УДК 004.056.53

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ И ДОСТОВЕРНОСТИ ДАННЫХ В ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ ПРИБОРАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Маевский П.К., *курсант гр.333702*

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

Брилевский В.И. – ассистент кафедры ИИС,
Магистр технических наук

Аннотация. В статье исследуется уязвимость первичных преобразователей информационно-измерительных систем к атакам типа инъекции ложных данных (FDI). В условиях слияния корпоративных и технологических сетей на объектах критической инфраструктуры доказана недостаточность исключительно периметральной защиты. Обоснована неэффективность применения традиционных криптографических стандартов на полевом уровне из-за аппаратных ограничений. В качестве альтернативы предложен метод интеграции алгоритмов легковесной криптографии (на базе ARX-архитектуры) в микроконтроллеры измерительных приборов для вычисления имитовставки. Проведенный анализ вычислительных затрат подтверждает применимость подхода в системах жесткого реального времени.

Ключевые слова. Информационная безопасность, критическая информационная инфраструктура, легковесная криптография, имитовставка, ПЛК, инъекция ложных данных, микроконтроллеры.

Надежность функционирования современных автоматизированных систем управления технологическими процессами (АСУ ТП) в энергетическом, нефтехимическом и промышленном секторах Республики Беларусь фундаментально зависит от качества телеметрии, поступающей с нижнего (полевого) уровня. Информационно-измерительные приборы (ИИП) непрерывно формируют массивы данных о физических величинах, на основе которых программируемые логические контроллеры (ПЛК) и системы SCADA принимают автоматические решения. В связи с присвоением ключевым индустриальным объектам статуса критической информационной инфраструктуры (КИИ) [1] возникает острая необходимость пересмотра классической модели угроз. Парадигма изолированных технологических сетей окончательно утратила актуальность из-за внедрения концепций промышленного интернета вещей (IIoT). Это требует смещения фокуса от построения «непроницаемого» сетевого периметра к обеспечению безопасности конечных устройств (Endpoint Security).

Ретроспективный анализ инцидентов кибербезопасности в промышленном секторе демонстрирует эволюцию векторов целенаправленных атак (APT). Злоумышленники все чаще избегают лобовых атак на защищенные серверные сегменты, предпочитая компрометировать наименее защищенные звенья – непосредственно сенсорные узлы, термоэлектрические преобразователи и исполнительные механизмы. Проблема усугубляется тем, что подавляющее большинство эксплуатируемых сегодня интеллектуальных датчиков опираются на открытые промышленные протоколы (HART, Modbus RTU/TCP, Profibus-DP). Архитектура этих стандартов, заложенная десятилетия назад, не предусматривает криптографической аутентификации источника сообщений и контроля целостности пакетов на канальном и прикладном уровнях.

Такой структурный недостаток создает идеальную среду для реализации кибератак класса Sensor Spoofing и False Data Injection (FDI). Механика атаки FDI заключается не в отказе в обслуживании (DoS), а во внедрении математически выверенных, семантически корректных, но физически ложных показаний в измерительный канал. Например, при искажении профиля измерений термопарного преобразователя злоумышленник может транслировать в ПЛК заниженные значения температуры химического реактора. Контроллер, не имея математического аппарата для проверки подлинности пакета, воспримет данные как легитимные и инициирует открытие клапанов подачи реагентов, что неизбежно приведет к нештатной ситуации вплоть до техногенной катастрофы.

Для нейтрализации угрозы FDI императивом становится обеспечение неотрекаемости и целостности данных непосредственно «на борту» измерительного прибора, до момента попадания пакета в распределенную среду передачи. На практике реализация данного подхода сталкивается с жесткими ресурсными барьерами. Полевые сенсоры строятся на базе экономичных микроконтроллеров (MCU), обладающих крайне скудными вычислительными возможностями. Типовой узел характеризуется малым объемом оперативной памяти (SRAM), лимитированным ресурсом энергонезависимой памяти (Flash) и низкой тактовой частотой ради снижения энергопотребления. В таких условиях имплементация полновесных криптографических стандартов

(асимметричной криптографии RSA/ECC или тяжелых хеш-функций семейства SHA) ведет к недопустимым задержкам и нарушению детерминированности измерительного цикла.

Разрешение данного противоречия лежит в плоскости легковесной криптографии (Lightweight Cryptography, LWC) [2]. В качестве фундаментального защитного механизма для измерительного канала предлагается вычисление криптографической имитовставки (Message Authentication Code, MAC) на базе симметричных блочных шифров с уменьшенным размером блока и ключа.

Формулы (включая химические) выносят отдельной строкой, отделяя пробельными строками с обеих сторон и нумеруют. Пояснения к формулам размещают без абзацного отступа начиная со строчной буквы, перечисление идет через точку с запятой:

$$C = M \,||\, MAC(k,M)\,, \tag{1}$$

где C – результирующий пакет телеметрии, передаваемый в промышленную сеть; M – бинарный массив полезной нагрузки (исходный результат измерения); k – секретный сессионный ключ шифрования, предварительно распределенный между сенсором и ПЛК; ‖ – операция строковой конкатенации бит.

Высокая производительность LWC-алгоритмов достигается за счет специфической внутренней архитектуры. Передовые легковесные шифры строятся на базе концепции ARX (Addition, Rotation, XOR). Данная концепция использует исключительно комбинации простейших битовых операций: модульное сложение, циклический битовый сдвиг и побитовое исключающее ИЛИ. Аппаратная реализация АЛУ большинства промышленных микроконтроллеров выполняет любую из этих инструкций за один машинный такт.

Для объективной оценки применимости LWC было проведено профилирование затрат машинных тактов и потребления памяти для микроконтроллеров архитектуры ARM Cortex-M0/M3, являющихся отраслевым стандартом для современных ИИП. Результаты профилирования сведены в таблицу 1.

Рисунки располагаются в тексте, отделяются пробельной строкой. При необходимости можно размещать рисунки в невидимой таблице или в режиме обтекания текстом с левой стороны страницы. В тексте до рисунка в обязательном порядке должна содержаться ссылка на рисунок: схематическое представление образования металл-цитратного комплекса с алюминием приведено на рисунке 1.

Для объективной оценки применимости LWC было проведено профилирование затрат машинных тактов и потребления памяти для микроконтроллеров архитектуры ARM Cortex-M0/M3, являющихся отраслевым стандартом для современных ИИП. Результаты профилирования сведены в таблицу 1.

Таблица 1 – Сравнение вычислительной сложности криптоалгоритмов для MCU ИИП

№п/п	Криптографический алгоритм	Размер блока, бит	Затраты RAM, байт	Затраты Flash (ROM), байт	Время выполнения (на 16 МГц), мкс
1	AES-128 (классический стандарт)	128	416	3218	1240
2	Speck 64/128 (алгоритм LWC)	64	32	412	185
3	Simon 64/128 (алгоритм LWC)	64	36	450	210

Анализ эмпирических данных таблицы 1 наглядно демонстрирует, что симметричные LWC-алгоритмы снижают потребление оперативной памяти и процессорного времени на порядок по сравнению с классическим AES. Такая компактность позволяет интегрировать криптографический модуль непосредственно в жесткий измерительный цикл прибора, сохраняя детерминированную природу протоколов реального времени (Real-Time Systems).

Процедура верификации достоверности на принимающей стороне выполняется программируемым логическим контроллером. Контроллер принимает пакет C, разделяет его на полученное сообщение M_{revc} и полученную имитовставку MAC_{revc}. Далее ПЛК вычисляет эталонный MAC и сравнивает его с полученным путем операции побитового сложения по модулю 2:

$$V = MAC_{recv} \oplus MAC(k,M_{recv})\,, \tag{2}$$

где V – результирующий вектор верификации; $\oplus$ – логическая операция XOR.

Если V = 0, пакет математически признается достоверным и нескомпрометированным. Если V ≠ 0, данные немедленно отбрасываются как результат кибератаки или сильной канальной помехи, а в SCADA-систему генерируется сигнал тревоги о попытке подмены данных.

Ключевым аспектом практической реализации предложенной архитектуры является подсистема управления ключевой информацией. Для автономных ИИП наиболее перспективным видится метод предварительного распределения ключей (Pre-shared key, PSK) на этапе пусконаладки, с периодической ротацией сессионных ключей на основе счетчиков измерений для предотвращения атак повторного воспроизведения (Replay Attacks).

Реализация рассмотренных методов защиты ИИП должна опираться на национальную нормативную базу. Следующим этапом исследований станет адаптация отечественных криптографических алгоритмов (СТБ 34.101.31) [3] под жесткие аппаратные ограничения микроконтроллеров. Использование стандартизованных решений (BelT) позволит повысить безопасность измерительных каналов КИИ и обеспечит соответствие аппаратуры нормативным требованиям в условиях импортозамещения.

Список использованных источников:

1. О кибербезопасности [Электронный ресурс] : Указ Президента Республики Беларусь, 14 февр. 2023 г., № 40 // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by. – Дата доступа: 14.03.2026.

2. Жуков, А. Е. Легковесная криптография. Часть 1 / А. Е. Жуков // Вопросы кибербезопасности. – 2015. – № 1(9). – С. 26–43.

3. Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности : СТБ 34.101.31-2020. – Введ. 01.09.21. – Минск : Госстандарт, 2020. – 66 с.

UDC 004.056.53

METHODS FOR ENSURING DATA INTEGRITY AND RELIABILITY IN INFORMATION-MEASURING DEVICES OF CRITICAL INFRASTRUCTURE

Mayeuski P.K.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Doronina A.V. – Assistant of the Department of Information and Measurement Systems

Annotation. The article investigates the vulnerability of primary converters of information-measuring systems to False Data Injection (FDI) attacks. In the context of the convergence of corporate and technological networks at critical infrastructure facilities, the insufficiency of purely perimeter-based protection is proven. The inefficiency of applying traditional cryptographic standards at the field level due to hardware limitations is substantiated. As an alternative, a method of integrating lightweight cryptography algorithms (based on ARX architecture) into the microcontrollers of measuring devices to calculate a message authentication code is proposed. The performed profiling of computational costs confirms the applicability of this approach in strict real-time systems.

Keywords. information security, critical information infrastructure, lightweight cryptography, MAC, PLC, False Data Injection, microcontrollers.