей потребностью в обслуживании. Однако их стоимость обычно выше.

Рисунок 1 - Литий-ионные батареи

Свинцово-кислотные батареи на рисунке 2. Эти батареи экономически эффективны и менее чувствительны к температуре, что делает их более

стабильными. Они подходят для систем с менее критичными требованиями к мощности. Однако свинцово-кислотные батареи крупнее, тяжелее и имеют меньший срок службы, чем литий-ионные.

Рисунок 2 – Свинцово-кислотная батарея

Замена батареи ИБП возможна, поскольку повреждения ИБП в основном вызваны старением батареи, пользователям достаточно заменить батарею, чтобы продлить срок службы и эффективность системы ИБП. При этом необходимо проверить совместимость и безопасность системы ИБП, так как батареи имеют разное напряжение и требования к зарядке.

По мощности модели ИБП разделяются на:

– ИБП малой мощности (до 3 кВА) на рисунке 3 – в основном это однофазные устройства, которые служат для защиты от скачков напряжения или отключения электроэнергии маломощных бытовых приборов на непродолжительное время. ИБП малой мощности могут защитить персональный компьютер от неожиданного отключения и потери данных, сохранить работу циркуляционного насоса для поддержания отопительной системы или сохранить работу морозильной камеры для сохранности продуктов;

Рисунок 3 – ИБП малой мощности

– ИБП средней мощности (до 20 кВА) на рисунке 4 – однофазные и трехфазные приборы, могут обеспечить работоспособность электросети частного дома, важного медицинского оборудования, влияющего на сохранение жизни человека или целого компьютерного зала;

Рисунок 4 – ИБП средней мощности

– ИБП большой мощности (от 20 кВА и выше – вплоть до 300 - 500 кВА) на рисунке 5 – трехфазные изделия, предназначенные для промышленных масштабов, обеспечивают автономной работой: производственные линии, центры обработки данных, серверных, отдельные корпуса и здания.

Рисунок 5 – ИБП большой мощности. Трехфазный ИБП серии VGD-II-33R (MODULAR)

Модели ИБП могут иметь следующие типы корпусов:

– настенные, пример на рисунке 6 – предполагают возможность крепления ИПБ к стене, также для увеличения емкости в отдельный настенный шкаф могут быть размещены дополнительные аккумуляторные батареи. Расположение таких источников должно быть недалеко от питаемой нагрузки. Данный тип ИБП имеет малую мощность и небольшие габариты, в основном служит для защиты

точечного оборудования, например газового котла в жилом помещении;

Рисунок 6 – Настенный ИБП

– напольные (tower), пример на рисунке 7 – имеют вертикальную ориентацию и устанавливаются на плоской, горизонтальной поверхности. Это устройства, предлагаемые в диапазоне от минимальной до максимальной мощности: например, 400 ВА для автономного ИБП и до 200 кВА для сетевого ИБП с двойным преобразованием. В зависимости от их мощности, технологии и количества встроенных батарей они могут быть более или менее громоздкими и тяжелыми. Например, для ИБП большей мощности необходимо даже предусмотреть системы вентиляции и воздушного охлаждения в центре обработки данных, чтобы обеспечить максимально возможную производительность всей установки;

Рисунок 7 – напольный ИБП

– стоечные (rack), пример на рисунке 8 – представляют собой ИБП формата 19 дюймов, предназначенные для установки в отсеки шириной 19 дюймов с использованием систем бокового крепления. Некоторые ИБП шириной менее 19 дюймов можно установить в стойку с помощью дополнительного комплекта RM, представляющего собой своего рода 19-дюймовый лоток. Для всех стоечных ИБП специалисты определили единицу измерения высоты ИБП как "U" (около 44 мм в высоту), которая позволяет установщику знать, сколько места ИБП будет занимать в стоечном отсеке;

Рисунок 8 – стоечный (rack) ИБП

– универсальные (tower/rack), пример на рисунке 9 – представляет собой сочетание стоечного и напольного типа, что позволяет, настроить его либо в вертикальном автономном режиме с помощью опорных ножек, либо в режиме стойки.

Рисунок 9 – универсальный (tower/rack) ИБП

1.2 Типы систем ИБП

Выделяют основные три технологии ИБП. У каждой технологии есть свои преимущества, и каждая может быть необходима для настройки экономически эффективной защиты электропитания, особенно в сложных системах. Выбор ИБП для конкретного применения требует изучения ряда факторов. Размер нагрузки, расположение и критичность защищаемого оборудования являются ключевыми, а также бюджетными соображениями при выборе ИБП для резервного питания.

Три основных типа конфигураций систем ИБП:

– С двойным преобразованием в режиме онлайн;

– Линейно-интерактивные;

– Автономные (также называемые резервными и батарейными).

Эти системы ИБП определяются тем, как энергия проходит через устройство.

Автономный/резервный ИБП (off-line, standby, back UPS). Автономные ИБП, также называемые резервными ИБП или резервными батареями, являются экономически эффективным выбором. Лучшие автономные ИБП достаточно быстро переключаются на батарею, чтобы предотвратить аномалии электропитания и пережить кратковременные отключения. Автономный ИБП защищает от большинства скачков напряжения, но не поддерживает идеальную мощность при незначительных просадках и скачках. «Если внешняя сеть работает в штатном режиме, то ИБП питает нагрузку напрямую от входа и работает аналогично сетевому фильтру. В случае отклонения напряжения от допустимых пределов или при его полном отключении, резервный ИБП автоматически переключает нагрузку на аккумуляторные батареи (питание в таком режиме осуществляется через инвертор, преобразующий постоянный ток в переменный). Обратное переключение выполняется также автоматически и производится после возвращения сетевого напряжения к норме» [7].

Ключевым фактором качества автономного ИБП является диапазон мощности, который устройство может изменить, прежде чем переключиться на резервное питание от батареи. Чем шире диапазон, тем меньше расход энергии на батарею и тем больше время резервного копирования при отключении питания. Чем чаще ИБП переключается на резервное питание, тем меньше срок службы батареи.

Технология автономных ИБП защищает от большинства скачков напряжения, сдерживая избыточное напряжение, и помогает пережить более 90% всех отключений. Система автономного ИБП пропускает электроэнергию переменного тока прямо через устройство, мимо переключателя и к точке выхода, к которой подключена защищаемая нагрузка.

Когда происходит сбой входного питания, встроенная батарея и инвертор, преобразующий постоянный ток батареи в переменный, активируются и подключаются к выходу с помощью переключателя. Обычно при переходе на резервное питание от аккумулятора перерыв в подаче энергии составляет 6-8 миллисекунд. Эта технология лучше всего подходит для устройств мощностью менее 1500 ВА, таких как малые офисы, персональные домашние компьютеры и другие менее критичные приложения. Автономные ИБП - хороший вариант для тех, кому требуется меньшая мощность и стоимость. Технология автономных ИБП обеспечивает резервную защиту питания для настольного оборудования, игровых консолей, рабочих станций, беспроводных сетей и другой электроники. Во время отключения электроэнергии они обеспечивают достаточное время работы для сохранения выполняемой работы и упорядоченного отключения оборудования. Помимо резервного питания, большинство автономных ИБП обеспечивают базовую защиту от скачков напряжения. Упрощенная схема автономного ИБП представлена на рисунке 10.

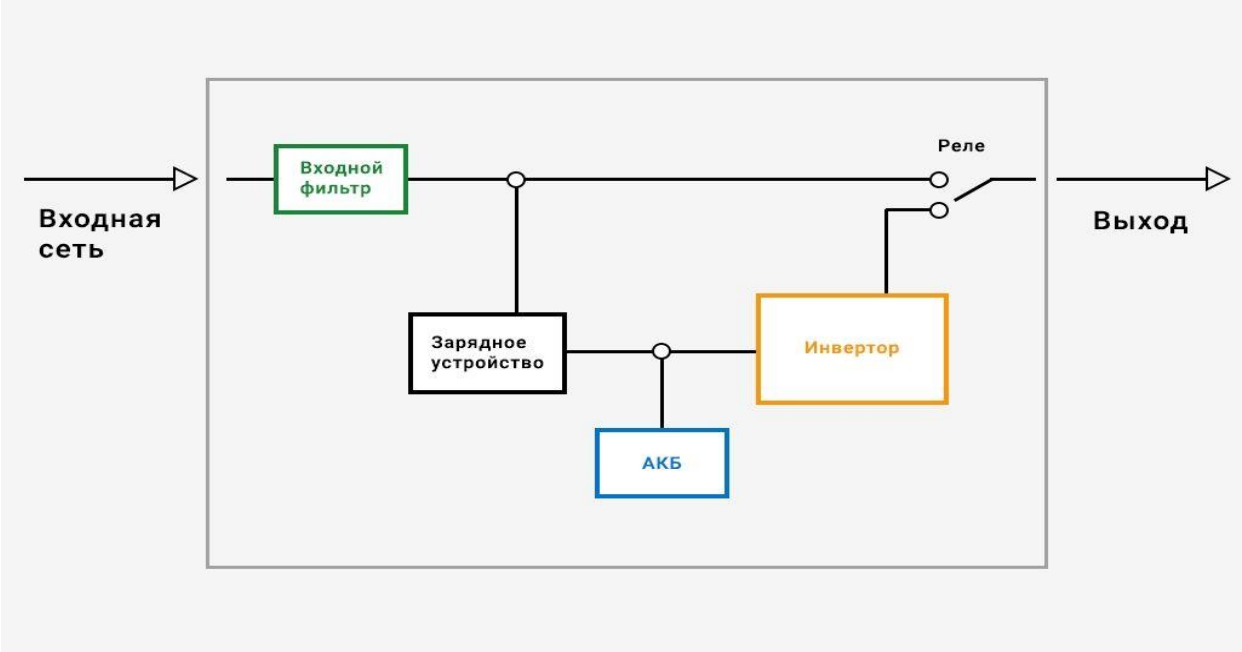


Рисунок 10 - Упрощенная схема автономного ИБП

Главное преимущество автономных ИБП при сравнении с другими типами можно выделить низкую стоимость.

К недостаткам автономных ИБП, можно отнести:

- переключение нагрузки происходит не мгновенно, задержка до 5 мс;
- при работе от электросети, напряжение и частоты не корректируются;
- быстрый износ аккумуляторов т.к. переход на аккумуляторную батарею происходит даже при небольших скачках напряжения;
- аппроксимированная синусоида выходного напряжения при работе в автономном режиме;
- практически отсутствует защита от скачков в напряжении и электромагнитных помех.

Недостатки резервных ИБП сужают область их применения. В основном ИБП данного типа подходят для использования в условиях стабильной электросети с приборами, которые нечувствительны к низкому качеству напряжения.

Линейно-интерактивные ИБП (line-interactive, Smart-UPS). Аналогичен автономному варианту, только схема дополнена входным регулятором напряжения. Линейно-интерактивные системы ИБП обеспечивают как кондиционирование питания, так и резервное питание от батарей. Эта технология особенно эффективна в районах, где перебои в электроснабжении редки, но часто происходят колебания напряжения. Линейно-интерактивные ИБП поддерживают широкий диапазон колебаний входного напряжения, прежде чем переключиться на резервное питание от батарей.

Помимо резервного питания, линейно-интерактивные ИБП обеспечивают гораздо лучший контроль над колебаниями напряжения, чем автономные системы. Важнейшим преимуществом линейно-интерактивных ИБП является схема усиления напряжения и диапазон входного напряжения, который принимает ИБП. Чем шире диапазон, тем больше полная защита.

Технология линейно-интерактивных ИБП обеспечивает кондиционирование питания с перерывом в 4-6 миллисекунд при переходе на резервное питание от батарей и защищает от наиболее распространенных проблем с электропитанием, возникающих в сети. При этом ИБП также контролирует уровень напряжения и выравнивает пониженное и повышенное напряжение. Эта технология обеспечивает хороший выбор между разумной защитой и умеренными эксплуатационными расходами.

В линейно-интерактивных ИБП инвертор становится частью выходного сигнала и всегда включен. Инвертор может работать в обратном направлении, заряжая батарею при нормальном входном сигнале переменного тока, и переключаться на питание от батареи при сбоях в работе, что обеспечивает фильтрацию и регулирование напряжения. Линейно-интерактивные системы ИБП полагаются на батарею для обеспечения питания, поэтому этот тип имеет тенденцию разряжать батарею чаще, чем онлайновые системы ИБП, которые обеспечивают питание через процесс двойного преобразования.

При отсутствии входного питания, переключатель размыкается, и питание поступает от АБ на выход ИБП, но т.к. инвертор всегда включен, линейно-интерактивный ИБП обеспечивает дополнительную фильтрацию и снижает переходные процессы при переключении по сравнению с резервным ИБП. Линейно-интерактивные ИБП обычно используются в стоечных системах мощностью менее 5000 ВА. Упрощенная схема линейно-интерактивного ИБП представлен на рисунке 11.

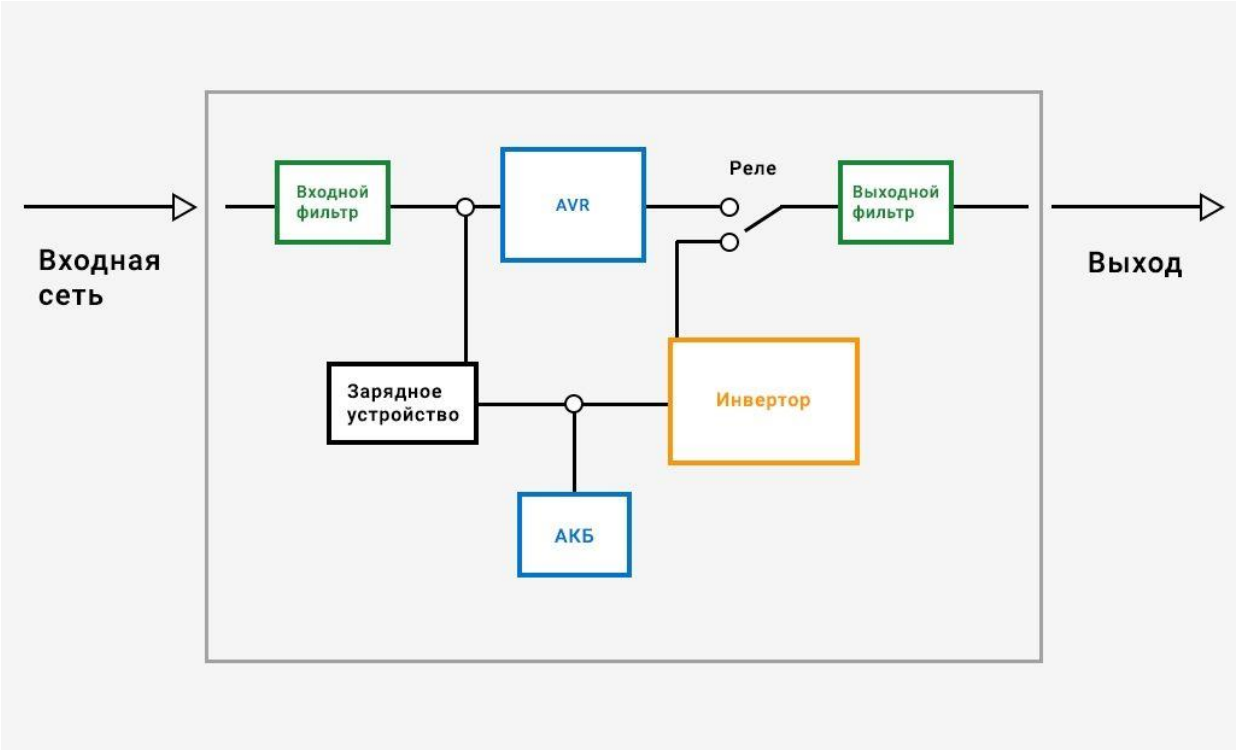


Рисунок 11 - Упрощенная схема линейно-интерактивного ИБП

Превосходство линейно-интерактивных ИБП перед автономными:

– выравнивание нестабильной сети, колебаний без переключения на АБ;
– синхронизация инвертора и входной сети позволяют более быстро производить процесс переключения.

К недостаткам линейно-интерактивных ИБП можно отнести:

– искажение выходного сигнала в виду поступательного регулирования напряжения;
– входное напряжения, частота, помехи не корректируются в режиме работы от электросети необходимым образом;
– в автономном режиме, многие модели не выдают безупречную синусоиду выходного напряжения.

Линейно-интегративные ИБП не подходят в работе с IT-оборудованием, медицинской техникой, т.к. выходное напряжение будет недостаточным для высоких требований чувствительного оборудования.

«Несмотря на большое количество ИБП, именно две модели используются наиболее часто. Различия между двумя типами ИБП приведены в таблице 2» [15].

Таблица 2 – Различия между ИБП типа back-UPS и smart-UPS

Свойство	Back-UPS	Smart-UPS
Форма выходного напряжения	При использовании ИБП повышается за счет возможности работы во время отключений напряжения	Позволяет создать более надежную компьютерную систему за счет принудительного тестирования ИБП, чувствительности ИБП к малейшим искажениям напряжения. В плохих электрических сетях часто переходит на работу от батареи (защищая при этом оборудование) и разряжает ее

Продолжение таблицы 2

Свойство	Back-UPS	Smart-UPS
Взаимодействие с компьютером	Базовые функции – подает сигналы о переключении на работу от батареи, разряде батареи, принимает сигнал на отключение ИБП. Регистрирует основные события в электрической сети на диске компьютера	Кроме базовых функций, имеет массу дополнительных: включение и выключение по расписанию, регистрация напряжения в электрической сети и т.д.
Защита оборудования	Защищает оборудование от потери данных при отключении или значительном кратковременном уменьшении напряжения	Кроме функций Back-UPS защищает компьютер от выхода из строя при значительном повышении напряжения. Блок питания компьютера защищается от перегрузки при низких напряжениях и от части импульсных нагрузок

Продолжение таблицы 2

Свойство	Back-UPS	Smart-UPS
Назначение	Для защиты отдельных недорогих компьютеров, потеря данных или выход из строя которых не приводят к критическим для пользователя последствиям	Для защиты более дорогих (примерно до 5000 долларов) работающих отдельно компьютеров или недорогих файловых серверов, работающих в условиях хорошей электрической сети
Применение в очень плохих электрических сетях	Не рекомендуется	Не рекомендуется

Онлайн ИБП (on-line, ИБП с двойным преобразованием энергии). «Устройство выполняет двойное преобразование поступающего из сети напряжения. Сначала из переменного в постоянное, а затем обратно – из постоянного в переменное. В силовой цепи on-line ИБП аккумуляторы занимают промежуточное положение между непрерывно функционирующими выпрямителем и инвертором (батареи соединены с выходом первого и входом второго). Такая схема позволяет избежать задержек при переходе в автономный режим, так как инвертор подключен к АБ постоянно и каких-либо дополнительных коммутаций, в случае проблем с внешней электросетью, не требуется» [7].

Электроэнергия переменного тока стабильна и чиста при генерации. Но во время передачи и распределения оно подвержено просадкам, скачкам напряжения и полным сбоям, которые могут прервать работу компьютеров, привести к потере данных и повреждению оборудования. Когда речь идет о защите критически важных ИТ-нагрузок, только технология двойного

преобразования онлайн полностью защищает от всех этих проблем с электропитанием, обеспечивая высочайший уровень безопасности сетей.

Онлайн-системы ИБП обычно называют системами с двойным преобразованием, поскольку входящая энергия преобразуется в постоянный ток (DC), а затем обратно в переменный. Такая конструкция AC-DC/DC-AC обеспечивает повышенную степень изоляции нагрузки от нестабильностей в основной сети. Онлайновый ИБП принимает входящий переменный ток и преобразует его в постоянный с помощью выпрямителя для питания батареи и подключенной нагрузки через инвертор, поэтому нет необходимости в переключении питания. Если основной входной сигнал переменного тока пропадает, выпрямитель отключается от цепи, и батареи поддерживают подачу энергии на устройство, подключенное к ИБП. Когда входное питание восстанавливается, выпрямитель снова принимает на себя большую часть нагрузки и начинает заряжать батареи. Поскольку питание проходит через онлайн-источник беспрерывно, на выходе получается идеальная синусоидальная волна. Этот тип ИБП защищает критическую нагрузку практически от всех помех, включая мелкие гармоники и искажения формы волны. Это означает, что качество электроэнергии от онлайн ИБП значительно выше, чем у других технологий. Автономные и линейно-интерактивные технологии снижают влияние скачков, перепадов и провалов напряжения, либо сглаживая пики и долины, либо повышая мощность, либо переключаясь на резервное питание от батарей. Однако в пределах нормального хода синусоиды большинство колебаний мощности остаются в стороне. Онлайновый ИБП восстанавливает синусоиду, а не просто кондиционирует исходное электропитание.

Онлайновый ИБП обеспечивает непрерывное высококачественное питание оборудования переменным током без перерыва при переходе на батарею, защищая оборудование практически от всех нарушений электроснабжения, связанных с отключениями, перебоями, просадками, скачками напряжения или шумовыми помехами. Настоящий онлайн ИБП с

двойным преобразованием обеспечивает 100-процентное питание, нулевое время перехода на батарею, отсутствие изменений в выходном напряжении и лучшее подавление переходных процессов по сравнению с линейно-интерактивными устройствами.

ИБП с двойным преобразованием в режиме онлайн — это наиболее распространенный режим работы ИБП, используемый для защиты крупных центров обработки данных и обеспечивающий высочайший уровень качества электропитания нагрузки. Онлайновые системы также обеспечивают регулирование частоты, что защищает от колебаний при пуске генератора. Упрощенная схема ИБП с двойным преобразованием в режиме онлайн представлена на рисунке 12.

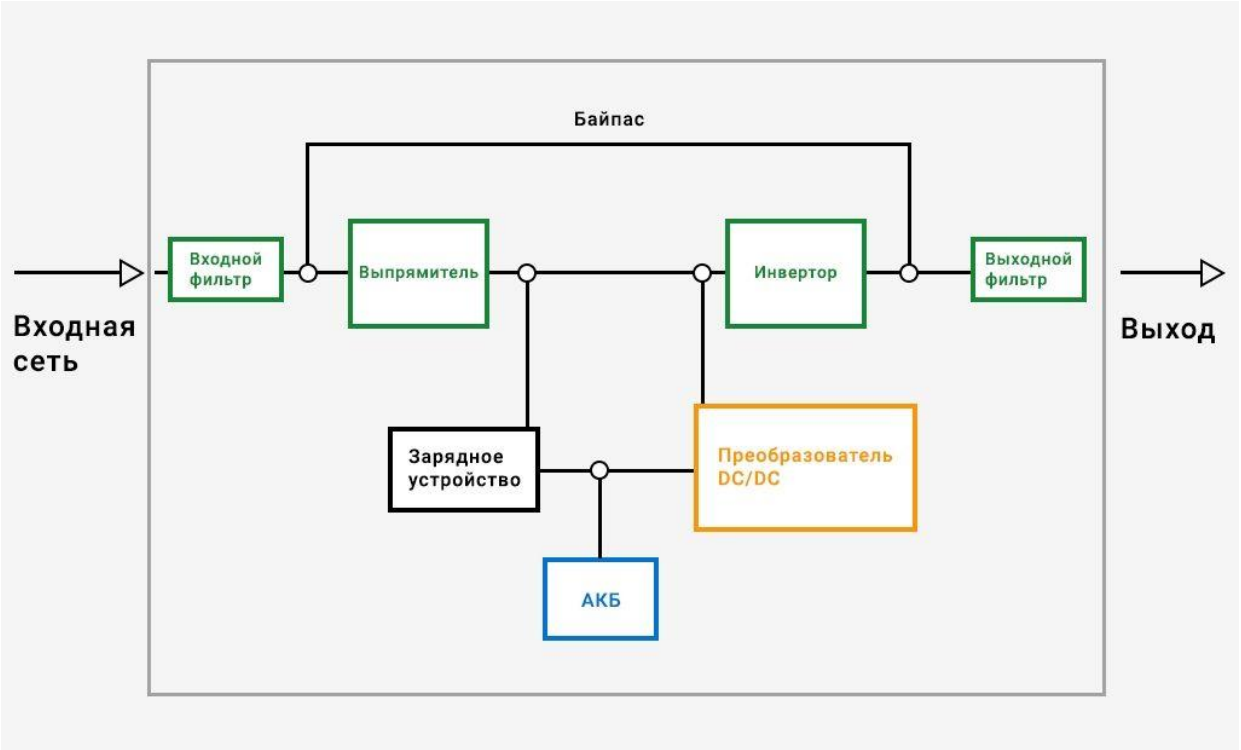


Рисунок 12 - Упрощенная схема ИБП с двойным преобразованием в режиме онлайн

К преимуществам онлайн ИБП можно отнести:

– мгновенное переключение;

– идеальная синусоидальная выходного напряжения при любом режиме работы;
– широкая амплитуда сетевых колебаний, исправляемых без перехода в автономный режим;
– максимальная защита нагрузки.

К недостаткам онлайн ИБП, можно отнести высокую стоимость.

Онлайн ИБП являются лучшим решением для обеспечения бесперебойного электропитания для любой технике, с любыми требования и чувствительности к электроэнергии от домашних устройств до ЦОД.

Для продления срока службы и корректной работы ИБП, в независимости от места расположения, необходимо убедиться, что он расположен в прохладном и сухом месте с надлежащим потоком воздуха и контролем температуры. Вентиляционные отверстия устройства не должны быть заблокированы, чтобы обеспечить циркуляцию воздуха во избежание перегрева. ИБП запрещено размещать вблизи открытых окон или в местах с высоким содержанием влаги и пыли. Системы ИБП и батареи должны храниться и эксплуатироваться в прохладной, сухой среде, при температуре 20-25 °С. Хранение батарей ИБП при температурах, выходящих за пределы этого диапазона, может привести к сокращению срока службы батарей. Для обеспечения надлежащей циркуляции воздуха система ИБП располагается так, чтобы вентиляционные отверстия не были заблокированы. Периодически необходимо производить осмотр вентиляционных отверстия и, если ИБП легко доступны, необходим производить чистку и удаление пыли, грязи или мусора. Отказы батарей - самая распространенная причина простоя ИБП. Необходимо следить за тем, чтобы батареи всегда были полностью заряжены, держа систему ИБП, подключенной к сети. Если по каким-то причинам не планируется использовать систему ИБП на долгое время, ее следует накрыть и хранить в сухом прохладном месте. Перед

хранением батарею ИБП рекомендовано зарядить в течение 24 часов, а затем подзаряжать каждые три месяца.

Если питание пропадет часто, требуется определить период времени для поддержания устройств в рабочем состоянии, чтобы сохранить важные данные и/или безопасно выключить оборудование. Для определения времени, необходимо рассчитать мощность, требуемую для работы подключенных устройств. На большинстве устройств мощность указана либо на самом устройстве, либо в руководстве пользователя. В большинстве случаев перебои в электроснабжении длятся не более пяти минут, но некоторые могут длиться и дольше. Чтобы рассчитать необходимое время работы, нужно выяснить, какая мощность, или нагрузка, требуется подключенным устройствам и какова емкость батареи системы ИБП.

Во-первых, необходимо определить основные характеристики для системы:

- напряжение. Большинство оборудования работает от сети переменного тока 220 В.
- сила тока, которую потребляет устройство, которая может составлять 1А или меньше и ограничивается максимальной силой тока в цепи. Как правило, в большинстве домов и предприятий используется розетка на 16А.
- мощность, количество энергии, потребляемое устройством.

Во-вторых, необходимо определить общую мощность защищаемого оборудования. Информацию о характеристиках устройств можно найти в руководстве пользователя устройства или данные указаны на этикетке безопасности устройства. Если мощность не указана, ее можно рассчитать самостоятельно, перемножив напряжение на силу тока.

В-третьих, зная все необходимые характеристики защищаемого оборудования, можно подобрать ИБП для обеспечения его работоспособности при отключении от центральной электросети, а также рассчитать время работы ИБП в автономном режиме по формуле ниже:

$$t = \frac{\mathrm{C} \times U}{P} \quad (1)$$

где t – расчетное время резерва в часах, ч;

C – суммарная емкость АКБ, А·ч;

U – суммарное напряжение АКБ, В;

P – полная мощность нагрузки, Вт.

К примеру, если известно, что мощность подключенной нагрузки к ИБП - 100 Вт, емкость АКБ – 100 А·ч, напряжение АКБ - 12 В, то время работы ИБП в автономном режиме составит 12 часов:

$$t = \frac{\mathrm{C} \times U}{P} = \frac{100 \times 12}{100} = 12 \text{ ч} \quad (2)$$

Также, используя данную формулу можно определиться с характеристиками емкости АКБ, чтобы определиться с выбором ИБП для конкретной системы. К примеру, мощность подключенной нагрузки к ИБП - 300 Вт, необходимое время работы в режиме резерв - 10 ч., напряжение АКБ - 12 В, суммарная емкость АКБ должна быть не ниже 250 А·ч:

$$\mathrm{C} = \frac{t \times P}{U} = \frac{10 \times 300}{12} = 250 \text{ А} \cdot \text{ч} \quad (3)$$

Если нужно больше времени работы, возможно, потребуется приобрести ИБП большей емкости или добавить модули батарей. В некоторых системах ИБП можно установить один или несколько модулей батарей увеличенной емкости для увеличения времени работы. Другие альтернативные варианты включают подключение системы ИБП к генераторам для получения более длительного резервного питания.

Система ИБП может контролироваться локально с помощью видимых и звуковых сигналов. Некоторые системы ИБП оснащены светодиодными индикаторами, ЖК-дисплеями и/или звуковыми сигналами, которые указывают на изменения в состоянии ИБП. С помощью программного обеспечения для мониторинга может быть организован удаленный контроль ИБП.

Существует огромное множество ИБП от разных производителей с разными характеристиками. Выбор конкретного, будет зависеть от многих факторов и задач, которые планирует решить компания. Размер нагрузки, какое оборудование предполагается защитить, финансовые возможности предприятия, частота отключения электроэнергии и много другое влияет на выбор ИБП.

2 Дистанционный контроль резервного питания

2.1 Стандарты и протоколы, используемые в промышленных коммутаторах

«ИБП является интеллектуальным устройством, обладающим широкими возможностями мониторинга и управления. Производительные цифровые сигнальные процессоры (DSP), применяемые в современных моделях ИБП, позволяют реализовать удаленный контроль статуса и основных параметров, используя несколько различных интерфейсов. Реализация интерфейсов может быть как в виде встроенных портов, так и дополнительных карт, примеры карт на рисунке 13 и рисунке 14, устанавливаемых во внутренний слот или подключаемых к порту RS-232. В большинстве трехфазных ИБП предусмотрено два внутренних слота для карт расширения и несколько встроенных коммуникационных портов» [8].

Рисунок 13 – Внутренняя однопортовая карта SNMP

Рисунок 14 - Внутренняя SNMP-карта с возможностью подключения датчика температуры и влажности

«ИБП, как правило, имеют на корпусе индикацию своего состояния, что позволяет ответственному лицу осуществлять мониторинг вручную, путем обхода всего оборудования, оснащенного ИБП. Однако для ручного контроля большого количества устройств, расположенных на значительном расстоянии в распределенной информационной инфраструктуре, потребуется значительное количество времени, что может привести к потере работоспособности некоторых объектов ИТ-инфраструктуры, а значит, и к нарушению сервисов. Для реализации системы дистанционного контроля основного и резервного электропитания, ниже, на рисунке 15, приведен пример возможной структурной схема СДК и принципиальной схемы модуля снятия показаний на рисунке 16» [9]

.

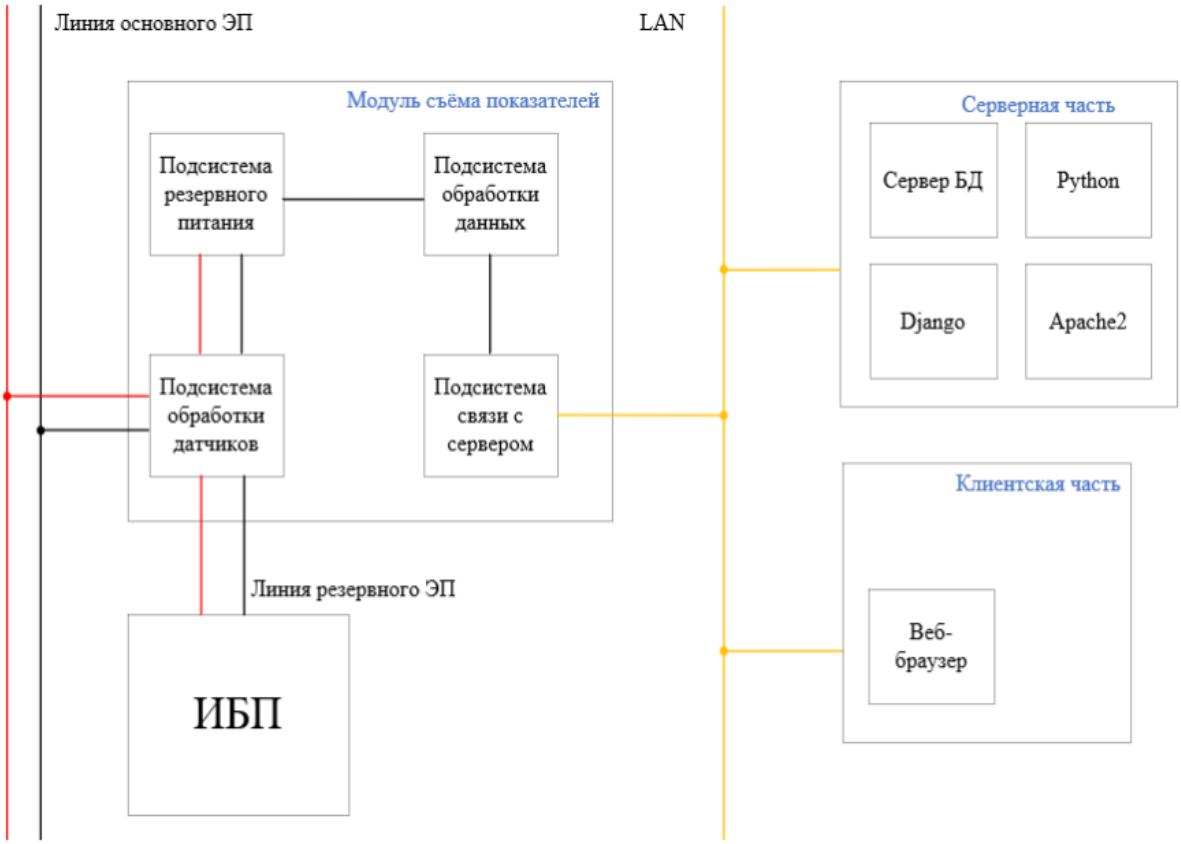


Рисунок 15 – Структурная схема системы дистанционного контроля

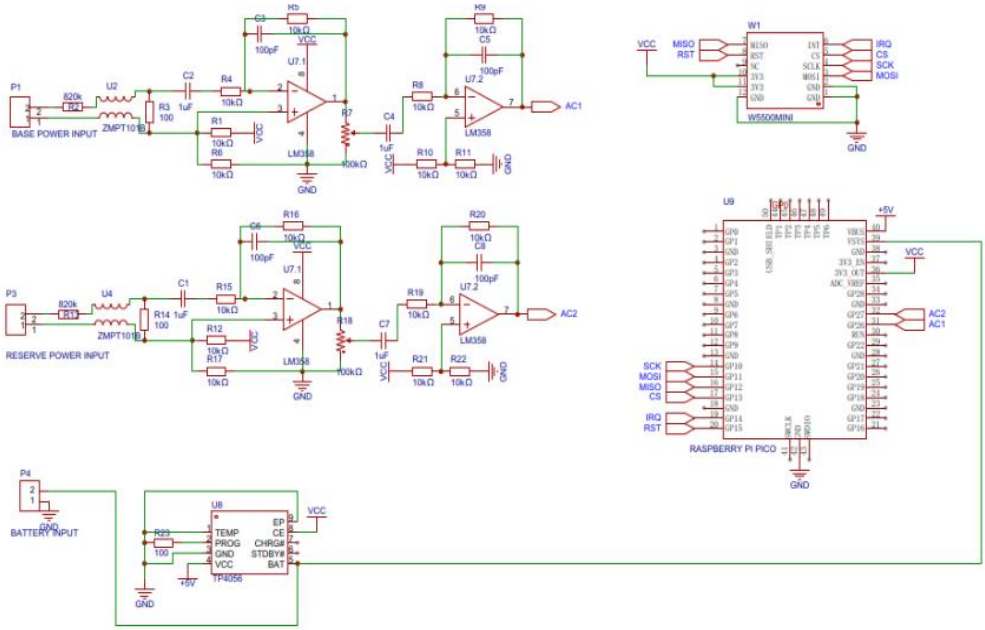


Рисунок 16 – Принципиальная схема модуля снятия показаний

Для организации систем промышленной автоматизации используются промышленные коммутаторы, пример на рисунке 17. Они отличаются надежностью, функциональностью. Для обеспечения бесперебойной связи между устройствами, эффективного контроля и мониторинга трафика используются различные протоколы и стандарты.

Рисунок 17 – Промышленный коммутатор

Протоколы промышленных коммутаторов — это стандартизированные наборы правил и процедур, которые регулируют связь и обмен данными в промышленных сетях. Протоколы определяют, как устройства обмениваются данными, передают и принимают их, обрабатывают ошибки, синхронизируют операции. Протоколы создают информационную структуру, обеспечивают бесперебойное, стабильное взаимодействие между устройствами. Они определяют формат пакетов данных, методы обнаружения и исправления ошибок. Каждый из них решает определенные задачи. Протоколы преимущественно делятся на открытые и закрытые.

Закрытые протоколы создаются поставщиками-разработчиками для использования в своих продуктах: ПО и оборудовании. Они зачастую защищены патентами, являются коммерческой тайной и называются проприетарными. Желающие ими воспользоваться могут сделать это при помощи предоставляемых компанией-разработчиком интерфейсов и разделяемых библиотек, но должны за это заплатить. Обычно это длится не

долго, большинство закрытых протоколов оканчивают свою жизнь всем известными и никому ненужными. Рано или поздно, они "утекают" в Интернет, а так как для их разработки и поддержки доступны ограниченные ресурсы одного-двух вендоров, они очень быстро морально устаревают. Пример такого закрытого протокола: VPN-протокол Microsoft PPTP (Point-to-point tunnelling protocol AKA Point-to-point toilet paper). Впрочем, существует немало успешных закрытых протоколов, например Skype.

Открытые протоколы, напротив, разрабатываются сообществами поставщиков-разработчиков, авторитетными институтами стандартизации или вообще возникают стихийно. Примеры открытых протоколов: IPSec, SMTP, HTTP, H323. Авторитетные международные институты и отдельные государства стандартизируют протоколы с целью нормализации взаимодействия производителей в различных отраслях. Цели у стандартов разные и зависят от того, кто эти стандарты создает и в каких сферах они применяются. В криптографии, например, стандарты устанавливают государства. Выглядит это как указание шифровать данные определенного уровня секретности при помощи алгоритмов шифрования. Цели таких рекомендаций не прозрачны. С одной стороны, следуя стандарту, бизнес и граждане надеются получить от государства гарантию защищенности шифруемых данных. С другой стороны, протоколы, рекомендуемые для шифрования коммерческих секретов зачастую значительно слабее протоколов, используемых для шифрования государственной тайны.

Отличным примером служит история возникновения протокола «DES». Первоначальная предложенная длина ключа шифра «Lucifer» составляла 128 бит, но в стандарт вошел его вариант с 64-битным ключом, причем только 56 бит использовались, собственно, для шифрования, а остальные 8 - для служебных целей протокола. В результате DES очень быстро устарел и был заменен на «3DES» (тройной DES), а US Deparment of Defence срочно объявил конкурс на лучшую долговременную замену. В результате конкурса был

выбран шифр «Rijndael», а стандарт получил название AES (Advanced Encrytion Standard) и успешно используется по сей день. Существуют страны, запрещающие использовать сильную криптографию в частных целях. Зачастую это объясняется их нежеланием допустить использование шифрования в незаконных целях. Казалось бы, открытые протоколы явно выигрывают перед закрытыми., но основным недостатком открытого протокола является возможность его изменения поставщиком-разработчиком для собственных нужд.

Для экономии времени и средств разработаны стандарты питания коммутаторов. PoE – стандарт, который питает промышленные коммутаторы через витые пары кабелей Ethernet. Он экономит ресурсы, так как не нужно оборудовать отдельную линию электропитания. Не требуется прокладка кабелей, обустройство розеток. Этот стандарт упрощает масштабирование сетей, развертывание оборудования. PoE делится на 4 типа в зависимости от мощности портов. Для промышленных сетей подходят 3 и 4 тип. Для использования всех преимуществ стандарта PoE нужно исключить все моменты, которые могут привести к проблемам. Разъемы RJ-45 рисунок 18 должны соединяться на 8 контактов, а также:

- витые пары, на рисунке 19, правильно подключены;
- нужно согласовать дополнительную мощность;
- проводка должна иметь соответствующий экран.

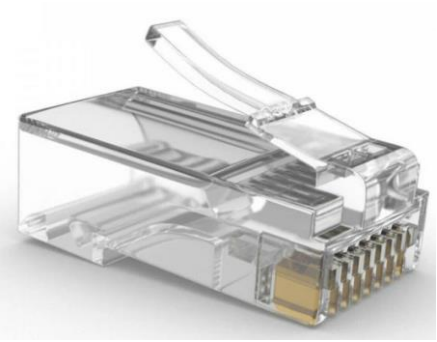


Рисунок 18 - Коннектор RJ45

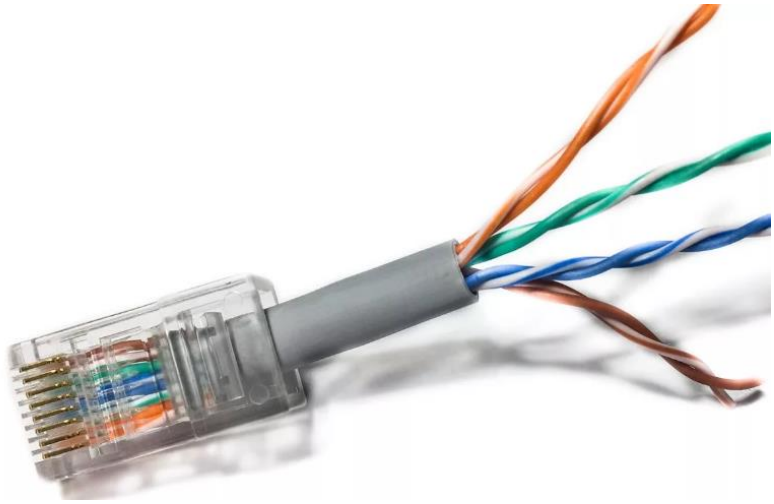


Рисунок 19 – Витая пара

Нельзя допускать нагрев витых пар. Это может спровоцировать снижение тока в них. Стандарт питания совершенствуется. Используются следующие его версии: PoE+ и PoE++. Они отличаются мощностью, которая нужна для поддержки устройств. С их помощью обеспечивается питание камер наблюдения, контроллеров, других компонентов, входящих в систему автоматизированного управления.

Открытые протоколы Modbus TCP и SNMP. SNMP совместим с различными устройствами, обеспечивает эффективное управление ими. С его помощью организуется мониторинг большого количества компонентов сетевой инфраструктуры. Низкие ресурсные требования позволяют использовать протокол SNMP для коммуникации с различными устройствами, включая датчики. Его использование требует настройки параметров передачи данных. Протоколы Modbus TCP и SNMP позволяют в режиме реального времени контролировать работу источников бесперебойного питания.

Протокол TCP\IP. Прикладной транспортный протокол TCP\IP обеспечивает обмен блоками двоичных данных. С его помощью информация доставляется на нужные адреса. На базе этого протокола работает Интернет.

Он используется многими известными производителями коммутационного оборудования. На его базе разрабатываются стандарты промышленной связи. Modbus TCP\IP – прикладной протокол, который сочетает физическую и сетевую составляющую. С его помощью обеспечивается обмен информацией между устройствами в локальной инфраструктуре, взаимодействие с внешними ресурсами.

Modbus - это протокол обмена сообщениями прикладного уровня, который обеспечивает связь клиент/сервер между устройствами, подключенными к различным типам шин или сетей. Являясь серийным стандартом в отрасли с 1979 года, Modbus продолжает обеспечивать связь между миллионами устройств автоматизации. Сегодня поддержка простой структуры Modbus продолжает расти. Интернет-сообщество может получить доступ к Modbus через зарезервированный системный порт 502 в стеке TCP/IP. Modbus представляет собой протокол запроса/ответа и предлагает услуги, определяемые функциональными кодами.

Функциональные коды Modbus являются элементами блока данных протокола (PDU - protocol data unit) запроса/ответа Modbus. Протокол Modbus определяет простую единицу данных протокола (PDU), не зависящую от нижележащих коммуникационных уровней. При отображении протокола Modbus на конкретные шины или сети может вводить некоторые дополнительные поля в блок данных приложения (ADU - Application discovery and understanding). Блок данных приложения Modbus создается клиентом, который инициирует транзакцию Modbus. Функция указывает серверу, какое действие необходимо выполнить. Прикладной протокол Modbus устанавливает формат запроса, инициируемого клиентом.

Поле кода функции в единице данных Modbus кодируется в одном байте. Допустимые коды находятся в диапазоне 1 ... 255 десятичных значений (диапазон 128 - 255 зарезервирован и используется для исключений ответов). Когда сообщение отправляется от клиента к серверному устройству, поле кода функции указывает серверу, какое действие

необходимо выполнить. Код функции "0" недействителен. К некоторым кодам функций добавляются коды подфункций для определения нескольких действий. Поле данных сообщений, отправляемых от клиента к серверным устройствам, содержит дополнительную информацию, которую сервер использует для выполнения действия, определенного кодом функции. Сюда могут входить такие элементы, например, адреса дискретных и регистровых элементов, количество обрабатываемых элементов и количество фактических байтов данных в поле. В некоторых типах запросов поле данных может отсутствовать (иметь нулевую длину), в этом случае серверу не требуется дополнительная информация. Только код функции определяет действие. Если в правильно принятом Modbus ADU нет ошибок, связанных с запрошенной функцией Modbus ADU, поле данных ответа сервера клиенту содержит запрошенные данные. Если возникает ошибка, связанная с запрашиваемой функцией Modbus, поле содержит код исключения, который может быть использован серверным приложением для определения следующего действия.

Например, клиент может считывать состояния «вкл.»/«выкл.» группы дискретных выходов или входов или он может читать/записывать содержимое данных группы регистров. Когда сервер отвечает клиенту, он использует поле кода функции, чтобы указать либо на нормальный (безошибочный) ответ, пример на рисунке 20, либо что произошла какая-то ошибка (так называемый ответ исключения), пример на рисунке 21. В случае нормального ответа сервер просто повторяет запрос с исходным код функции.

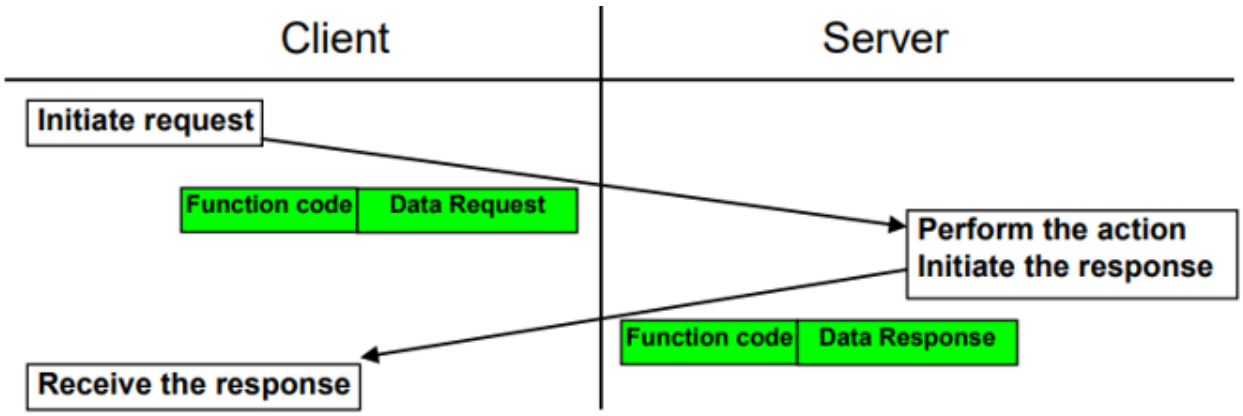


Рисунок 20 - Операция Modbus (без ошибок)

Для ответа на исключение сервер возвращает код, эквивалентный исходному коду функции код из PDU запроса с наиболее значимым битом

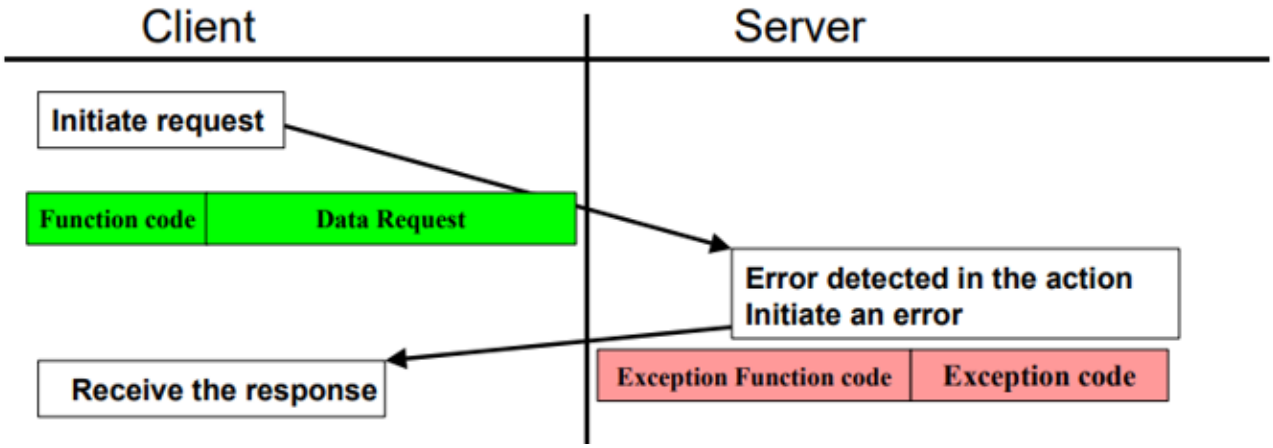


Рисунок 21- Операция Modbus (с ошибками)

Modbus это последовательный коммуникационный протокол, не требующий существенных вычислительных ресурсов, поэтому часто применяемый в промышленных системах для сбора информации от несложных датчиков и устройств. Для его реализации на устройствах, как правило, используется физический порт RS-485 или RS-232, пример на рисунке 22.

Рисунок 22 – интерфейсы RS232 и RS485

SNMP — это стандартный интернет-протокол прикладного уровня, позволяющий различным устройствам в сети взаимодействовать и обмениваться данными. Он входит в набор протоколов TCP/IP и является одним из самых распространенных сетевых протоколов. Протокол упрощает управление сетью, предоставляя единый интерфейс для множества различных устройств, подключенных к одной сети.

SNMP позволяет пользователям идентифицировать устройства, контролировать производительность сети, отслеживать изменения в сети и состояние устройств в режиме реального времени. SNMP контролирует элементы сети с помощью агента SNMP, который должен быть включен для работы. К устройствам, использующим SNMP для связи, относятся маршрутизаторы, коммутаторы, принтеры, брандмауэры, балансировщики нагрузки, рабочие станции, серверы, камеры и многие другие. SNMP собирает и упорядочивает данные со всех этих устройств, используя их IP-

адреса, что облегчает поиск и устранение неисправностей, мониторинг и управление сетью.

Мониторинг SNMP помогает пользователям собирать различную информацию с сетевых устройств. Поскольку многие производители устройств поддерживают SNMP, можно легко собирать данные с различных сетевых устройств. Использование SNMP для мониторинга и управления сетевыми устройствами также улучшает качество обслуживания клиентов, поскольку позволяет администратору предвидеть потребности и быстро устранять любые сетевые ошибки.

Использование SNMP имеет множество преимуществ:

- подходит для всех предприятий. Поскольку SNMP работает практически со всеми типами устройств, его можно использовать для комплексной настройки мониторинга как в небольших сетевых средах, так и в крупных сетях с большим количеством компонентов. Утилита может легко получить различные типы данных, например уровень тонера в принтере или температуру в серверной комнате;
- простой мониторинг. Почти все производители включают SNMP-агент в свои устройства, поэтому для мониторинга не нужно устанавливать стороннее программное обеспечение. Таким образом, SNMP делает мониторинг доступным для любого пользователя без необходимости использования другого программного обеспечения или дополнительных прав доступа;
- совместимость. SNMP работает на уникальном языке, позволяющем пользователям взаимодействовать с устройствами разных производителей. Одно из его главных преимуществ заключается в том, что он позволяет администраторам управлять сетевыми ресурсами, которые не имеют операционной системы, но нуждаются в мониторинге - например, принтерами. Единообразие SNMP делает

его совместимым с любой операционной системой, включая Windows, Linux, macOS или Java.

Система SNMP состоит из следующих основных компонентов:

– network management system (NMS). Система управления сетью. Управляет сетевыми элементами в сети;
– SNMP-agent. Программное обеспечение, которое работает на контролируемом оборудовании, собирает метрические данные и выполняет операции, запрошенные в MIB управляемого устройства;
– management Information Base (MIB). База управленческой информации. MIB — это информационная база данных, содержащая параметры управляемого устройства;
– managed device. Управляемое устройство. Узел в сети (маршрутизаторы, серверы доступа, коммутаторы и т. д.), содержащий SNMP-агент и MIB.

Все компоненты работают вместе, позволяя сетевым инженерам извлекать информацию из сетевых устройств, независимо от производителя, типа устройства или программного обеспечения, на котором оно работает.

На рисунке 23 показаны основные компоненты SNMP и пути связи:

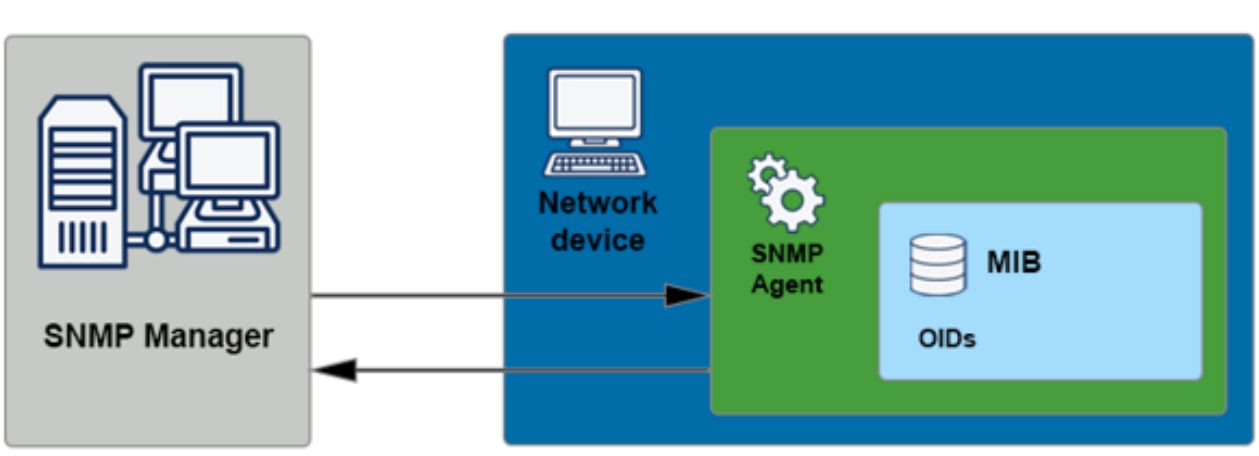


Рисунок 23 – Компоненты SNMP и их взаимосвязь

Менеджер SNMP (или сервер SNMP) — это централизованная станция управления, отвечающая за связь с устройствами, на которых запущен агент SNMP. Менеджер отправляет запросы агенту SNMP и получает ответы через регулярные промежутки времени. Обычно это ЭВМ, на которой работает одна или несколько систем управления сетью. Основными функциями SNMP-менеджера являются:

- отправка запросов и заявок агентам SNMP;
- получение ответов от агентов SNMP;
- установка или изменение различных переменных в агентах SNMP;
- подтверждение асинхронных событий от агентов.

Агент SNMP — это часть программного обеспечения, содержащаяся в сетевом устройстве и используемая для мониторинга и управления этими устройствами в сети. Включение агента позволяет ему принимать запросы от SNMP-менеджеров и отвечать на них, предоставляя статус устройства и необходимые метрики или устанавливая требуемую переменную. Агент получает необходимые данные из MIB управляемого объекта. В зависимости от типа устройства SNMP-агент может быть стандартным или специфическим для конкретного производителя. Основными функциями SNMP-агента являются:

- сбор данных о своем локальном окружении;
- хранить и извлекать данные из MIB;
- уведомлять менеджера о событиях;
- действовать в качестве прокси для некоторых сетевых узлов, не управляемых по протоколу SNMP.

SNMP имеет два номера портов по умолчанию, которые он использует для отправки пакетов данных UDP (User Datagram Protocol - протокол пользовательских датаграмм) при отправке или ответе на запрос:

- порт 161. Используется, когда NMS отправляет запросы агенту SNMP. Если требуется изменить номер порта NMS по умолчанию,

необходимо убедитесь, что номер порта, используемый для отправки запросов и агентом SNMP для ответа на запросы, одинаков;

– порт 162. Используется агентом SNMP для отправки ловушек или сообщений в NMS. При изменении номера порта требуется проверить, что он совпадает с номером порта, используемого NMS для получения сообщений traps и inform.

Управляемое устройство — это сетевой узел, содержащий SNMP-агент. Почти каждое устройство в сети (например, маршрутизаторы, коммутаторы, серверы, принтеры и т. д.) функционирует как управляемое устройство. NMS осуществляет мониторинг и контроль управляемых устройств с помощью трех команд SNMP:

– команда «read» - чтение. Используется NMS для мониторинга управляемых устройств;
– команда «write» - запись. Используется NMS для управления управляемыми устройствами;
– команда «trap» - ловушка. Используется управляемыми устройствами для сообщения о событиях в NMS.

NMS периодически опрашивает устройства, запрашивая информацию о состоянии или отправляя изменения конфигурации, когда это необходимо.

Management Information Base (MIB) или база управленческой информации — это структура данных, содержащая значения устройств локальной сети, которые можно собирать, настраивать и изменять. Это текстовый файл, описывающий все объекты данных, используемые конкретным устройством, которые можно запрашивать или контролировать с помощью SNMP. Как правило, значения в MIB включают набор статистических и управляющих значений для аппаратных узлов сети. Эти значения соответствуют возможным запросам, которые SNMP Manager может запросить у SNMP-агента. Агент собирает и хранит данные локально. SNMP-агент поддерживает базу данных, а SNMP-менеджер использует ее

для отправки или получения информации и передачи ее в NMS. Существует множество различных стандартизированных MIB, определенных IETF (Internet Engineering Task Force – инженерный совет Интернета) или ISO (International Organization for Standardization - Международная организация по стандартизации), а также собственные MIB, определенные конкретными производителями. SNMP позволяет пользователям расширять значения MIB для конкретного агента, если они используют собственные MIB.

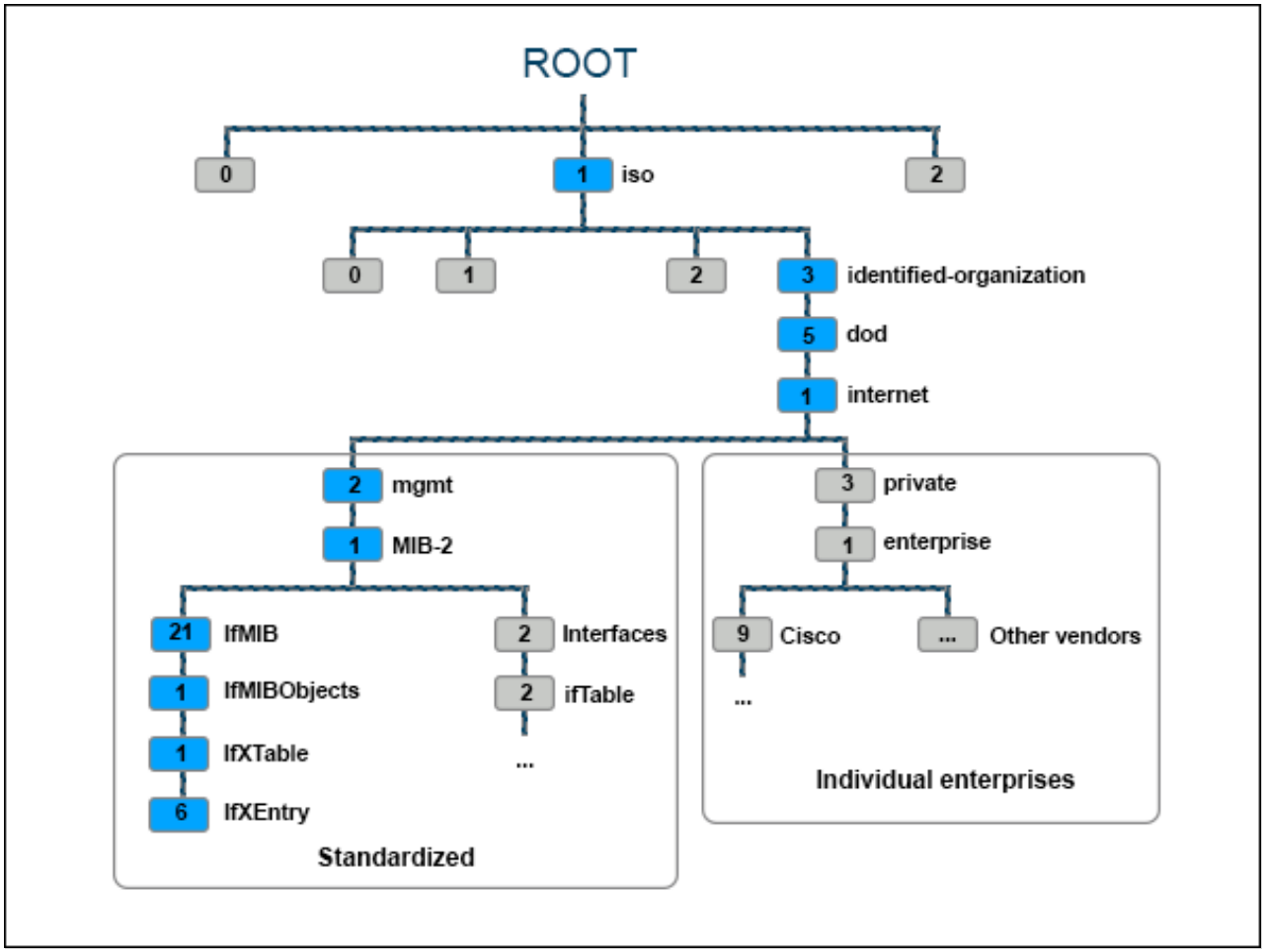


Рисунок 24- Иерархия и организация данных в MIB

Выше, на рисунке 24 показана иерархия и организация данных в MIB. Древовидная структура содержит все управляемые функции всех сетевых

устройств. Каждая ветвь имеет номер и имя, а каждый пункт называется по полному пути от вершины дерева до самого пункта.

OID (Object identifier - идентификатор цифрового объекта). MIB содержит множество управляемых объектов, идентифицируемых с помощью идентификаторов объектов (OID). OID — это числовой идентификатор MIB, используемый для различения различных устройств в базе. Система использует OID для доступа к управляемым объектам MIB.

Существует два типа управляемых объектов:

– скалярные объекты. Уникальные, определяются одним экземпляром объекта;
– табличные объекты. Определяются несколькими связанными экземплярами объектов, сгруппированными в таблицы MIB.

Каждый OID состоит из строк чисел, обозначающих управляемые объекты, разделенных точками. Идентификаторы OID организованы иерархически, в виде древовидной структуры, с отдельными идентификаторами переменных для каждого OID.

SNMP-ловушки — это сообщения, которые агент SNMP отправляет, чтобы уведомить NMS о событиях или тревогах в сетевом устройстве. Ловушки информируют сетевого администратора о состоянии и событиях устройства. Существует два типа уведомлений - «trap» и «inform». Хотя их цель одна и та же - проинформировать администратора о событии, они отличаются тем, что сообщение «inform» требует ответа от NMS, а сообщение «trap» - нет. Каждое сообщение ловушки содержит следующую информацию:

– «enterprise». Устройство, генерирующее сообщение-ловушку (источник ловушки);
– адрес агента. IP-адрес источника ловушки;
– общая ловушка. Указание типа ловушки;

– специфическая ловушка. Включает частную информацию о ловушках предприятия;
– временная метка. Указывает время, прошедшее между повторной инициализацией сетевого объекта и созданием сообщения ловушки;
– связи переменных. Список имен переменных и соответствующих им значений.

На рисунке X показана схема как работают сообщения «trap» и «inform»:

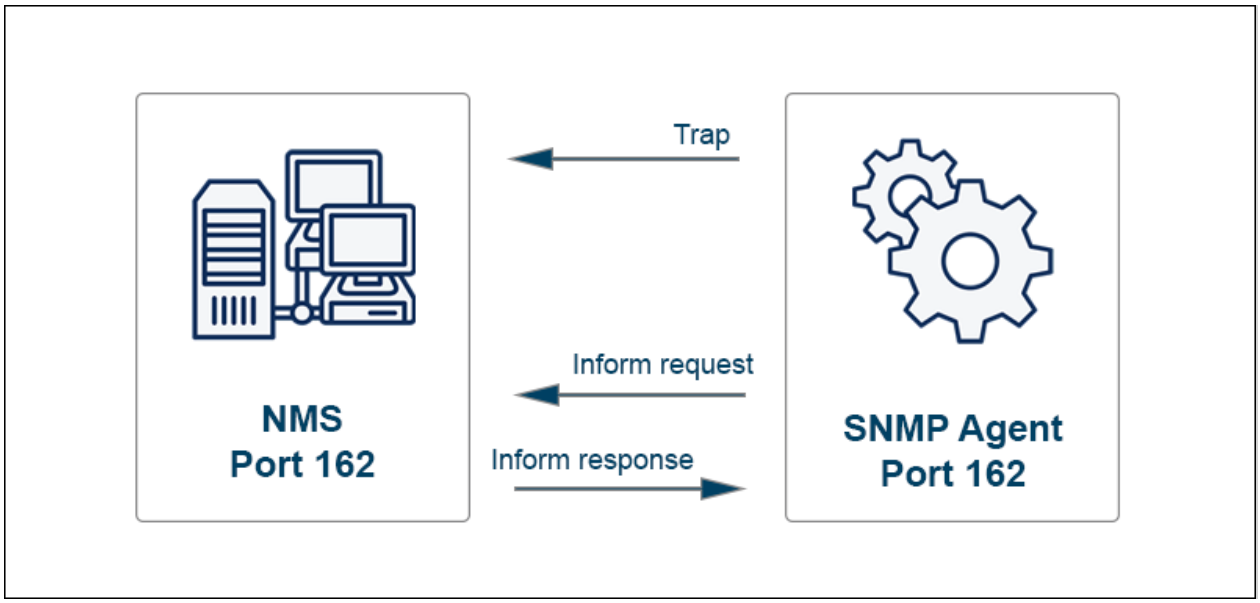


Рисунок 25 – Схема работы сообщений «trap» и «inform»

На сегодня можно выделить три основные версии SNMP. Различные версии SNMP имеют разные возможности, особенно в плане безопасности.

SNMPv1 — это самая старая и оригинальная версия SNMP, поддерживающая 32-битные счетчики. Она имеет слабые функции безопасности, идентифицируя устройства с помощью строки сообщества в открытом виде, что является устаревшим методом аутентификации. Кроме того, сетевые администраторы могут запрашивать информацию без шифрования. SNMPv1 использует некоторые стандартные учетные данные

для доступа, что позволяет легко получить конфиденциальные данные о сети. В сочетании с отсутствием шифрования это позволяет любому человеку, имеющему доступ к сети, перехватывать данные или брать на себя роль сетевого администратора, подвергая опасности всю систему.

SNMPv2 был выпущен в 1993 году и ввел усовершенствования безопасности, которые в настоящее время считаются достаточно хорошими для внутренних сетей. Однако он не должен использоваться в устройствах, предназначенных для общего пользования, поскольку его слабая система аутентификации и шифрования делает сеть уязвимой для атак. Тем не менее SNMPv2 до сих пор является наиболее распространенной версией SNMP, хотя в 1998 году ее заменила SNMPv3.

SNMPv3 отличается повышенной безопасностью, поддержкой шифрования и аутентификации данных. Последняя версия протокола также обеспечивает защиту пакетов при передаче. SNMPv3 также позволяет сетевым администраторам устанавливать аутентификацию на основе ролей, предотвращая несанкционированный доступ к важным сегментам сети. Кроме того, SNMPv3 может быть настроен на шифрование при передаче данных.

SNMP-мониторинг предоставляет данные, позволяющие отслеживать состояние сетевого устройства, что делает его идеальным для ИТ-мониторинга. Он позволяет сетевым администраторам отслеживать наиболее важные параметры системы, включая коммутаторы, точки доступа и маршрутизаторы, а также другие подключенные к сети устройства, такие как принтеры, аппаратные датчики и другие. Утилита мониторинга SNMP является центральным узлом для получения данных от агентов SNMP на контролируемых устройствах. Однако, несмотря на то что устройства содержат SNMP-агент, этот мониторинг считается безагентным, поскольку нет необходимости устанавливать программное обеспечение для мониторинга на устройства, так как производители уже реализовали протокол SNMP на устройствах. Поэтому мониторинг работает с

программным обеспечением устройства по умолчанию, не требуя дополнительных прав доступа от производителя устройства. Если вы решили использовать пользовательский агент мониторинга, необходимо установить его на систему.

Обмен информацией при SNMP-мониторинге осуществляется с помощью набора команд. Эти команды перечислены ниже:

- «get». Эта команда представляет собой запрос, отправляемый SNMP-менеджером сетевому устройству. Ее цель - получить данные от устройства;
- «getNext». Аналогична «Get», но извлекает значение следующего OID в дереве MIB;
- «getBulk». Извлекает большие объемы данных из крупных таблиц MIB. Работает путем выполнения нескольких запросов «getNext» и возвращает все в одном ответе;
- «set». Используется для изменения или присвоения значения управляемому устройству;
- «trap». SNMP-агент отправляет команду SNMP-менеджеру, информируя его о событии;
- «inform». Как и «trap», «tnform» также отправляется SNMP-агентом менеджеру, информируя о событии. Разница в том, что сообщения «inform» требуют подтверждения от SNMP-менеджера, что сообщение было получено;
- «response». Ответные сообщения передают значение или инструкции для устройства в соответствии с указаниями SNMP-менеджера.

SNMP позволяет пользователям собирать различные метрики с устройств, подключенных к сети. К таким метрикам относятся:

- время работы. Количество времени, в течение которого устройство было включено и подключено к сети;

– пропускная способность. Количество данных, переданных от источника к месту назначения за определенный промежуток времени;
– температура. Текущая рабочая температура устройства;
– ошибки интерфейса. Список ошибок, возникших во время работы устройства;
– использование процессора и памяти. Статистика производительности и ресурсов устройства.

Сетевые администраторы могут использовать инструменты SNMP-мониторинга для анализа данных, полученных с устройства, визуализации данных и получения предупреждений о превышении некоторыми метриками определенных пороговых значений. Еще одним полезным инструментом являются теги, которые позволяют упорядочивать метрики и сравнивать их по подмножествам. Сетевые администраторы используют инструменты мониторинга SNMP для управления устройствами в сети, выделения портов или их освобождения, а также для обеспечения бесперебойной работы сети и продолжительного времени безотказной работы устройств. Инструменты мониторинга требуют от администратора настройки SNMP-агента, чтобы SNMP-менеджер правильно получал данные мониторинга. Средства мониторинга автоматически обнаруживают новые устройства и запускают процесс мониторинга. Инструмент получает ключевые показатели производительности от каждого устройства и предоставляет полный обзор его работы. Инструмент позволяет администраторам настраивать пороговые значения и генерировать уведомления об определенных аномалиях. На основе данных, полученных с помощью инструментов мониторинга, сетевые администраторы отслеживают доступность и производительность сетевых устройств и оперативно выявляют любые проблемы в сети. Некоторые инструменты также предоставляют приборную панель или графики собранных данных.

Ниже приведен список различных инструментов SNMP-мониторинга, который может помочь в управлении сетью:

- SolarWinds Network Performance Monitor (NPM) — это инструмент SNMP-мониторинга, который отличается автоматическим обнаружением устройств, интеллектуальным отображением и интерактивной динамической панелью для всестороннего обзора данных;
- ManageEngine OpManager. Одной из ключевых особенностей ManageEngine OpManager является элемент обработки, который управляет до 300 сообщений-ловушек в секунду. Администратор получает организованную обратную связь, которая помогает выявить потенциальные проблемы или дефекты, а функция протоколирования показывает полный обзор сообщений-ловушек;
- сетевой монитор Paessler PRTG. Paessler PRTG предоставляет три метода мониторинга сети, включая SNMP-мониторинг. В основе PRTG лежат сенсоры - основные элементы мониторинга, каждый из которых предназначен для отслеживания определенного участка сети. Предварительно настроенные SNMP-датчики отслеживают сетевые устройства;
- инструмент SNMP-мониторинга SysAid позволяет сетевым администраторам осуществлять мониторинг сетевых устройств, автоматически определяя указанные события и оповещая о них в случае возникновения проблем. Он может отслеживать службы, процессы, доступность веб-сайтов, изменения в аппаратном или программном обеспечении, порты и т. д.;
- Atera — это инструмент SNMP-мониторинга, поддерживающий неограниченное количество рабочих станций и серверов. Инструмент отслеживает использование и производительность приложений, активность пользователей, генерирует отчеты и

регистрирует сообщения SNMP-ловушек. Он имеет систему оповещений в реальном времени и позволяет получить удаленный доступ. Прозрачная и гибкая система ценообразования, основанная на техническом обслуживании.

Протоколы на основе Ethernet. Промышленные протоколы Ethernet отличаются от стандартных усиленным экранированием. Они обеспечивают постоянную передачу небольшого объема данных. Это нужно для взаимодействия контроллеров, используемых в автоматизированных промышленных системах. С помощью протоколов Ethernet обеспечивается бесшовная интеграция в стандартные сети и системы, решаются следующие задачи:

- организация системы информирования;
- визуализация топологии сети;
- передача информации от устройств сети в центр ее сбора;
- синхронизация работы агрегатов.

Они поддерживают широкий спектр устройств, предоставляют доступ к гибким сетевым топологиям для плавной интеграции в системы. С помощью протоколов Ethernet обеспечивается масштабируемость и гибкость сетей, а также детерминированная и недетерминированная коммуникация. Они подходят для выполнения операций, которые чувствительны к скорости проведения.

Протоколы Ethernet совместимы с разными устройствами, что делает их практичными и удобными в использовании. Они поддерживают приложения, которые отличаются высокой производительностью.

EtherCAT. Этот протокол отличается быстродействием, обеспечивает обмен данными между узлами, которые размещены на большом расстоянии друг от друга. Для передачи информации используются стандартные фреймы Ethernet, поэтому протокол является универсальным, его поддерживает оборудование разных производителей. Высокая скорость передачи пакетов данных обеспечивается за счет одновременного отправления их на все

сопряженные узлы и точки. Независимо от особенностей топологии локальной сети, EtherCAT формирует кольцо. Так обеспечивается последовательность передачи данных. Протокол реализуется на базе гигабитных или оптических линий.

CAN. Это универсальный протокол, который не привязан к определенному производителю оборудования. Он позволяет размещать на линии несколько ведущих устройств, отличается отказоустойчивостью. Поэтому используется в промышленности для автоматизации производственных процессов. Скорость передачи данных достигает 1 Мбит/с.

Она зависит от следующих факторов:

– емкости передающих линий;
– количества абонентов;
– расстояния, на которые передаются данные.

Протокол использует различные методы обнаружения ошибок, информирования об их наличии. При столкновениях на шине исключается потеря информации. Это контроль формы пакета данных, а также:

– поразрядный контроль;
– проверка пакета полиномом CRC;
– прямое заполнение битового потока.

С помощью протокола организуется передача данных в сложных условиях. Он обладает многочисленными преимуществами, отличается гибкостью конфигурации. К наиболее значимым плюсам относится ретрансляция разрушенных сообщений, автономное отключение поврежденных узлов, присвоение приоритета каждому пакету данных. Помимо универсальных протоколов таких, как CAN и EtherCAT существуют разработки производителей коммутационного оборудования.

Протокол VLAN. С помощью этого протокола обеспечивается независимость логической топологии сети от физической. Он позволяет

разделять устройства на группы, которые не взаимодействуют друг с другом, но имеют доступ к серверу. Это означает, что локальную сеть можно упорядочивать в соответствии с текущими требованиями путем разделения сетевых приложений.

Кроме того, протокол позволяет устанавливать приоритетность. Это означает, что можно улучшать качество определенных каналов связи, например, телефонии или передачи видео, голосовых сообщений. VLAN повышает безопасность локальных сетей, упрощает управление ими. С его помощью сокращается объем широковещательного трафика. Для разделения сетевых устройств на группы не нужно дополнительно покупать коммутаторы. Достаточно настроить уже имеющееся оборудование. Для его конфигурирования через стандартные ОС потребуется установка специальных драйверов.

Протоколы маршрутизации OSPF и BGP. Протокол BGP обеспечивает связь между локальными сетями, а OSPF, – между компонентами внутри них. Последний ищет кратчайший путь доставки информации, обеспечивает быстрые переходы в случае сбоев. При этом протокол BGP разработан для глобальной маршрутизации. Он используется крупными компаниями Интернет-провайдерами, требует тонкой и правильной настройки. OSPF используется внутри локальных сетей.

Контроль работы ИБП через web-интерфейс. Некоторые модели ИБП и стабилизаторов напряжения имеют специальный функционал, позволяющий организовывать дистанционный мониторинг их состояния через web-интерфейс. При этом подключение к прибору может осуществляться с помощью практически любого имеющего выход в интернет-устройства, даже смартфон. Web-интерфейс ИБП или стабилизатора представляет собой генерируемую устройством web-страницу (посредствам протокола HTTP), которая отображает его основные параметры и позволяет менять некоторые настройки (в частности, настройки сетевого подключения: IP адрес, адрес

шлюза, DNS-сервер). Стоит отметить, что открываться такая web-страница может практически в любом интернет-браузере, однако рекомендованы:

- Opera (версия не ниже 12);
- Chrome и его клоны;
- Microsoft Edge.

Удаленный мониторинг через web-интерфейс в первую очередь необходим ИБП и стабилизаторам, которые питают критических потребителей, в особенности, если рядом с ними постоянно не находится отслеживающий их состояние человек. Примером критических потребителей является отопительное оборудование в частном доме или работающая в непрерывном режиме компьютерная техника на промышленном предприятии. Для того чтобы устройство (ИБП или стабилизатор) можно было контролировать по web-интерфейсу, оно должно обладать возможностью соединения с IP-сетью через протокол TCP/IP. Дают такую возможность Ethernet разъемы или слоты для установки карт мониторинга с такими разъемами.

2.2 Недостатки и меры по улучшению дистанционного управления ИБП

Для исследования и сравнения методов дистанционного контроля резервного питания рассмотрим следующие ключевые методы в таблице 3.

Таблица 3 - Методы дистанционного контроля

№	Метод дистанционного контроля	Описание метода	Преимущества	Ограничения
1	SNMP (Simple Network Management Protocol)	Стандартный протокол для мониторинга и управления сетевыми устройствами. Протокол SNMP предоставляет широкие возможности для мониторинга сетевых устройств и в том числе резервного питания. Он имеет низкую стоимость реализации, но может потребовать дополнительных настроек для обеспечения безопасности.	Широкая поддержка, стандартизация, простота настройки.	Недостаточная безопасность, ограниченный функционал.

Продолжение таблицы 3

№	Метод дистанционного контроля	Описание метода	Преимущества	Ограничения
2	Modbus TCP/IP	Протокол передачи данных для промышленной автоматизации. Modbus TCP/IP обеспечивает высокую скорость передачи данных и простоту интеграции с различными протоколами. Он широко применяется в промышленных средах и обеспечивает надежную связь между оборудованием и системами мониторинга.	Высокая скорость передачи данных, простота интеграции, применим в промышленных средах.	Сложности в конфигурации в сложных сетевых топологиях.

Продолжение таблицы 3

№	Метод дистанционного контроля	Описание метода	Преимущества	Ограничения
3	Web-based monitoring	Мониторинг и управление через веб-интерфейс для удобного удаленного доступа. Modbus TCP/IP обеспечивает высокую скорость передачи данных и простоту интеграции с различными протоколами. Он широко применяется в промышленных средах и обеспечивает надежную связь между оборудованием и системами мониторинга.	Удобный доступ через веб-браузер, интуитивно понятный интерфейс.	Зависимость от интернет-соединения, ограниченный контроль за безопасностью данных.

Анализ различных методов дистанционного контроля резервного питания показал, что каждый имеет свои преимущества и ограничения, а также необходимо постоянно работать по защите, улучшению работы дистанционного управления ИБП. SNMP отлично подходит для сложных систем мониторинга, Modbus TCP/IP обеспечивает высокую скорость передачи данных, а веб-мониторинг предоставляет удобство визуализации.

К общим недостаткам дистанционного контроля резервного питания, можно отнести: возможность сбоев в соединении, уязвимость к кибератакам, зависимость от интернет-соединения, сложность настройки и обслуживания и др.

Проанализировав недостатки дистанционного контроля резервного питания, можно предложить следующие меры по улучшению дистанционного управления ИБП:

- создание резервного канала связи для обеспечения непрерывной связи при возможных сбоях основного канала;
- регулярное обновление ПО, установка антивирусов, использование механизмов шифрования данных и многофакторной аутентификации для защиты системы от кибер-угроз;
- создание предварительно настроенных автоматических сценариев действий для быстрого реагирования на типичные события или проблемы, что позволит сократить время реакции и минимизировать человеческий фактор;
- дистанционная поддержка, удаленный доступ к экрану и управление системой через интернет для оперативного решения;
- использование искусственного интеллекта для анализа поведения системы ИБП, выявления аномалий и автоматического реагирования на возникающие проблемы;
- установка дополнительной резервной системы энергоснабжения для обеспечения бесперебойной работы дистанционного управления в случае сбоев основного источника.

Дистанционное управление системой резервного питания становится все более важным элементом в обеспечении стабильности энергоснабжения и защите оборудования от сбоев в энергопитании. Эта технология помогает снизить риски и обеспечить бесперебойную работу критически важных систем. Выбор подходящего метода дистанционного контроля ИБП зависит

от специфики организации, конкретных потребностей и требований системы резервного питания.

3 Разработка системы удаленного мониторинга и оценки работы ИБП.

Основным источником питания ИБП является свинцово-кислотная батарея с регулируемым клапаном. В настоящее время существующее оборудование контролирует общее напряжение и ток, но оно не может контролировать параметры отдельной батареи, такие как напряжение, емкость, сопротивление, определять неисправность батареи, которая появляется после сбоя. Также отсутствует возможность предоставления информации о неисправности и напоминание персоналу о необходимости своевременной смены батареи.

Когда в городской сети происходят скачки напряжения или отключение электроэнергии, это может привести к разряду аккумулятора или к её выходу из строя, тем самым нет гарантий нормальной работы системы ИБП, что может привести к негативным последствиям. Например, сообщение о городском отключении электроэнергии не уведомит администратора, до того, как разрядится аккумулятор, из-за этого невозможно будет своевременно отключить все виды сетевого оборудования, что может привести к сбою программного обеспечения, потере или повреждению системных данных, всё это влияет на повседневную работу и наносит серьезные убытки предприятию. Следовательно, необходимо внедрить управление системой ИБП для онлайн-мониторинга, посредством удаленного мониторинга в режиме реального времени, чтобы отслеживать рабочее состояние батареи, степень её износа, а также своевременного сигнал о неисправностях, для продления срока службы батареи ИБП. Программное обеспечение может выполнить оценку оставшегося заряда и неисправности батареи, чтобы обеспечить стабильную работу ИБП.

Для реализации связи и настройки теста передачи данных о состоянии аккумуляторных батарей ИБП на рисунке 26, показана схема системы передачи данных. Через интерфейсы RS-485 на местные инженерные

станции передаются и контролируются сетевые данные батареи ИБП, в свою очередь, программная система инженерной станции, через сеть, передает данные, которые необходимы для отображения и мониторинга в режиме реального времени, в платформу удаленного мониторинга, которая обеспечивает дистанционный контроль состояния батареи и подачу сигналов.

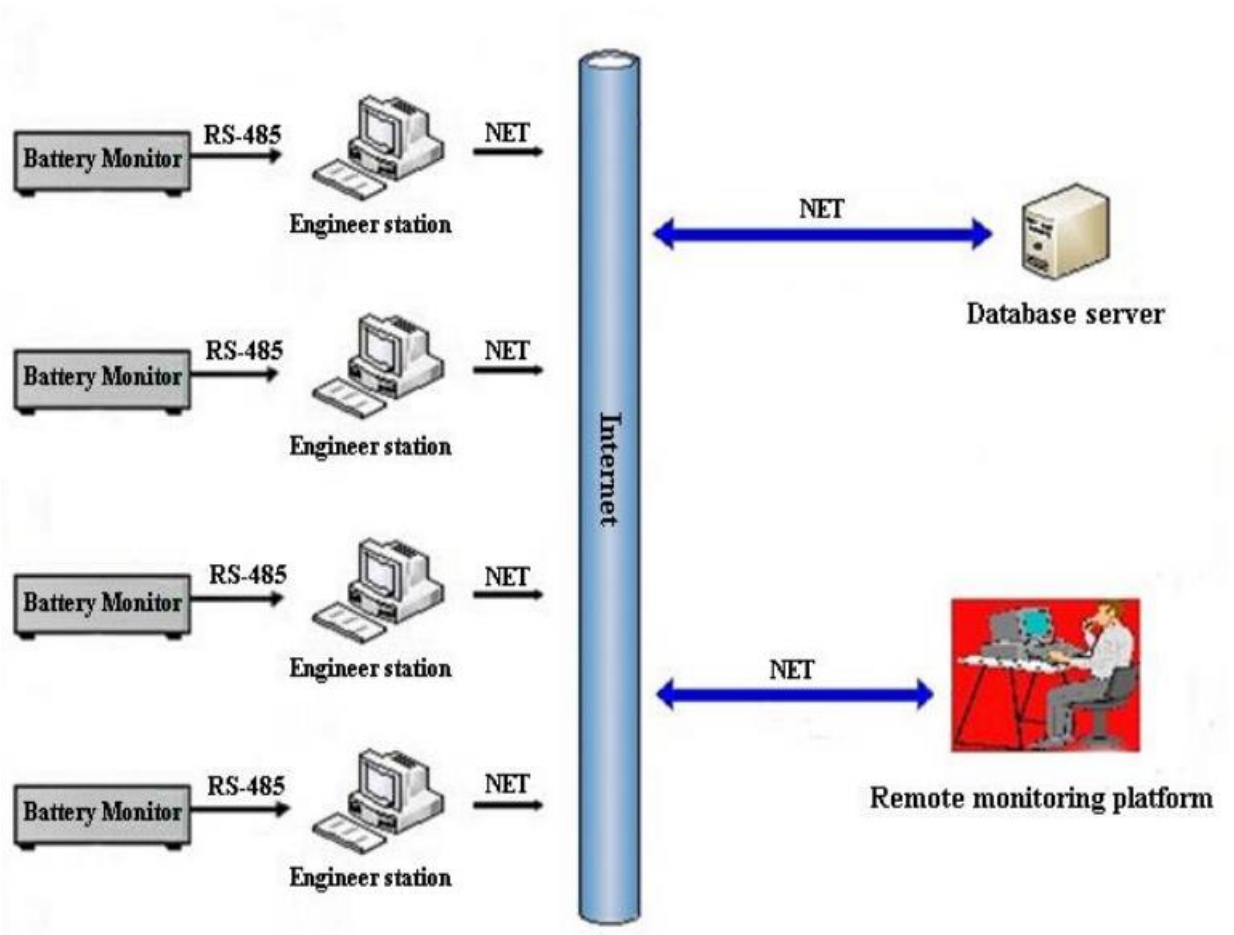


Рисунок 26 - Схема системы передачи данных.

Подключение батареи и системы мониторинга выполняется через модуль связи 485, платформа программного обеспечения в качестве языка разработки использует C++, которая используется в промышленной сфере.

Путем настройки IP-адреса, маски подсети, шлюза, настройки скорости передачи последовательного порта, битов данных, стоп-битов, номера

локального порта в соответствии с программой передачи MCU (Multipoint Control Unit), необходимо организовать прием и передачу данных.

При передаче байтовых данных мониторинга батареи, информация преобразуются в данные, которые необходимо отобразить. Данные отображаются в программном обеспечении локальной системы мониторинга в режиме реального времени, инженеры могут отслеживать и передавать данные о состоянии батареи в базу, чтобы персонал, осуществляющий мониторинг, мог удаленно отслеживать состояние каждой батарет. Схема локальной системы мониторинга в режиме реального времени показана на рисунке 27.

Рисунок 27 - Схема локальной системы мониторинга
в режиме реального времени

Система должна обеспечивать нормальную работу DS (local engineering station monitoring software - программное обеспечение для мониторинга локальных инженерных станций) и системы веб-приложений, которые могут взаимодействовать и открывать указанный TCP-порт (протокол управления передачей). Когда веб-приложение запускается, устанавливается связь через TCP. DS через TCP соединение, направляет данные, которые поступают с источника в сеть. Код подключения, следующий:

DataSource.username=sa

DataSource.password=snow

data.dbCreate=update

tcpservice.port=8888

Через код подключения tcpservice.port, начинается обработка и передача данных. С помощью коммуникационного протокола, данные преобразуются в формат, который требуется веб-приложению, и сохраняются в базе. Схема системы удаленного онлайн -мониторинга показана на рисунке 28.

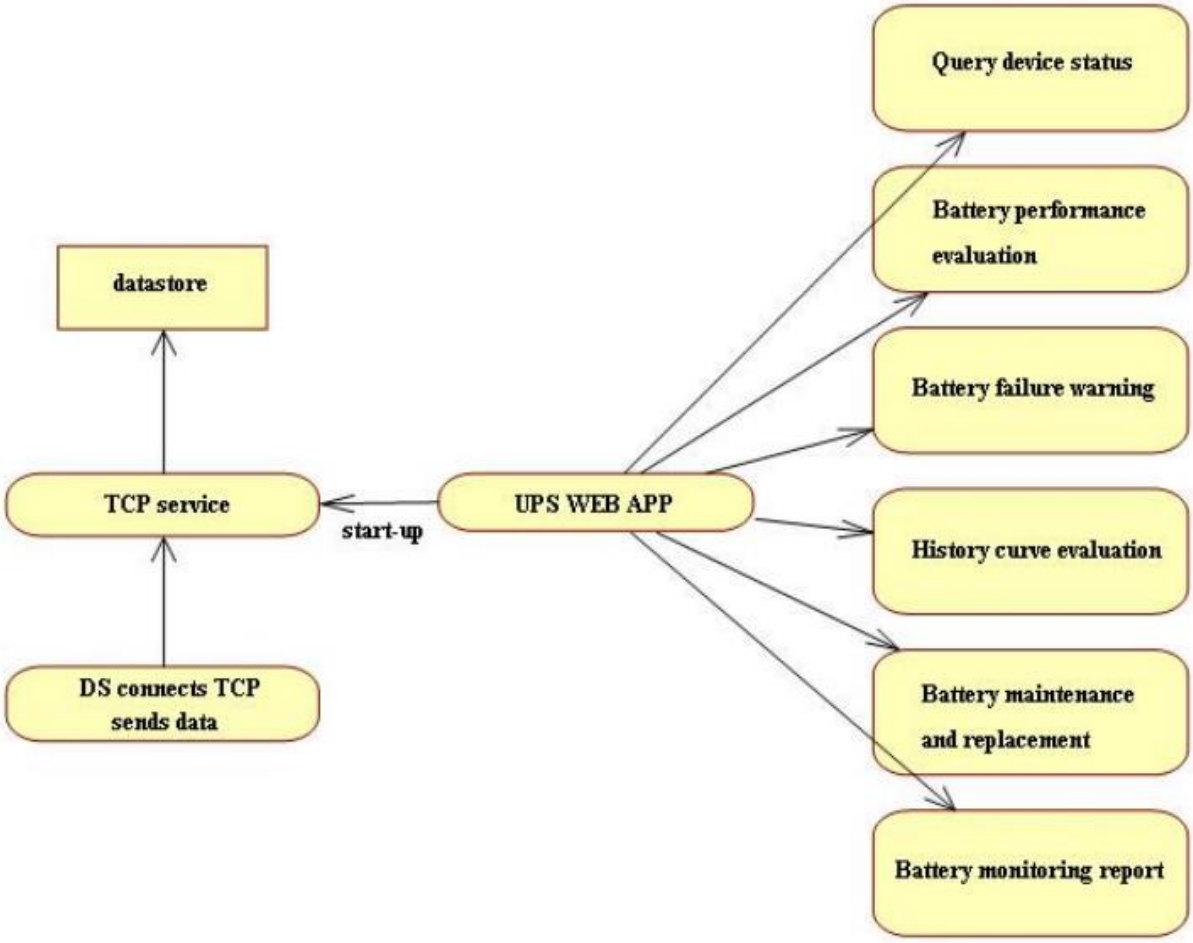


Рисунок 28 - Схема системы удаленного онлайн -мониторинга

На рисунке 29 показано проектирование процесса разработки программного обеспечения удаленной системы, включающее инициализацию веб-программы и программного обеспечения DS, завершение

передачи данных для отображения данных в системе удаленного мониторинга.

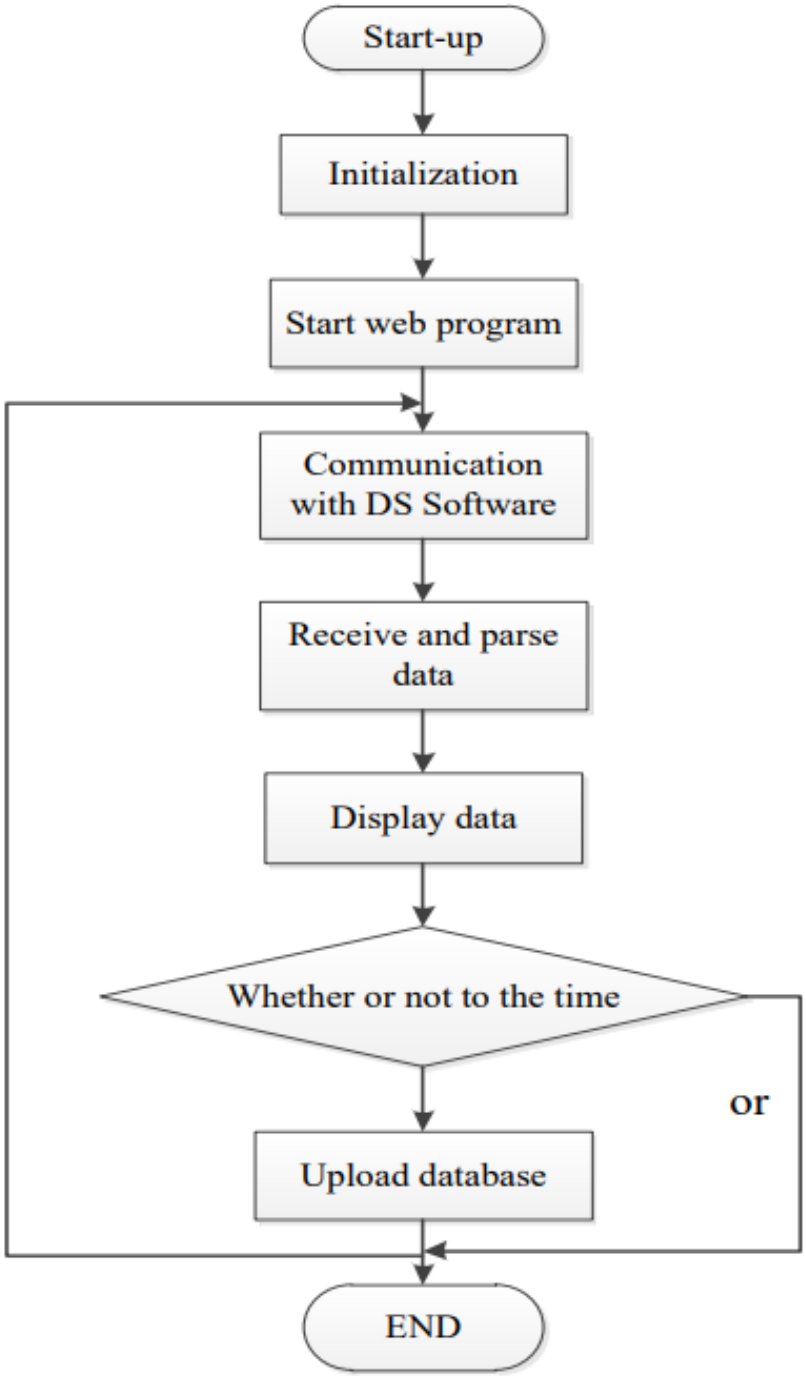


Рисунок 29 - Процесс разработки программного обеспечения удаленной системы

Состояние, производительность батареи измеряется в основном через показатели SOC и SOH. State of Health (SOH) — степень работоспособности

аккумулятора, отражающая текущее состояние аккумулятора по сравнению с его идеальным состоянием. State of Charge (SOC) — уровень заряда аккумуляторной батареи, где 0% это полностью разряжен, а 100% полностью заряжен. При зарядке и разрядке SOH демонстрирует тенденцию к снижению. В настоящее время исследовательские идеи SOH основаны на механизме старения батареи в циклах, процесс деградации в электрохимической системе при каждом её заряде и разряде. Каждый цикл уменьшает ёмкость аккумулятора (количество накапливаемой энергии) и мощность (скорость отдачи энергии), через N-циклов достигается критическая точка, когда аккумулятор уже не может удовлетворять требованиям устройства. Таким образом, система удаленного мониторинга использует данные о напряжении U и сопротивлении R батареи в реальном времени, которые передаются через программное обеспечение DS. Чтобы персонал мог контролировать состояние батареи, значения SOC и SOH отображаются на интерфейсе удаленного мониторинга.

Для оценки SOC используется следующая формула:

$$SOC = \frac{U_{now} - U_{min}}{U_{max} - U_{min}} \times 100\% \quad (4)$$

где U min – минимальное напряжение одиночной батареи, В;

U max – максимальное напряжение одиночной батареи, В;

U now – текущее напряжение батареи, В.

Процесс старения батареи часто сопровождается изменениями внутреннего сопротивления батареи, поэтому можно оценить состояние работоспособности батареи по внутреннему сопротивлению батареи, внутреннее сопротивление батареи указывает на то, что батарея разряжена.

Для оценки SOH используется следующая формула:

$$SOH = \frac{R_{now} - R_{new}}{R_{old} - R_{new}} \times 100\% \quad (5)$$

где R new – внутреннее сопротивление новой батареи, Ом;

R old – полная устойчивость батареи к старению, Ом;

R now – внутреннее сопротивление батареи, Ом.

Код, зависящий от реализации, для системы показан на рисунке 30.

```
g_CurrentBatData[m_nArkID].BatteryData[k].dwSOC = (g_CurrentBatData[m_nArkID].BatteryData[k].Voltage
    -g_nSVoltageMin[m_nDeviceID])*100/(double)(g_nSVoltageMax[m_nDeviceID]-g_nSVoltageMin[m_nDeviceID]);

g_CurrentBatData[m_nArkID].BatteryData[k].dwSOH = (g_CurrentBatData[m_nArkID].BatteryData[k].Resistance
    -g_nSResistanceNew[m_nDeviceID])*100/(double)(g_nSResistanceOld[m_nDeviceID]-g_nSResistanceNew[m_nDeviceID]);
```

Рисунок 30 - Код зависящий от выполнения.

С помощью анализа моделирования кривой данных в режиме реального времени можно определить данные отдельной батареи. Например, по номеру сигнала батарее от 1 до 10, соответственно, моделируются напряжение одиночной батареи и кривая SOC, сопротивление одиночной батареи и кривая SOH, как показано на рисунке 31 и рисунке 32.

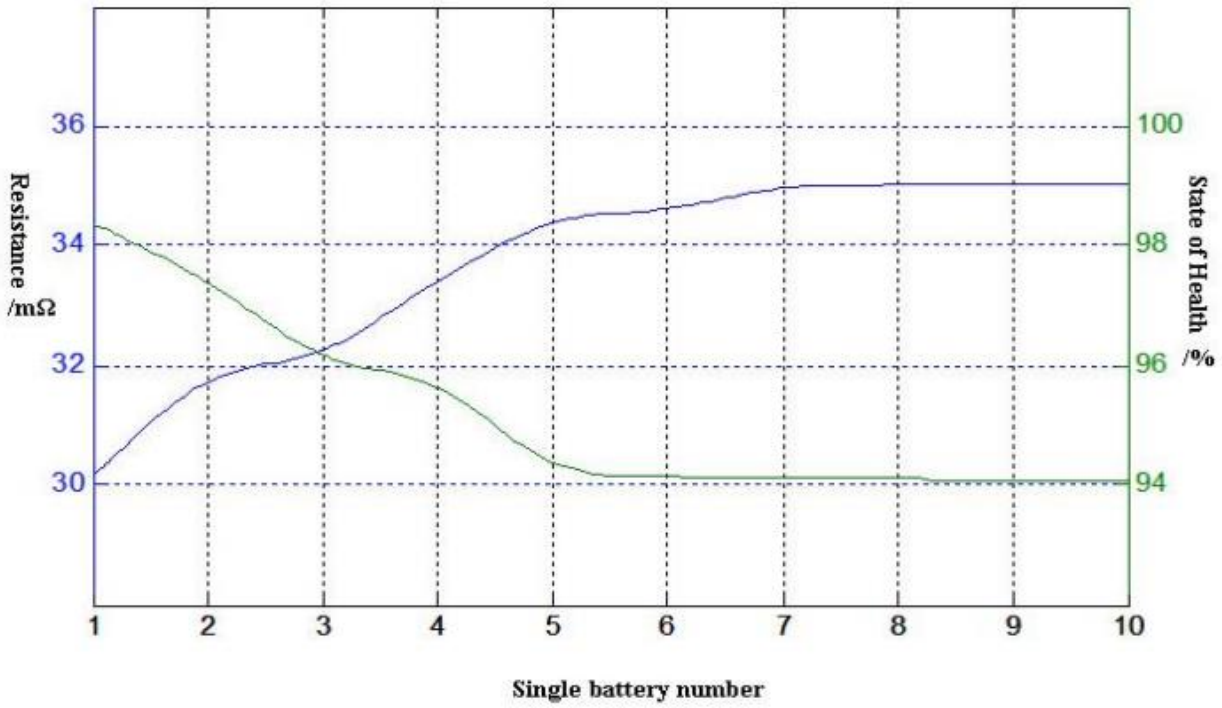


Рисунок 31 - Кривая сопротивления и SOH.

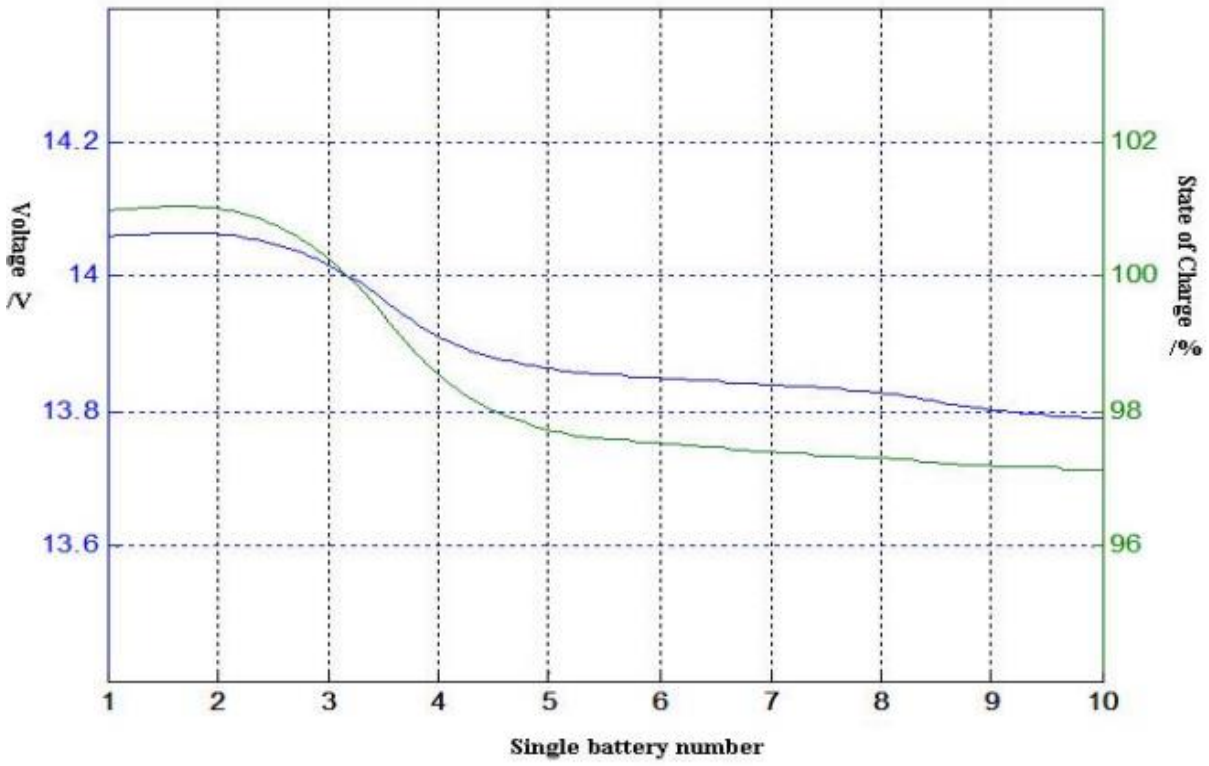


Рисунок 32 - Кривая напряжения и SOC.

Как видно из рисунка, оставшийся заряд отдельной батареи сигнала от 1 до 10 соответствует SOC> 50%, аккумулятор используется, имеет незначительный разряд.

В соответствии со стандартом IEEE1188-1996, SOH>80% объясняют, что батарея находится в исправном состоянии, SOH батареи, свидетельствующий о состоянии здоровья, составляет более 90%, иллюстрируя значения на сигналах от 1 до 10, батарея находится в исправном состоянии, эта система мониторинга может оценить работоспособность батареи.

Система обеспечивает последовательную и параллельную передачу данных по локальной и глобальной сети, четыре интерфейса мониторинга и управления, открытые коммуникационные интерфейсы, подходят к различным требованиям сетевых ресурсов (RS232, WIFI, RS485, TCP / IP и т.д.), обеспечивая оперативный мониторинг каждой батареи. А используя

единое управление базой данных, в которой хранится вся история данных мониторинга, можно своевременно анализировать и оценивать степень износа аккумулятора. Такие параметры, как напряжение батареи, внутреннее сопротивление, температура окружающей среды и другие, могут быть оценены профессионально и синтетически, что позволяет определить, разрядилась ли батарея. Практика показывает, что система может эффективно отслеживать параметры состояния батареи.

Заключение

Существуют критически важные телекоммуникационные системы, на которые мы полагаемся каждый день, чтобы вести бизнес, спасать жизни и выполнять повседневных задач. Наши предприятия, наши системы реагирования на чрезвычайные ситуации, медицинские учреждения и даже наши дома - все они зависят от бесперебойного источника чистой энергии. Эти телекоммуникационные системы работают на множество единиц электронного оборудования - компьютеры, серверы, узлы локальных сетей и т. д. - и это оборудование должно работать непрерывно. Перебои в подаче электроэнергии наносят ущерб коммерческих и правительственных организаций - отключения, перебои, скачки и перепады напряжения вот лишь некоторые прерывания, от которых защищает ИБП.

Современный мир почти полностью зависит от электричества, а также существуют природные и экологические условия, а также человеческие ошибки, которые приводят к перебоям в подаче электроэнергии. Внезапное отключение электроэнергии нарушит работу большинства деловых, правительственных и коммерческих и правительственных операций. Существует множество примеров, когда компании ликвидируются в результате отключения электричества сбоев. Однако не только полное отключение электричества не только полные сбои или "блэкауты", которые могут привести к разрушительные последствия. Дистанционный контроль ИБП (источника бесперебойного питания) позволяет оперативно управлять и мониторить работу ИБП на расстоянии. Это может включать в себя возможность удаленного включения/выключения ИБП, мониторинг статуса батарей, управление настройками работы и многие другие функции. Такой контроль обеспечивает оперативную реакцию на любые проблемы с электроснабжением и помогает поддерживать стабильную работу оборудования, подключенного к ИБП.

Существует огромное множество ИБП от разных производителей с разными характеристиками. Выбор конкретного ИБП будет зависеть от многих факторов и задач, которые планирует решить компания. Размер нагрузки, какое оборудование предполагается защитить, финансовые возможности предприятия, частота отключения электроэнергии и много другое влияет на выбор ИБП.

Формирования единой систем контроля и управления ИБП может быть реализовано по-разному, используя разные протоколы для передачи данных. Каждый протокол имеет свои особенности, достоинства и недостатки. Компания должна определиться с помощью какого протокола будет реализована связь между электроприборами и ИБП, так как переделывание системы на другой вид протокола дорогостоящее мероприятие и занимает много времени. В ходе практической работы была разработана и предложена схема удаленного доступа, которая может быть применена в организации для своевременного отслеживания износа батареи ИБП, что позволяет не потереть важные данные, организовать контроль и управление ИБП, своевременно получать данные о состоянии АБ и помогает увеличит срок их службы. ИБП — это простой и эффективный способ обеспечения работоспособности нашего мира.

Список используемой литературы и используемых источников

1. Лапко И.А., Ковалева В., Валынчиков В., Автомобильный рынок России в 2023 году – стагнация или адаптация? от июля 2023 : [Электронный ресурс]. URL: https://www.ra-national.ru/wp-content/uploads/2023/07/rynok_avto_2023.pdf (дата обращения 12.03.2023).

2. Приказ Министерства энергетики РФ от 28 февраля 2023 г. N 108 "Об утверждении схемы и программы развития электроэнергетических систем России на 2023-2028 годы" [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/406404497/ (дата обращения 15.04.2024).

3. Системы резервного электропитания — применение и варианты исполнения от 08 июня 2017 : [Электронный ресурс]. URL: https://enext.md/press/articles/Sistemy-rezervnogo-elektropitaniya-primenenie-i-varianty-ispolneniya (дата обращения: 14.03.2024).

4. Мочар В.Ю. Тренды российского рынка ИБП от 8 ноября 2023 : [Электронный ресурс]. URL: https://www.itbestsellers.ru/reviews/detail.php?ID=54884 (дата обращения: 14.03.2024).

5. UPS static uninterruptible power suppliers, EXB21082 - September 2021 : [Электронный ресурс]. URL: https://ups.legrand.com/media/document/ups-technical-guide-en.pdf (дата обращения 25.03.2024).

6. J. Kurtz, G. Saur, S. Sprik, and C. Ainscough; «Backup Power Cost of Ownership Analysis and Incumbent Technology Comparison» Technical Report NREL/TP-5400-60732, National Renewable Energy Laboratory : [Электронный ресурс]. URL: https://www.nrel.gov/docs/fy14osti/60732.pdf (дата обращения: 15.03.2024).

7. Типы источников бесперебойного питания от 25 марта 2019 : [Электронный ресурс]. https://www.shtyl.ru/support/articles/tipy-istochnikov-besperebojnogo-pitaniya/ (дата обращения 01.03.2024).

8. Удаленный мониторинг и управление ИБП : [Электронный ресурс]. https://www.a-energy.ru/article/monitoring-ibp-si/ (дата обращения 15.04.2024).

9. Заручевский Я.А., Терехов В.Г, Гончаренко В.А. «Система дистанционного контроля резервного электропитания объектов информационной инфраструктуры железных дорог» Intellectual Technologies on Transport. 2023. No 1. DOI: 10.24412/2413-2527-2023-133-15-20.

10. Обзор современных протоколов промышленной автоматизации — Modbus, Profinet, EtherCAT и др. от 10 августа 2023 : [Электронный ресурс]. URL: https://odinelectric.ru/industry-automation/promyshlennye-protokoly-obzor (дата обращения: 10.03.2024).

11. Протокол управления SNMP от 12 января 2021 : [Электронный ресурс]. URL: https://selectel.ru/blog/snmp/ (дата обращения: 10.03.2024).

12. ABB library. Low-power UPS product catalog : [Электронный ресурс]. URL: https://library.abb.com/d/4NWP104969R0001_EN (дата обращения 10.05.2024).

13. Ahmad Omrani, Majid Dehghani, Mohammad Reza Yousefi; «Design and Implementation a Single-Phase UPS Based on Microcontroller with AVR at Input and Full-Bridge Inverter at Output for Improving Sinusoidal Output Voltage», Signal Processing and Renewable Energy, December 2021 : [Электронный ресурс]. URL: https://research.iaun.ac.ir/pd/mr-yousefi/pdfs/PaperM_6870.pdf (дата обращения 26.03.2024).

14. Федоров С.Д., Облакевич С.В., Основные схемотехничекие решения при проектировании систем гарантированного электроснабжения, «Электропанорама». 2000.- № 3, 4, с. 23-28.

15. Источники бесперебойного питания: [Электронный ресурс]. URL: http://i.cons-systems.ru/u/a5/c0af8c029e11e3a4b9605af3284aaa/-/ИБП%20%28учебник%29.pdf (дата обращения 20.04.2024).

16. Лаврус В.С. Источники энергии//"Наука и Техника", Киев, 1997г. 200 с.

17. Цыркин М.И., Гольдинер А.Я., Тюляков К.А., Соколов С.В. Система «ДЭС-ИБП». Согласование работы дизельной электростанции (ДЭС) и источника бесперебойного питания (ИБП). Двигателестроение, №4, 2000г., с. 18-21.

18. Кромптон Т. Первичные источники тока. М.: Мир, 1986. - 326с.

19. Кромптон Т. Вторичные источники тока. М.: Мир, 1985. - 301с.

20. Modbus Organization, «Modbus application protocol specification V1.1b3», April 26, 2012 : [Электронный ресурс]. URL: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf (дата обращения 10.04.2024).

21. Системы бесперебойного питания [Электронный ресурс]. URL: https://www.sekventa.ru/service/system-power.html (дата обращения 29.04.2024).

22. Кашкаров, А. П. Все об источниках питания. Энциклопедия радиолюбителя / А.П. Кашкаров. - М.: ДМК Пресс, 2019. - 184 с.

23. Стандарты и протоколы, используемые в промышленных коммутаторах [Электронный ресурс]. URL: https://consteel-electronics.ru/standarty-i-protokoly-ispolzuemye-v-promyshlennyh-kommutatorah (дата обращения 01.05.2024).

24. Соколов С.В. Создание системы бесперебойного питания (ИБП/UPS) с большим временим автономной работы. Экономическая целесообразность и технические проблемы.

25. Кузмина О., о совместной работе ДГУ и ИБП, Сети и бизнес, №2(3), 2002, с. 25-27.

26. T.Kataoka, Y. Fuse, D. Nakajima, S. Nishikata A three-phases Voltage-type PWM Rectifier with the Function of an Active Power Filter, Proc. Power Electronics and Variable Speed Drives, 2000, p. 10.

27. Климов В.П. современные направления развития силовых преобразователей переменного тока, Электронные компоненты, №3, 2008г. стр. 26-31.

28. Климов В.П., Климова С.Р. Энергетические показатели ИБП переменного тока, Электронные компоненты, №4, 2004г. стр. 21-25.

29. Контроль работы ИБП и стабилизатора напряжения через web-интерфейс [Электронный ресурс]. URL: https://www.shtyl.ru/support/articles/kontrol-raboty-ibp-i-stabilizatora-cherez-web-interfejs/ (дата обращения 01.02.204).

30. Three Ways to Maximize UPS System Performance, June 14, 2022 by CyberPower [Электронный ресурс]. URL: https://www.cyberpowersystems.com/blog/three-ways-to-maximize-ups-system-performance/ (дата обращения 15.05.2024).

31. Zhi Yuan, Weiqing Wang & Shan He, Application of sustainable computing based advanced intelligent powerelectronic technology for smart grid systems International Journal of Computers and Applications, Published Online: 15 Feb 2019.

32. Лопухин А.А., Источники бесперебойного питания без секретов, М.: «А и Т системы», 2000.

33. Ковалева Ф.И., Рябчицко М.В., Силовая электроника: краткий энциклопедический словарь терминов и определений - М.: Издательский дом МЭИ, 2008. - 90 с.

34. Битюков В. К., Симачков Д. С., Бабенко В. П., Источники вторичного электропитания: учебник /- 4-е изд. - Москва ; Вологда : Инфра Инженерия, 2020. - 376 с. ISBN 978-5-9729-0471-6.

35. Гамазин С.И., Пупин В.М., Марков Ю.В. Обеспечение надежности электроснабжения и качества электроэнергии./ Промышленная энергетика.2006-№ 11.- С. 51-56.

36. Абакумова Ю.П. Химические источники тока. СПб: СПбГУПС, 2004. -26с.

37. Воробьев А.Ю. Влияние ИБП на систему электроснабжения, Вестник связи, №7, 2006г., с. 35-38.