Мониторинг и предикативная аналитика для систем бесперебойного питания и аккумуляторных батарей

И.Н. Моисеев, Д.Е. Намиот, А.Н. Чеботарев

***Аннотация*—В настоящей статье описан отечественный программно-аппаратный комплекс (ПАК) Многофункциональный контроллер (МФК) Абсолайт-ПРО. Это оригинальная разработка компании Абитех-Про, предназначенная для мониторинга работы источников бесперебойного питания (ИБП) и аккумуляторных батарей (АКБ). В работе описана архитектурная модель, программное обеспечение и схема применения ПАК для задач мониторинга и предикативной аналитики. ПАК поддерживает опрос отслеживаемых устройств по SNMP и Modbus. Собранные параметры могут храниться как на самом ПАК, так и выгружаться для последующей визуализации и анализа во внешние базы данных. ПАК может использовать различные сетевые подключения для передачи собранных данных, включая использование GSM-модема. В последнем случае вся система мониторинга будет полностью изолирована от сети предприятия, где установлены ИБП и АКБ.**

***Ключевые слова*—ИБП, АКБ, SNMP, Modbus, мониторинг**

I. Введение

Для критических информационных (производственных) систем, где сбои и простои недопустимы, источники бесперебойного питания (ИБП) и аккумуляторные батареи (АКБ) играют роль системы жизнеобеспечения. Простое игнорирование их текущего состояния – это фундаментальная ошибка, которая рано или поздно приведёт к катастрофическим последствиям [1].

Любой ИБП - это именно то устройство, которое призвано спасать как технологические процессы, так и само оборудование в аварийной ситуации. Именно поэтому собственная авария ИБП и может стать фатальной. При этом аккумуляторные батареи, особенно в больших массивах, характерных для мощных промышленных ИБП, например, в датацентрах, являются самым уязвимым местом всей системы. Они стареют, перегреваются, теряют ёмкость, при этом их состояние может значительно варьироваться даже в пределах одной цепочки (линейки). Когда критическая нагрузка переключается на ИБП, то неисправный или разряженный аккумулятор становится может, например, сократить время автономной работы и, соответственно, воспрепятствовать сохранению данных, корректной остановке процессов и т.д.

Мониторинг решает эту проблему на корню. Позволяя отслеживать напряжение, температуру и внутреннее сопротивление каждого элемента в режиме реального времени, эксплуатант получает возможность увидеть проблему до того, как она вызовет аварию. Это проактивный подход: вместо того чтобы ликвидировать последствия, мы предотвращаем их, увеличивая срок службы батарей и сокращая общую стоимость владения.

Веб-мониторинг - это современный стандарт для мониторинга критической инфраструктуры. При таком подходе информация о состоянии ИБП и каждой аккумуляторной батареи может быть доступна в любой точке мира с любого устройства. Оператору больше не нужно физически находиться в серверной, чтобы сверить показания с дисплея – они доступны через веб-браузер с любого устройства [2]. Это также наиболее гибкий, безопасный и экономически эффективный способ организации мониторинга, который радикально ускоряет реакцию на аварийные сигналы.

Отметим также, что для организаций, которое ориентированы на хранение абсолютно всех данных внутри своего периметра, веб-мониторинг все равно остается одним из наиболее часто используемых решений. Просто в данном случае веб-сервер и соответствующие базы данных находятся в локальной сети организации, а инструментом доступа является тот же самый веб-браузер. Доступ с мобильных устройств решается в данном случае сетевыми настройками [3, 4].

Естественно, что современные веб-решения уделяют большое внимание защите. Протоколы HTTPS с сертификатами, строгие политики паролей и шифрование (например, TLS 1.3) — всё это соответствует современным стандартам кибербезопасности, включая рекомендации ISO/IEC 62443 [5]. Это критически важно, так как инженерная инфраструктура сама по себе становится объектом для потенциальных атак, особенно на объектах КИИ.

Важно отметить, что веб-интерфейс даёт не только текущие показатели. Он же используется для доступа к анализу данных. Собственно говоря, просмотр и визуализация текущих данных представляет собой

Статья получена 20 июля 2026.
И.Н. Моисеев – ООО Абитех-Про; МАИ. (email:154@itdepo.ru)
Д.Е. Намиот – ООО Абитех-Про; МГУ имени М.В. Ломоносова (email: 135@itdepo.ru)
А.Н. Чеботарев – ООО Абитех-Про (email: checbotarev@abitech-pro.ru)

относительно простую задачу. Гораздо больший смысл имеет так называемая предиктивная аналитика [6], которая позволяет анализировать исторические данные, определять тренды и предсказывать, например, состояние отдельных аккумуляторных батарей. Это позволяет сервисным инженерам не просто реагировать на сбои, а прогнозировать их, планируя техническое обслуживание [7,8].

В настоящей статье описана разработка компании Абитех-Про[1] – многофункциональный контроллер Абсолайт-Про, разработанный для веб-мониторинга устройств ИБП и аккумуляторных батарей. Компания Абитех-Про более 15 лет занимается разработкой, поставкой и, главное, сопровождением систем бесперебойного и гарантированного электропитания, являясь одним из основных игроков на этом рынке. Но главным для данной разработки явилось наличие в компании большого технического центра, инженеры которого работают в области ИБП, практически, с момента зарождения этого рынка (направления) в России. Именно их опыт и экспертиза нужны были для оценки реализации и различных математических моделей с практической точки зрения. Важно также, что анализ данных для данного сегмента промышленного Интернета вещей есть не единовременная акция, а продолжающийся процесс, отражающий как смену поколений аппаратуры (свинцовые батареи и литий-ионные, совершенствование ИБП и т.д.), но и накопление опыта (в первую очередь, сбора датасетов) эксплуатации систем.

Таким образом, многофункциональный контроллер Абсолайт-ПРО представляет собой программно-аппаратный комплекс, состоящий из:

- одноплатного компьютера российского производства (реестр Минпромторга);
- российского программного обеспечения “Мониторинг Абсолайт-Про” для сбора, визуализации и анализа данных ИБП и аккумуляторных батарей (реестр Минцифры).

Дальнейшая часть статьи организована следующим образом. В разделе II представлена общая архитектура системы. В разделе III обсуждается мониторинг и аналитическая обработка данных.

II. Общая архитектура системы

Мониторинг, безусловно, начинается со сбора параметров отслеживаемых устройств. Необходима программа, которая опрашивает доступные сенсоры, либо принимает информацию о событиях, распространяемую по инициативе этих сенсоров. Первый вопрос – где запускать такую программу? Было принято решение для запуска такой программы использовать отдельное вычислительное устройство – одноплатный компьютер в типоразмере Raspberry Pi 4. Это радикальным образом решает вопрос с кибербезопасностью – система мониторинга будет изолирована от сети предприятия, в котором находится отслеживаемое оборудование.

Интерфейсы одноплатного компьютера позволяют использовать Ethernet-соединение (RJ-45) для связи с SNMP-картой ИБП [9]. Это может быть так называемый crossover-кабель[2], который позволяет соединить два устройства напрямую, безо всякого сетевого оборудования. Таким образом, система мониторинга может быть физически изолирована от сети предприятия. Собранные данные при этом система мониторинга может передавать на внешний сервер по протоколу HTTP (HTTPS) используя GSM-модем (на одном из USB-портов) или встроенный Wi-Fi модуль.

Рис.1. Пример одноплатного компьютера

Другой USB-порт может быть задействован для мониторинга Modbus, используя конвертор интерфейса USB-RS-485.

Имеющиеся на одноплатном компьютере интерфейсы GPIO[3] могут быть использованы для присоединения внешних датчиков. Например, для мониторинга температуры и влажности[4] (имеет важное значение для помещений, где размещены аккумуляторные батареи).

Альтернативно, и одноплатный компьютер и ИБП (его SNMP-карта) могут быть подключены к сети предприятия. В этом случае данные мониторинга могут сохраняться в базе данных, также расположенной в сети предприятия и быть доступны через веб-интерфейс. При этом база данных может быть расположена на самом одноплатном компьютере, а результаты мониторинга можно просматривать через поднятый на нем же локальный веб-сервер.

Все эти опции легко настраиваются (меняются) через конфигуратор системы мониторинга.

Таким образом, МФК для передачи данных по протоколу HTTPS может использовать:

1. подключение по Ethernet к сети заказчика. База данных может быть при этом на внешнем хостинге, в локальной сети предприятия или непосредственно на контроллере;
2. подключение по Wi-Fi к сети заказчика. База

[1] https://abitech-pro.ru/

[2] https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%BE%D1%81%D1%81-%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C_Ethernet

[3] https://ru.wikipedia.org/wiki/GPIO

[4] https://know.smartelements.ru/main:sensors:dht22

данных при может быть при этом на внешнем хостинге или непосредственно на контроллере;

3. отдельный GSM-модем. В этом случае и контроллер и ИБП будут полностью изолированы от сети заказчика. База данных при может быть при этом на внешнем хостинге

Общая схема подключения представлена на рис. 2.

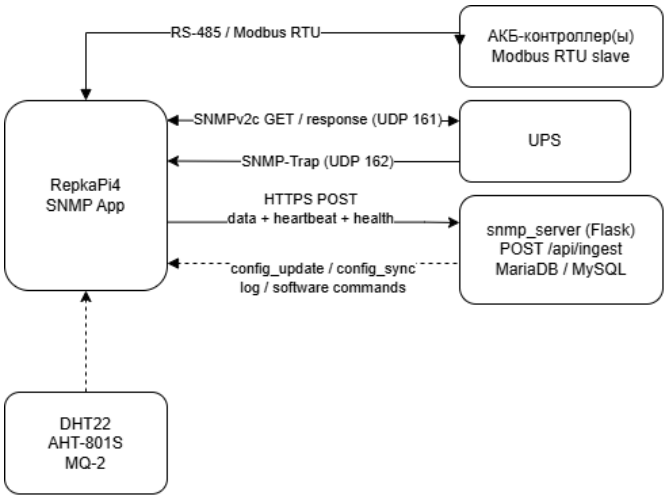

Рис. 2. Общая схема подключения

SNMP App здесь – это и есть приложение мониторинга, которое аккумулирует данные сенсоров и осуществляет их публикацию. Отметим, что приложение помимо опроса SNMP устройства осуществляет также и прием аварийных сообщений.

Задачи приложения могут быть описаны следующим образом:

- Обеспечить непрерывный сбор телеметрии с ИБП по протоколу SNMPv2c.
- Обеспечить сбор показаний аппаратных датчиков (температура, влажность, вибрация) через интерфейс GPIO.
- Опрашивать АКБ-контроллеры (BMS) по протоколу Modbus RTU через интерфейс RS-485.
- Принимать аварийные уведомления (SNMP-трапы) от ИБП и сохранять их для последующей передачи.
- Буферизовать собранные данные на локальный диск при отсутствии связи с сервером.
- Передавать накопленные данные на удалённый (локальный) HTTP-сервер по мере восстановления связи.
- Обеспечить возможность добавления новых источников данных без изменения ядра системы

SNMP App реализует модульную архитектуру (рис. 3) на основе подключаемых плагинов и supervisor-уровня отказоустойчивости. Ядро системы не содержит бизнес-логики конкретных источников данных: оно регистрирует фабрики, создаёт общий контекст, запускает plugin-группы задач, контролирует их состояние и передаёт нижний уровень восстановления отдельному восстановления системы.

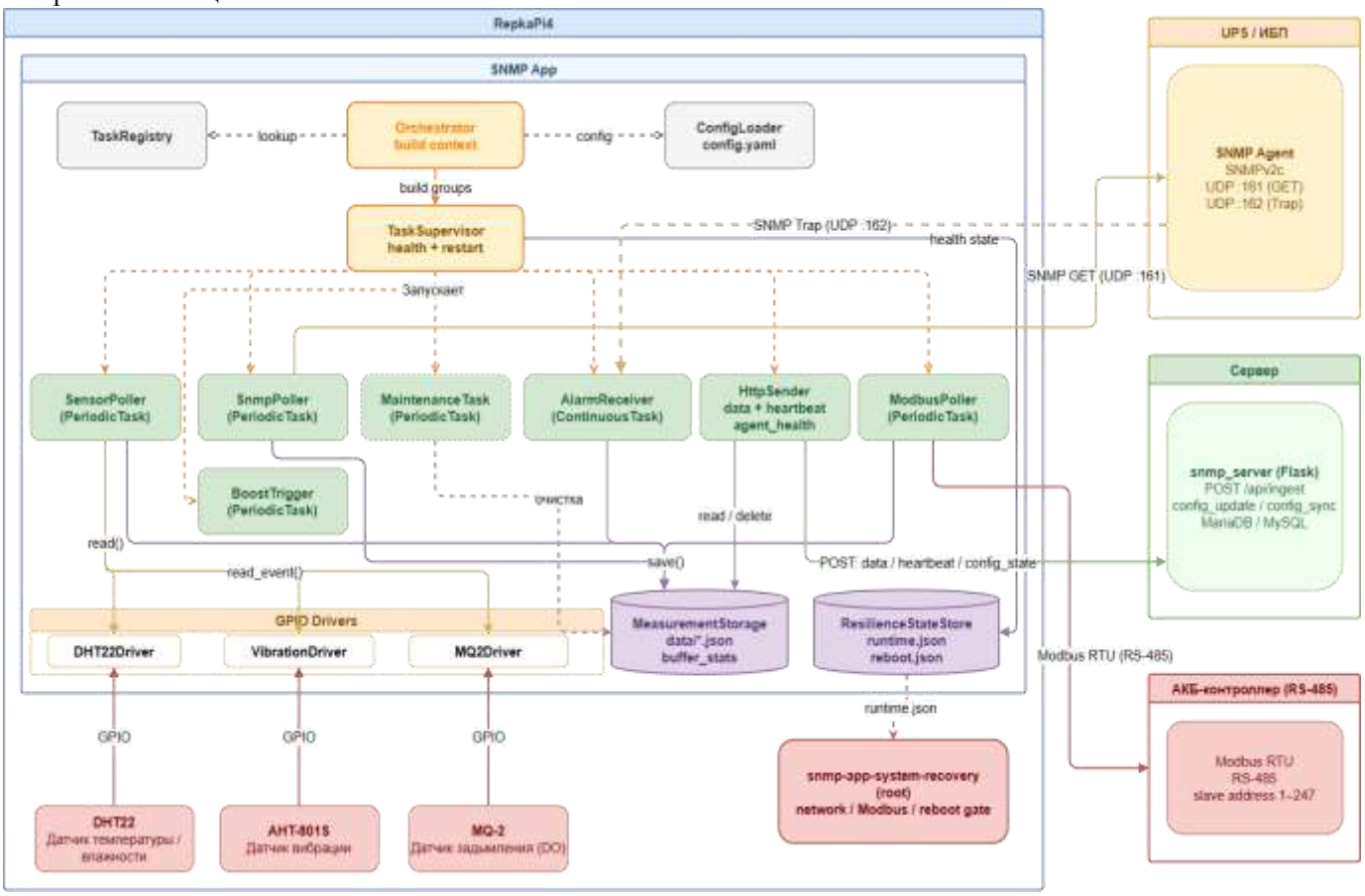

Рис. 3 – Архитектура приложения.

Архитектура «ядро + плагины» обеспечивает: изоляцию изменений (новый плагин не влияет на существующие), упрощённую сертификацию обновлений (только изменённый плагин проходит повторную проверку), возможность независимого тестирования каждого модуля, масштабируемость без роста сложности ядра.

Система состоит из нескольких слоев периода выполнения (рис. 4):

- Ядро (core) — оркестратор, supervisor, реестры, загрузчик конфигурации, файловое хранилище, логирование,
- Плагины-задачи (tasks) — набор модулей, каждый из которых реализует конкретный источник или потребитель данных.
- Драйверы (drivers) — низкоуровневые адаптеры для аппаратных датчиков

III. Мониторинг и аналитическая обработка

Собранные в процессе мониторинга данные представляют собой временные ряды, где каждое измерение (отсчет) содержит информацию о локальном времени получения данных, серверном времени (при записи на внешний сервер эти значения могут различаться), типе датчика (сенсора) и полученном значении.

Внешние сенсоры могут быть заданы явно, для аккумуляторных батарей сенсоры – это регистры Modbus, которые позволяют опрашивать информацию о напряжении, температуре и внутреннем сопротивлении батарей. Остальные же “сенсоры” – это параметры опроса ИБП по SNMP, которые описываются в RFC-1628[5].

RFC 1628 - это официальный стандарт IETF, определяющий базу управляющей информации (MIB) для мониторинга систем бесперебойного питания (ИБП) с помощью протокола SNMP (Simple Network Management Protocol). Он предоставляет универсальную структуру данных, охватывающую идентификацию устройства, показатели батареи и состояние входного/выходного питания. Эта база содежит конкретные значения идентификаторов (OID), которые и используются для запроса значений. RFC 1628 содержит следующие группы идентификаторов:

upsIdent (1.3.6.1.2.1.33.1.1): Название производителя, модель ИБП и версии прошивки.
upsBattery (1.3.6.1.2.1.33.1.2): Состояние батареи, время работы от батареи (в секундах), оставшееся время работы, напряжение, ток и температура.
upsInput (1.3.6.1.2.1.33.1.3): Количество входных фаз, частоты, напряжения и входные токи.
upsOutput (1.3.6.1.2.1.33.1.4): Выходные фазы, источник питания, частоты, напряжения и процент нагрузки.
upsBypass (1.3.6.1.2.1.33.1.5): Фазы байпаса, частоты и напряжения.
upsAlarm (1.3.6.1.2.1.33.1.6): Количество активных аварийных сигналов и записи в таблице upsAlarmTable.

Конкретные значения OID и используются в качестве наименований сенсоров при хранении данных в базе.

Говоря о конкретной базе данных, отметим, что в данном случае хранение временных рядов можно организовать и в реляционной базе данных, записывая измерения в одну таблицу. Такая схема оказалась вполне работающей, а смысл отказа от специализированного хранилища может состоять в том, что для хранения данных и визуализации может вполне подойти самый простой хостинг, включающий Apache и PostgreSQL, например. Это существенно удешевляет решение, а также упрощает сопровождение системы.

Решение по хранению и визуализации данных в таком случае может быть развернуто на самом простом веб-хостинге со стандартной связкой Apache + PostgreSQL. Отметим, что для конфигурации, когда данные мониторинга должны собираться в локальной сети предприятия может быть использована точно такая же связка открытых приложений.

В дальнейшем, приложение будет поддерживать и специализированные базы временных рядов.

Для реализации веб-сервера непосредственно на одноплатном компьютере используется FastAPI.

[5] https://datatracker.ietf.org/doc/html/rfc1628

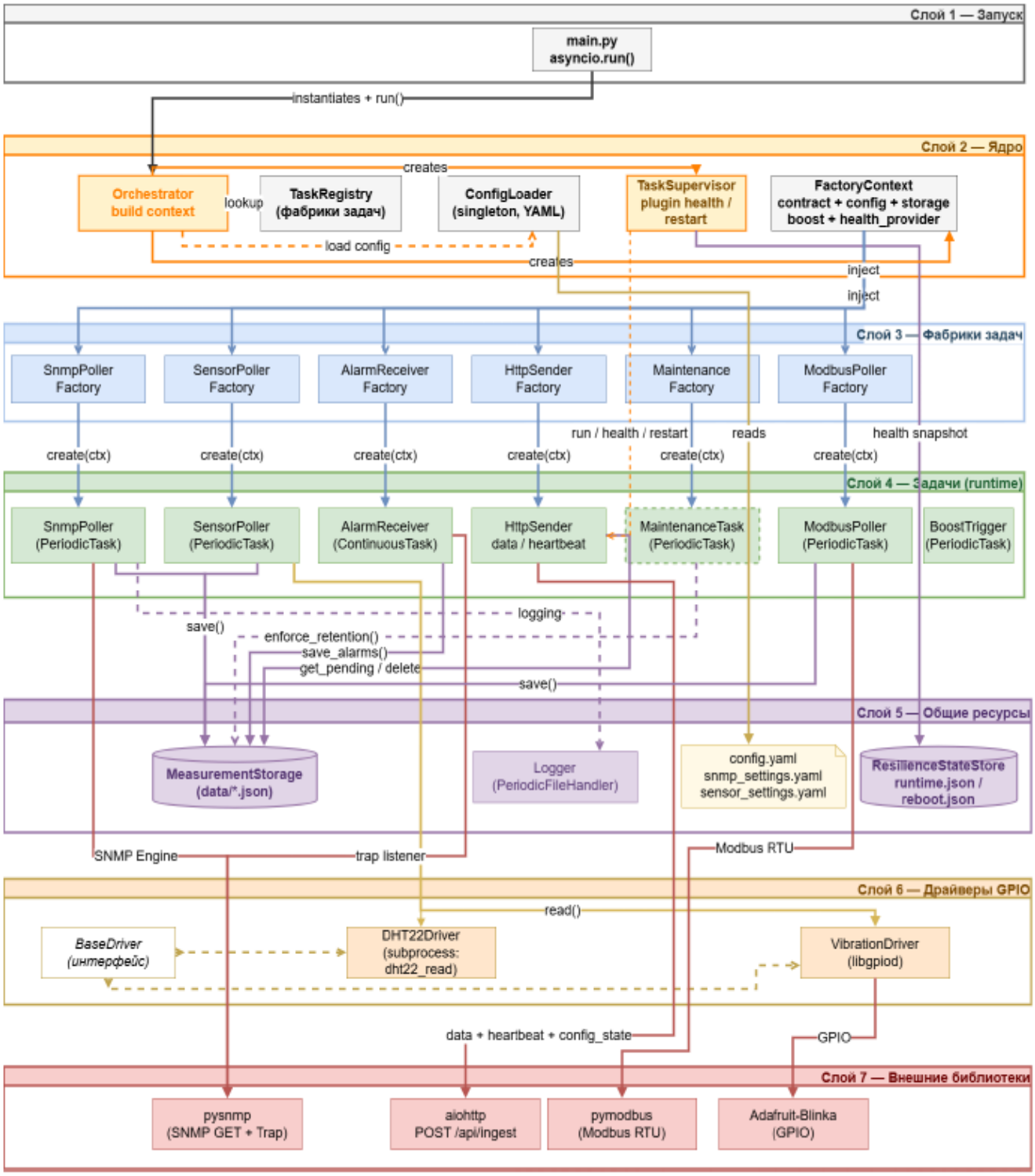

Рис.4 Структура программы

Говоря непосредственно о мониторинге, в первую очередь, можно выделить визуализацию данных, которая наглядно демонстрирует тренды и границы изменения параметров. Примеры представлены ниже на рисунках 5 и 6. Программное обеспечение системы мониторинга позволяет легко переключаться между просмотром сырых данных и обработанным трендом.

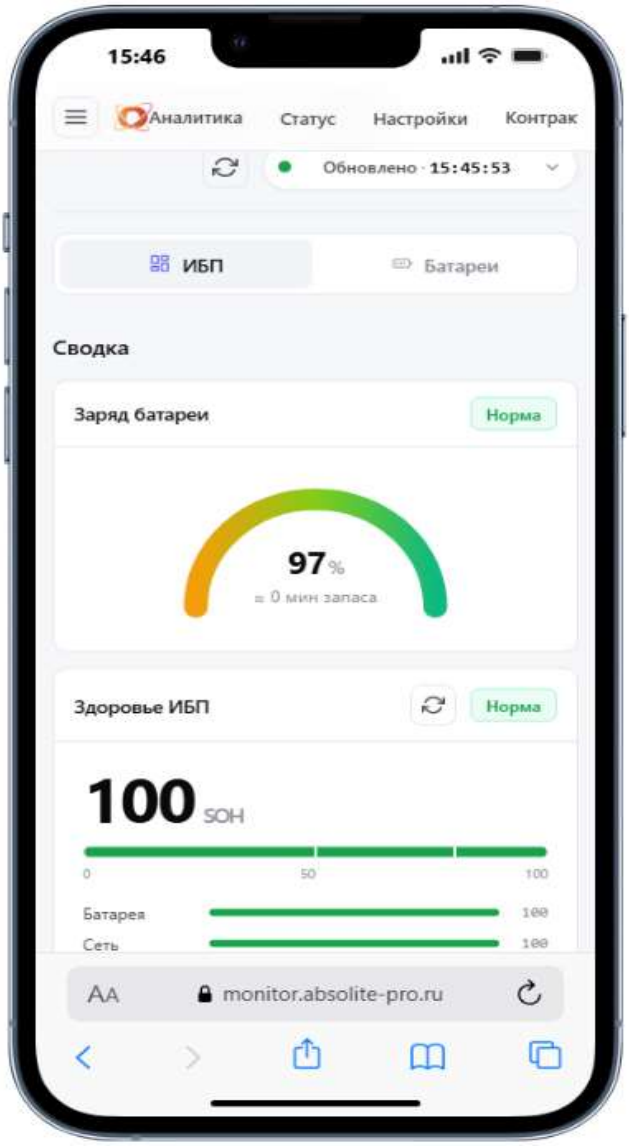

Рис. 5. Дашборд

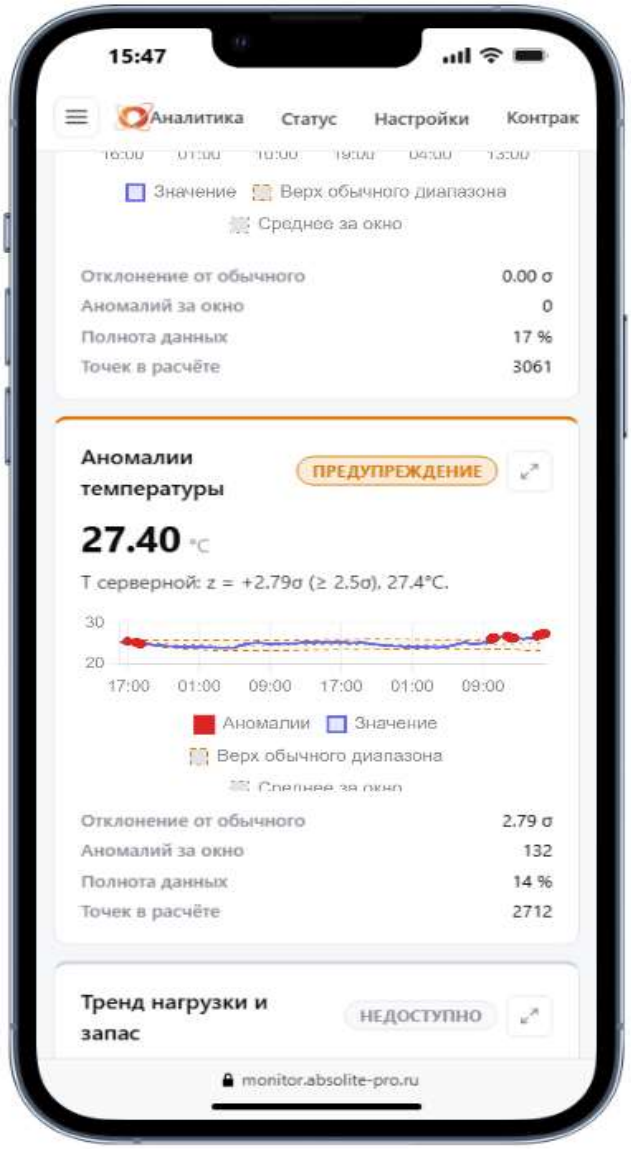

Рис.6. Закладка Аналитика

Дашборд представляет собой набор виджетов, отображающих параметры ИБП (АКБ).

Закладка Аналитика позволяет видеть границы изменения параметров временных рядов, а также статистические характеристики. Показываются предупреждения об аномальных значениях.

Аналитика для аккумуляторных батарей построена на отслеживании стабильности измеряемых показателей, где основную роль играет параметр внутреннего сопротивления батареи.
Система рассчитывает SOH (State of Health) аккумулятора - степень его износа и работоспособности, измеряемая в процентах. Она показывает, сколько емкости или пусковой мощности осталось у батареи по сравнению с совершенно новой.

Веб-интерфейс, как следует из приведенных снимков экранов поддерживает просмотр с мобильных устройств, что, естественно, облегчает работу инженерам сопровождения.

В том случае, если данные мониторинга собираются в локальной базе данных, то, при необходимости расследования инцидентов, инженерам сопровождения может быть предоставлен дамп этой базы, которые они смогут анализировать локально.

IV Заключение

В работе представлен отечественный программно-аппаратный комплекс “МФК Абсолайт-Про”, который позволяет проводить сбор и последующий анализ эксплуатационных характеристик источников бесперебойного питания и аккумуляторных батарей. ПАК построен на отечественном одноплатном компьютере и оригинальном программном обеспечении, которое поддерживает как сбор данных, так и его аналитическую обработку.

В качестве базового инструмента для доступа к данным выбран веб-браузер, так что данные мониторинга доступны с любого устройства с браузером. Технически, собранные данные могут накапливаться как на внешнем веб-сайте, так и

непосредственно на самом одноплатном компьютере. Передача данных на внешний сайт может осуществляться как из сети эксплуатирующей организации, как исходящие запросы по HTTPS (то есть, нужен обычный доступ к Интернет), так с помощью WiFi или GSM модема. В последних случаях контроллер вместе с опрашиваемым ИБП полностью отделены от сети эксплуатирующей организации.

Тестовая эксплуатация разработанного контроллера подтвердила удобство его использования на отечественных сетях. Мониторинг в режиме реального времени позволяет полностью отказаться от дорогостоящего и трудоемкого ручного обслуживания и выполняемых вручную контрольно-измерительных процедур. Именно это приводит к значительному снижению стоимости владения (TCO - total cost of ownership) системой бесперебойного питания.

Разработанный ПАК зарегистрирован в реестре Минцифры РФ.

Благодарности

Авторы благодарны инженерам технического центра компании Абитех-Про за помощь, критику и конструктивные советы в процессе разработки и тестовой эксплуатации устройства.

Библиография

[1] Aamir, Muhammad, Kafeel Ahmed Kalwar, and Saad Mekhilef. "Uninterruptible power supply (UPS) system." Renewable and sustainable energy reviews 58 (2016): 1395-1410.

[2] Ragnoli, Mattia, et al. "A condition and fault prevention monitoring system for industrial Computer Numerical Control machinery." Ieee Access 12 (2024): 20919-20930.

[3] Rao, Molli Srinivasa, et al. "The use of virtual private networks to facilitate remote working: a critical review of cyber security implications to develop successful VPN systems." 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, 2023.

[4] Nyakomitta, Peter S., and Silvance O. Abeka. "Security investigation on remote access methods of virtual private network." Global journal of computer science and technology 20.1 (2020): 1-10.

[5] Livshitz, Ilya I., and Olga M. Safonova. "Identifying Risks of Implementing Imposed Security Measures for IT Critical Infrastructure." 2024 International Conference" Quality Management, Transport and Information Security, Information Technologies"(QM&TIS&IT). IEEE, 2024.

[6] Akbar, Adnan, et al. "Predictive analytics for complex IoT data streams." IEEE Internet of Things Journal 4.5 (2017): 1571-1582.

[7] Tang, Jing-Xian, et al. "Predictive maintenance of VRLA batteries in UPS towards reliable data centers." IFAC-PapersOnLine 53.2 (2020): 13607-13612.

[8] Bolsi, Pedro C., et al. "Battery autonomy estimation method applied to lead–acid batteries in uninterruptible power supplies." Journal of Energy Storage 58 (2023): 106421.

[9] Kadena, Esmeralda, et al. "An Overview of UPS Configurations and Redundancy Techniques for Containerized Data Centers." 2025 IEEE 29th International Conference on Intelligent Engineering Systems (INES). IEEE, 2025.

Monitoring and Predictive Analytics for Uninterruptible Power Supply Systems and Batteries

I.N. Moiseev, D.E. Namiot, A.N. Chebotarev

***Abstract*— This article describes the Absolite-PRO Multifunctional Controller (MFC), a Russian hardware and software system (HSS). This original development by Abitech-Pro is designed for monitoring uninterruptible power supplies (UPS) and batteries. The paper describes the architectural model, software, and application diagram for the HSS for monitoring and predictive analytics. The HSS supports polling of monitored devices via SNMP and Modbus. Collected parameters can be stored both on the HSS itself and downloaded to external databases for subsequent visualization and analysis. The HSS can use various network connections to transmit collected data, including a GSM modem. In the latter case, the entire monitoring system will be completely isolated from the enterprise network where the UPS and batteries are installed.**

***Keywords*— UPS, battery, SNMP, Modbus, monitoring**

REFERENCES

[1] Aamir, Muhammad, Kafeel Ahmed Kalwar, and Saad Mekhilef. "Uninterruptible power supply (UPS) system." Renewable and sustainable energy reviews 58 (2016): 1395-1410.

[2] Ragnoli, Mattia, et al. "A condition and fault prevention monitoring system for industrial Computer Numerical Control machinery." Ieee Access 12 (2024): 20919-20930.

[3] Rao, Molli Srinivasa, et al. "The use of virtual private networks to facilitate remote working: a critical review of cyber security implications to develop successful VPN systems." 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, 2023.

[4] Nyakomitta, Peter S., and Silvance O. Abeka. "Security investigation on remote access methods of virtual private network." Global journal of computer science and technology 20.1 (2020): 1-10.

[5] Livshitz, Ilya I., and Olga M. Safonova. "Identifying Risks of Implementing Imposed Security Measures for IT Critical Infrastructure." 2024 International Conference" Quality Management, Transport and Information Security, Information Technologies"(QM&TIS&IT). IEEE, 2024.

[6] Akbar, Adnan, et al. "Predictive analytics for complex IoT data streams." IEEE Internet of Things Journal 4.5 (2017): 1571-1582.

[7] Tang, Jing-Xian, et al. "Predictive maintenance of VRLA batteries in UPS towards reliable data centers." IFAC-PapersOnLine 53.2 (2020): 13607-13612.

[8] Bolsi, Pedro C., et al. "Battery autonomy estimation method applied to lead–acid batteries in uninterruptible power supplies." Journal of Energy Storage 58 (2023): 106421.

[9] Kadena, Esmeralda, et al. "An Overview of UPS Configurations and Redundancy Techniques for Containerized Data Centers." 2025 IEEE 29th International Conference on Intelligent Engineering Systems (INES). IEEE, 2025.