УДК 621.317.08

АППАРАТНО-ПРОГРАММНАЯ АРХИТЕКТУРА ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ С СЕТЕВЫМИ ВОЗМОЖНОСТЯМИ

Зокиров Д.Т., гр.426401

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Гусинский А.В. – доктор технических наук, профессор

Аннотация. В докладе рассматривается разработанная аппаратно-программная архитектура информационно-измерительной системы (ИИС) с сетевыми возможностями, обеспечивающая метрологически корректную, надёжную и безопасную работу в условиях распределённых и дистанционных измерений, а также поддержку интеграции модулей искусственного интеллекта.

Ключевые слова. Аппаратно-программная архитектура, информационно-измерительная система, сетевые возможности, дистанционные измерения, метрологическая корректность.

Цель разработки – обеспечить метрологически корректную, удобную в эксплуатации и безопасную ИИС СВЧ диапазона с возможностью дистанционного управления, централизованного хранения результатов и интеграции ИИ-модулей. Основные требования включают учёт сетевых влияний в бюджете неопределённости, аппаратную синхронизацию времени, отказоустойчивость и встроенные механизмы безопасности. [1,2]

Ключевые принципы. Базовым требованием архитектуры является метрологическая корректность: все элементы сети и программного обеспечения учитываются при составлении бюджета неопределённости, а привязка ко времени выполняется аппаратными средствами (PTP/GPS) для минимизации вклада сетевой инфраструктуры в фазовые и временные погрешности. Для этого в метаданные каждого измерения включается информация об источнике времени и аппаратных timestamp.

Для обеспечения устойчивости к сбоям система проектируется с локальной буферизацией и возможностью автономной работы: при потере связи накопленные данные сохраняются в устойчивой очереди, что позволяет продолжать измерения без потери информации. После восстановления соединения механизм реплея гарантирует корректную и детерминированную доставку данных на центральный сервер.

Безопасность реализована по принципу «secure by default»: все каналы связи защищены mTLS/TLS, результаты подписываются цифровыми подписями, а операции фиксируются в журнале только для дозаписи (append‑only) для последующего аудита. Ключи для подписи хранятся в HSM или защищённых элементах, что снижает риск компрометации.

Модульность и масштабируемость достигаются через строго определённые интерфейсы между аппаратными блоками (генератор, СВЧ тракт, FPGA/АЦП), контроллерами и сетевыми шлюзами. Каждый модуль имеет документированный API и набор метаданных, что облегчает замену, добавление или обновление компонентов и интеграцию внешних сервисов, включая модули искусственного интеллекта.

Технические требования. Коммуникационные интерфейсы устройств должны обеспечивать как минимум 1 GbE, при высоких нагрузках – предпочтительна поддержка 10 GbE; для выездных/полевых применений возможна опция Wi‑Fi или LTE с учётом их влияния на метрологию. Важным требованием является аппаратная синхронизация времени: предпочтительны PTP с аппаратными timestamp'ами или GPS PPS; NTP допустим только для задач, не чувствительных к фазе.

Для управления системой рекомендуется применять REST/WebSocket через TLS, а для плотных потоков измерительных данных – двоичные протоколы (Protocol Buffers или Chunked TCP). Каждый пакет данных должен включать обязательные поля: идентификатор устройства, порядковый номер, метку времени и источник времени, полезные данные, сетевые метрики (RTT, loss, jitter), цифровую подпись и CRC для контроля целостности.

Локальная persistent‑буферизация обязана покрывать минимум суточный объём измерений при типичной нагрузке, обеспечивая выживание при падении сети и возможность корректной повторной передачи данных после восстановления связи. Механизмы очереди должны выдерживать перезапуск приложения и аппаратные рестарты.

Требования к безопасности включают mTLS для связи прибор↔сервер, подписание результатов с ключами в HSM, append‑only журнал аудита и регламент ротации ключей. Политики доступа реализуются через централизованные механизмы аутентификации и авторизации.

Ключевые показатели эффективности. Необходим контроль вклада сетевых факторов в расширенную неопределённость измерений – U_net должен быть ограничен на уровне, согласованном с категорией измерений. Ограничение по временной синхронизации выражается в допуске по offset, вычисляемом из допустимой фазовой ошибки по формуле $\Delta\phi = 2\pi f_{max} \Delta t$, что задаёт целевое значение Δt.

Сетевые операционные метрики включают медианный RTT (p50) порядка 50 ms для эффективной дистанционной калибровки; при RTT до 100 ms допускается работа с адаптивными алгоритмами. Приемлемый уровень потерь пакетов – до 0.5%; при превышении этого порога система переключается в режим повышенной усреднённости или локальной обработки. Допустимый RMS джиттера для фазочувствительных задач – порядка 5 ms.

Надёжность оценивается долей успешной доставки накопленных данных после восстановления сети (целевой показатель ≥ 99.9%) и временем выравнивания очереди (time‑to‑sync) не более 5 минут при стандартных объёмах записей.

Операционные метрики включают время отклика API (p95 < 200 ms, p99 < 1 s) и время установления удалённой сессии (handshake + readiness) в LAN менее 2 секунд. По безопасности – требования к подписанным файлам и ежегодной ротации ключей.

Поведение при авариях. При ухудшении качества сети система автоматически переводится в автономный режим: данные продолжают накапливаться локально и маркируются как «offline», при этом сохраняется информация о сетевых условиях в net_metrics. После восстановления соединения запускается упорядоченная передача накопленных данных с контролем целостности и подписи.

В случае потери синхронизации времени измерения помечаются, raw‑данные сохраняются, генерируется уведомление для оператора и предпринимаются автоматические попытки восстановления PTP/GPS. Если синхронизация не восстанавливается, в отчётах фиксируется степень неопределённости, связанная с временным источником.

При обнаружении недействительной цифровой подписи или несоответствии CRC отправка пакета блокируется, инцидент попадает в журнал и администратор оповещается. Дополнительно инициируются процедуры расследования и, при необходимости, повторной верификации данных.

Требуемые при вводе в эксплуатацию тесты. Необходимо провести проверку пропускной способности (iperf3 для 1 GbE и 10 GbE), длительные тесты синхронизации времени (оценка offset и drift PTP/GPS в течение 24–72 часов), а также сценарии эмуляции сетевых сбоев с использованием netem (моделирование задержек, потерь, джиттера) для проверки корректности буферизации и восстановления данных. Тесты безопасности включают проверку конфигурации TLS/mTLS, валидацию схем подписи и базовый penetration testing.

Документы и артефакты поставки. Поставляемая документация должна включать спецификацию API (REST/WS), схемы protobuf/JSON, шаблон измерительного отчёта с полями net_metrics и подписи, скрипты для тестирования сети (netem, iperf3), чек‑лист инсталляции, а также политику управления ключами и инструкции по обновлению ПО с процедурами rollback.

Предложенная архитектура сочетает строгие метрологические требования с практичной эксплуатационной гибкостью: аппаратная привязка ко времени и гарантии целостности данных обеспечивают доверие к удалённым измерениям; локальная буферизация и адаптивные алгоритмы поддерживают непрерывность исследований в реальных сетевых условиях; предусмотренные механизмы безопасности и документооборот позволяют проводить аудит и верификацию результатов. Такая платформа упрощает интеграцию ИИ-модулей, масштабирование и дальнейшее развитие измерительных комплексов.

Список использованных источников:

1. Богуш В.А. Векторные анализаторы цепей сантиметрового и миллиметрового диапазонов длин волн / В.А. Богуш [и др.]. – Москва: Горячая линия–Телеком, 2019. – 328 с.

2. Зокиров Д. Т. Методики дистанционной калибровки информационно-измерительной системы СВЧ диапазона = Methodologies for distance calibration of microwave range information and measurement systems / Д. Т. Зокиров // Информационная безопасность : сборник материалов 61-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 21–25 апреля 2025 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2025. – С. 158–161.