РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **U** (11) **11920**
(51) ***H04L 9/00*** (2022.01)

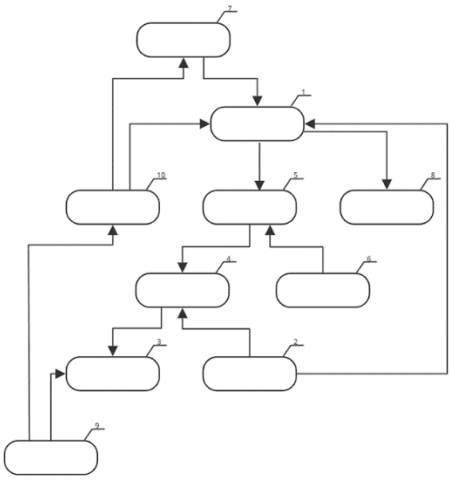
МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ
К ПАТЕНТУ

(21) 2025/1564.2
(22) 14.10.2025
(45) 20.03.2026, бюл. №11
(72) Адилжанова Салтанат Альмуханбетовна (KZ); Прокопович-Ткаченко Дмитрий Игоревич (UA); Амирханов Алихан Бауыржанұлы (KZ); Амирханова Гульшат Аманжоловна (KZ)
(73) Амирханова Гульшат Аманжоловна (KZ)
(56) US 11128473 B1, 21.09.2021

(54) **СИСТЕМА АВТОНОМНОЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ И КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ ЦИФРОВОГО ДВОЙНИКА ХЛЕБОПЕКАРНОЙ ЛИНИИ**

(57) Полезная модель относится к области цифровых информационных технологий, промышленной автоматики и защиты информации, в частности к средствам криптографического контроля целостности данных в системах «цифровой двойник — технологическое оборудование» хлебопекарных линий. Устройство представляет собой автономный криптомодуль на базе микроконтроллера ESP32 с локальным генератором тактовой частоты, криптографическим блоком хеширования, генератором одноразовых значений, модулем шифрованной Wi-Fi-передачи, блоками фильтрации электромагнитных помех и отказоустойчивого питания, а также модулем индикации состояния. Модуль выполняет нормализацию параметров состояния узлов линии (тестомес, расстоечная камера, печь), вычисляет хеш-идентификатор по алгоритму SHA-256 с меткой времени и одноразовым значением, после чего передаёт защищённый пакет телеметрии в систему мониторинга. Технический результат заключается в повышении доверия к данным цифрового двойника за счёт локального контроля целостности и подлинности телеметрии, предотвращении вмешательства в параметры технологического процесса и обеспечении устойчивой работы при электромагнитных помехах и перебоях питания.



Фиг. 1 - Автономный криптомодуль цифрового двойника хлебопекарной линии

(19) KZ (13) U (11) 11920

Область техники

Полезная модель относится к области цифровых информационных технологий, промышленной автоматики и защиты информации, а именно к средствам криптографической защиты и контроля целостности данных в системах «цифровой двойник — технологическое оборудование» хлебопекарных линий.

2. Уровень техники (известные решения и прототипы)

Известны телеметрические модули на базе микроконтроллеров с Wi-Fi-интерфейсом, применяемые для сбора параметров технологического процесса (температура, влажность, скорость привода) и передачи их в SCADA/MES. Недостатком таких решений является отсутствие локального криптографического преобразования и контроля целостности на стороне источника данных, вследствие чего возможны подмена телеметрии и навязывание несанкционированных воздействий.

В качестве ближайшего “типового” решения часто рассматривается Wi-Fi-модуль сбора данных с последующей проверкой подлинности на сервере. Недостатки: зависимость от сетевой доступности и удалённых сервисов для верификации; отсутствие автономного опорного генератора тактовой частоты; отсутствие аппаратной индикации компрометации и устойчивого питания при провалах напряжения.

Для выполнения требования экспертизы о наличии идентифицируемых источников раскрытия аналогов (патенты, публикации и т. п.), в качестве нероссийских прототипов использованы следующие запатентованные решения.

Прототип 1 (тип: защищённый автономный/съёмный модуль мониторинга с криптографическим преобразованием данных)

EP 2 928 202 A2 – «Secure Utility Metering Monitoring Module» (заявка № 15169458.5; приоритет 22.12.2010 US 201061425830 P; публикация 07.10.2015).

Ключевые признаки: автономный съёмный модуль для установки на существующий счётчик; хранение уникального идентификатора и персонального ключа; формирование криптограммы на основе данных и передача её в составе сообщения в удалённый центр управления.

Причины недостаточности: решение ориентировано на учёт потребления и защищённую передачу показаний; не раскрывает специализированный контроль технологических (рецептурных) параметров в связке «цифровой двойник — производственное оборудование», не описывает нормализацию/канонизацию набора технологических параметров перед формированием контрольного значения, а также не ориентировано на промышленную помехозащищённость и резервирование питания, заявленные в полезной модели.

Прототип 2 (тип: архитектура “доверенных сенсоров” с подписью показаний доверенным модулем) US 8 832 461 B2 – «Trusted Sensors» (заявка US 12/823 150; приоритет 25.06.2010; публикация 09.09.2014).

Ключевые признаки: каждый сенсор снабжён доверенным вычислительным модулем (TPM), который подписывает данные датчика и обеспечивает проверку целостности; хранение секретного ключа; обеспечение доверенных примитивов платформы.

Причины недостаточности: решение задаёт общую архитектуру доверия к данным датчиков, однако не раскрывает состав и взаимодействие узлов именно промышленного криптомодуля для контура «цифровой двойник — хлебопекарная линия», включая детерминированную нормализацию/канонизацию рецептурных параметров, одностороннюю телеметрическую политику обмена и комплексную помехозащиту/резервирование питания, заявленные в полезной модели.

Прототип 3 (тип: ранняя криптографическая фиксация/подпись сенсорных данных внутри устройства)

US 11 128 473 B1 – «Systems and methods for assuring authenticity of electronic sensor data» (заявка US 16/359 723; приоритет 20.03.2019; публикация 21.09.2021).

Ключевые признаки: криптопроцессор внутри устройства подписывает электронные данные сенсора немедленно после захвата; подпись формируется в раннем окне до возможной модификации данных; криптопроцессор размещается рядом с датчиком, а процесс подписи защищён от вмешательства других компонентов.

Причины недостаточности: решение направлено на обеспечение подлинности универсальных сенсорных данных (в т.ч. для потребительских устройств) и не раскрывает специализированный состав узлов и алгоритмический контур контроля именно рецептурных технологических данных, включая канонизацию набора параметров, вычисление хеш-идентификатора с учётом метки времени и одноразового значения (nonce), индустриальную фильтрацию помех и отказоустойчивое питание, заявленные в полезной модели.

Преимущество заявляемого решения по сравнению с прототипами состоит в том, что контроль целостности реализован непосредственно на стороне источника технологических параметров, с формированием детерминированного (канонизированного) буфера данных и вычислением контрольного значения, а также с аппаратной индикацией и повышенной устойчивостью к помехам и провалам питания.

3. Сущность полезной модели

Технический результат — повышение доверия к данным цифрового двойника за счёт локального контроля целостности и подлинности телеметрии, снижение риска вмешательства в параметры технологического процесса и обеспечение устойчивой передачи данных при электромагнитных помехах и перебоях питания.

Система представляет собой автономный криптомодуль на базе микроконтроллера ESP32 с локальным генератором тактовой частоты. Модуль принимает параметры состояния узлов хлебопекарной линии (тестомес, расстоечная камера, печь), выполняет нормализацию и канонизацию набора данных, вычисляет хеш-значение SHA-256 с включением метки времени и одноразового значения (nonce), а затем передаёт телеметрию вместе с хеш-идентификатором по шифрованному Wi-Fi-каналу в систему мониторинга. Отличительные признаки: наличие локального опорного генератора, криптографического блока хеширования, генератора одноразовых значений, модуля шифрованной передачи, помехозащищённого и резервируемого питания, а также аппаратной индикации состояния целостности.

4. Краткое описание чертежей

Фиг.1 — Структурная схема автономного криптомодуля цифрового двойника, включающая:

1 — микроконтроллерный узел (ESP32);

2 — локальный генератор тактовой частоты;

3 — интерфейс к узлам линии (тестомес/расстойка/печь);

4 — блок нормализации и канонизации данных;

5 — криптографический блок хеширования (SHA-256);

6 — генератор одноразовых значений (nonce)/источник энтропии;

7 — модуль шифрованной Wi-Fi-передачи;

8 — модуль индикации состояния;

9 — блок фильтрации электромагнитных помех (EMI) на линиях питания и сигналов;

10 — блок отказоустойчивого питания (DC/DC, суперконденсатор/аккумулятор, защита от провалов).

5. Подробное описание реализации

Микроконтроллерный узел 1 реализован на базе ESP32 и выполняет функции управления потоками данных, взаимодействия с периферией и криптографической обработки. Узел соединён с локальным генератором тактовой частоты 2, выполненным, например, в виде высокостабильного кварцевого или температурно-компенсированного генератора, обеспечивающего независимую временную привязку и устойчивость к внешним помехам. Сигналы состояния технологических узлов линии поступают через интерфейс 3, включающий гальваническую развязку и согласование уровней (аналоговые входы для температурных датчиков, дискретные входы для концевых датчиков, промышленный интерфейс, например, RS-485/OPC-совместимый шлюз).

Поступающие параметры направляются в блок нормализации и канонизации 4, где выполняются: приведение к единому формату и диапазонам; сортировка и детерминированная нумерация полей; прикрепление метки времени, сформированной на основе опорного генератора 2; формирование канонизированного буфера данных согласно внутреннему регламенту полей.

Криптографический блок 5 вычисляет хеш-значение по алгоритму SHA-256 над канонизированным буфером, включающим также одноразовое значение (nonce), формируемое генератором 6. В качестве источника энтропии используется встроенный в ESP32 аппаратный TRNG и/или внешний шумовой источник, прошедший первичную статистическую фильтрацию.

Сформированный пакет {данные, метка времени, nonce, хеш} передаётся модулю шифрованной Wi-Fi-связи 7. Модуль обеспечивает установление защищённого канала (уровень канала — WPA2/WPA3; при обмене с сервером — аутентифицированный прикладной протокол, например TLS 1.3, с проверкой сертификата сервера). На стороне модуля реализована политика «только исходящая телеметрия», что предотвращает удалённое вмешательство в технологические параметры.

Блок индикации 8 отображает состояние целостности и связи (например: зелёный — передача успешна, верификация хеша подтверждена ответом системы мониторинга; жёлтый — подтверждение не получено; красный — локальная ошибка/несоответствие; мигающий красный — компрометация энтропии/частые повторения nonce). Дополнительно может быть предусмотрен аппаратный «сухой» контакт/сигнальная линия для передачи аварийного статуса в существующую систему сигнализации.

Блок 9 фильтрации EMI включает LC-фильтры, ограничители перенапряжения (варисторы/TVS-диоды) на входе питания и синфазные дроссели на сигнальных линиях, снижая влияние высокочастотных помех, характерных для электроприводов тестомеса и печи. Блок 10 отказоустойчивого питания содержит DC/DC-преобразователь, узел резервирования на суперконденсаторе или аккумуляторе малой ёмкости и схему мониторинга проседания напряжения; при кратковременных провалах питания обеспечивается корректное завершение вычисления хеша и сохранение последнего состояния с последующей ретрансляцией.

Последовательность обмена с системой мониторинга: чтение и нормализация параметров (блок 4); генерация nonce и метки времени (6, 2); хеширование SHA256 (5); формирование и отправка пакета по защищённому каналу (7); при наличии — приём квитанции сервера о корректной верификации; индикация статуса (8) и протоколирование результата во встроенной памяти.

Для повышения стойкости могут применяться сторожевой таймер микроконтроллера, защита загрузчика (secure boot), шифрование внутренней флеш-памяти и аппаратное отключение режима приёма управляющих команд через Wi-Fi в штатной конфигурации.

6. Технический результат

При реализации полезной модели достигается:

— защита телеметрических данных от подмены за счёт локального хеширования и включения меток времени и одноразовых значений;

— предотвращение вмешательства в технологические параметры путём односторонней (телеметрической) модели связи и шифрованного канала передачи;

— повышение электромагнитной совместимости и устойчивости к помехам благодаря фильтрации EMI и резервированию питания;

— снижение зависимости от внешних сервисов синхронизации за счёт локального опорного генератора;

— оперативная аппаратная индикация состояния целостности и связи.

7. Перечень условных обозначений (Фиг.1)

1 — микроконтроллерный узел (ESP32);

2 — локальный генератор тактовой частоты;

3 — интерфейс к узлам линии (тестомес/расстойка/печь);

4 — блок нормализации и канонизации данных;

5 — криптографический блок хеширования (SHA-256);

6 — генератор одноразовых значений (nonce)/источник энтропии;

7 — модуль шифрованной Wi-Fi-передачи;

8 — модуль индикации;

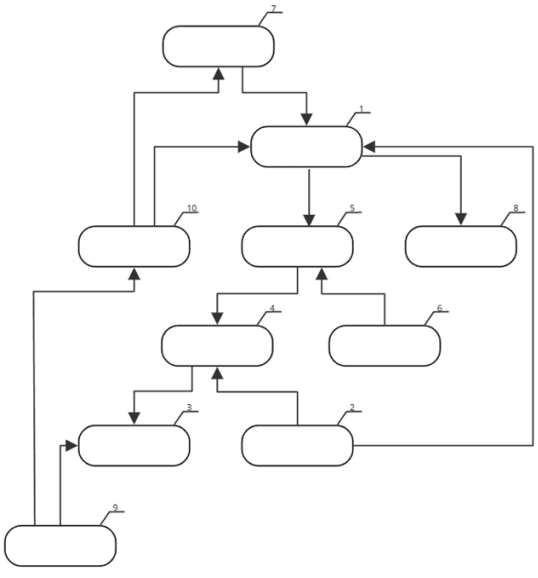
9 — блок фильтрации электромагнитных помех;

10 — блок отказоустойчивого питания.

ФОРМУЛА ПОЛЕЗНОЙ МОДЕЛИ

1. Система автономной криптографической защиты и контроля целостности данных цифрового двойника хлебопекарной линии, содержащий микроконтроллерный узел, интерфейс к узлам хлебопекарной линии и модуль беспроводной связи, ***отличающийся*** тем, что дополнительно содержит локальный генератор тактовой частоты, блок нормализации и канонизации данных, криптографический блок хеширования по алгоритму SHA-256, генератор одноразовых значений (nonce), модуль индикации состояния целостности и связи, блок фильтрации электромагнитных помех и блок отказоустойчивого питания, при этом микроконтроллерный узел выполнен с возможностью формирования канонизированного буфера технологических параметров, вычисления хеш-значения над указанным буфером совместно с меткой времени и nonce, и передачи пакета {данные, метка времени, nonce, хеш} по защищённому беспроводному каналу.

2. Система автономной криптографической защиты и контроля целостности данных цифрового двойника хлебопекарной линии по п.1, ***отличающийся*** тем, что модуль беспроводной связи выполнен с политикой односторонней телеметрической передачи, при которой входящие команды управления блокируются на транспортном уровне, а модуль индикации выполнен с возможностью отображения состояний «передача успешна/подтверждение не получено/ошибка целостности/признаки деградации энтропии».



Фиг. 1 - Автономный криптомодуль цифрового двойника хлебопекарной линии

Верстка Д. Женысова
Корректор Г. Косанова