РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **U** (11) **12422**
(51) ***G06F 21/64*** (2013.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ
К ПАТЕНТУ

(21) 2025/1566.2
(22) 14.10.2025
(45) 19.06.2026, бюл. №24
(72) Амирханова Гульшат Аманжоловна (KZ); Адилжанова Салтанат Альмуханбетовна (KZ); Прокопович-Ткаченко Дмитрий Игоревич (UA); Амирханов Алихан Бауыржанұлы (KZ)
(73) Адилжанова Салтанат Альмуханбетовна (KZ)
(56) US 11403428 B2, 02.08.2022

(54) **ИНТЕЛЛЕКТУАЛЬНЫЙ КОНТРОЛЛЕР ПРОВЕРКИ ЦИФРОВОЙ ПОДПИСИ ТЕХНОЛОГИЧЕСКИХ ЖУРНАЛОВ**

(57) Полезная модель относится к области цифровых информационных технологий, промышленной автоматики и защиты информации и предназначена для контроля целостности и подлинности технологических журналов параметров (температура, влажность и смежные показатели) в кибер-физических системах пищевой промышленности, включая цифровые двойники хлебопекарных процессов, с учётом требований HACCP и ISO 22000.

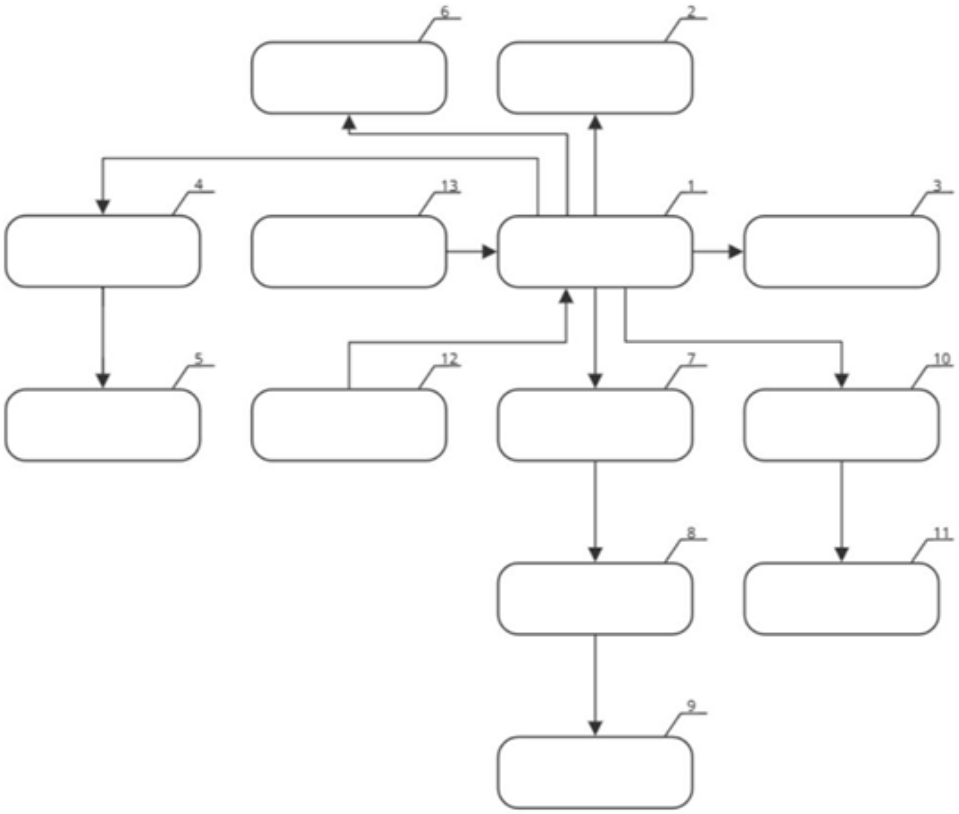
Техническим результатом является обеспечение контролируемой неизменности и проверяемой подлинности записей технологических журналов с автономной индикацией состояния целостности и возможностью работы при сбоях питания и связи, а также повышение достоверности прослеживаемости и доказуемости записей для целей аудита.

Система выполнена в виде интеллектуального контроллера, включающего микроконтроллерный узел, криптографический модуль безопасного хранения ключей, модуль доверенного времени (RTC с резервным питанием и/или NTP-синхронизацией), сетевой интерфейс (Ethernet/Wi-Fi), интерфейс к цифровому двойнику/SCADA (OPC UA/MQTT/HTTP-API), интерфейсы к датчикам, блок канонизации и нормализации записей, блок вычисления хеш-подписи и хеш-сцепления, энергонезависимую память журналов с режимом WORM-логики, модуль индикации (световой/релейной), сервисный/audit-порт только чтение, блок отказоустойчивого питания и фильтрации ЭМП и датчик вскрытия.

Функционирование контроллера заключается в приёме нормализованных записей от цифрового двойника и/или датчиков, канонизации полей записи, формировании контрольной хеш-подписи текущей записи с учётом метки времени, одноразового значения (nonce) и хеша предыдущей записи (формирование хеш-цепочки), сохранении записей и метаданных в энергонезависимой памяти в режиме WORM, а также верификации целостности при чтении/экспорте путём рекомбинации хеш-цепочки и проверки меток времени и подписи. При выявлении несоответствия формируется событие нарушения целостности и активируется визуальная/релейная индикация; предусмотрена блокировка использования спорных данных на уровне управления процессом.

Область применения: предприятия пищевой промышленности и иные производства, где требуется доказуемая целостность и подлинность технологических журналов параметров в условиях возможных сбоев связи и электропитания.

(19) KZ (13) U (11) 12422



Фиг. 1 - Интеллектуальный контроллер проверки цифровой подписи технологических журналов

Область техники

Полезная модель относится к области цифровых информационных технологий, промышленной автоматики и защиты информации и предназначена для обеспечения контроля целостности и подлинности технологических журналов параметров (температура, влажность и смежные показатели) в кибер-физических системах пищевой промышленности, в частности в цифровых двойниках хлебопекарных процессов, с учетом требований систем менеджмента безопасности пищевой продукции (HACCP, ISO 22000).

Уровень техники (известные решения и прототип)

Известны технические средства регистрации технологических параметров с сетевым интерфейсом.

Так, в китайском патенте CN 104298173 A (публикация 21.01.2015; приоритет 26.09.2014; заявитель Beijing Satellite Manufacturing Factory Co., Ltd.) "Способ получения параметров обработки станка с ЧПУ для сетевого мониторинга в реальном времени" описана система, в которой станок с ЧПУ подключается к серверу сбора данных через RJ 45 интерфейс и коммутатор сети; в серверной базе данных фиксируются номер станка, тип системы управления, IP адрес и номер порта, состояние работы и другие параметры. Клиентское приложение с использованием SDK пакетов FOCAS, HEIDENHAIN, FANUC и SIEMENS устанавливает соединение по IP адресу и порту (функция Connect(IP, Port, Timeout, Handle)), получает базовые параметры, текущую скорость, режим работы и записывает их в базу данных【500407399239727†L680-L702】. Этот прототип обеспечивает непрерывный сбор данных о работе оборудования по сети и хранение их в серверной БД. К существенным признакам заявляемой модели относятся сетевой интерфейс для передачи нормализованных записей журнала и регистрация параметров технологических процессов; указанные признаки присутствуют и в китайском прототипе. Однако в этом решении отсутствует механизмы криптографической канонизации и цепного связывания записей журнала, нет выделенного криптографического модуля и доверенного времени, что не позволяет гарантировать неизменность и подлинность каждой записи.

Известен германский (публикация 30.07.2015; патент DE 102014100920 A1 приоритет 27.01.2014; заявитель WTW Wissenschaftlich Technische Werkstätten GmbH) "Data logger". В устройстве предусмотрены процессорный узел, датчики, энергонезависимая память и интерфейс для подключения к внешнему компьютеру. При соединении с ПК регистратор распознаётся как накопитель; измеренные данные сохраняются в стандартных форматах, например PDF【266795556718689†L300-L308】. Для передачи данных пользователю они могут быть автоматически прикреплены к создаваемому электронной почтой письму или скопированы в каталоги корпоративной сети либо в облачное хранилище 【266795556718689†L308-L314】. Признаками, совпадающими с заявляемой моделью, являются наличие энергонезависимой памяти для журналов и возможность экспорта данных через сетевой интерфейс (LAN/интернет). Недостатком данного прототипа является отсутствие аппаратной хеш цепочки записей, защищённого хранения ключей и контроля доверенного времени; данные могут быть перезаписаны и удалены, что не позволяет использовать его для обеспечения аудита целостности технологических журналов.

Известны программные средства электронного документооборота с использованием цифровых подписей для контроля целостности журналов. Например, американский патент US 11403428 B2 (публикация 02.08.2022; приоритет 16.01.2019; заявитель Siemens AG) "Protecting integrity of log data" раскрывает способ формирования защищённых журналов. Логическая схема принимает записи лога, а модуль аппаратной безопасности (HSM) формирует новый защищённый элемент, вычисляя HMAC значение и включая в него хеш предыдущего элемента, идентификатор сеанса и счётчик; секретные ключи и параметры протокола хранятся в HSM и недоступны атакующему【195616852495605†L516-L523】. Каждый новый элемент вместе с хешем предыдущего передаётся в систему обнаружения вторжений, формируя цепочку, изменение которой невозможно без знания ключей【195616852495605†L526-L550】. Данный прототип решает задачу контроля целостности журналов, но реализован как специализированный модуль в составе компьютерной системы. Он не взаимодействует с датчиками технологического процесса, не обеспечивает нормализацию записей по HACCP/ISO 22000, не имеет автономного доверенного времени и энергии, а контроль цепочки зависит от внешней вычислительной инфраструктуры.

Отличительные особенности заявляемой полезной модели по отношению к рассмотренным прототипам заключаются в интеграции нескольких функций: аппаратная канонизация и хеш сцепление технологических записей с использованием криптографического модуля и доверенного времени; WORM журнал с невозможностью перезаписи; автономное питание и тампер контроль; визуальная и релейная индикация состояния целостности. Эти меры позволяют обеспечить проверяемую неизменность и подлинность технологических журналов пищевой промышленности при сбоях связи и питания, чего не достигают приведённые аналоги.

Сущность полезной модели

Технический результат — обеспечение контролируемой неизменности и проверяемой подлинности технологических журналов цифрового двойника с индикацией состояния целостности и автономной работой при сбоях питания и связи,

соответствующей принципам HACCP и требованиям ISO 22000 к прослеживаемости и доказуемости записей.

Заявляемое устройство представляет собой интеллектуальный контроллер, который:

• принимает от цифрового двойника и/или датчиков нормализованные записи журнала параметров;

• выполняет канонизацию полей записи и формирует контрольную хеш-подпись текущей записи с учетом метки времени, одноразового значения (nonce) и хеша предыдущей записи (цепочка хешей);

• сохраняет журнал и сопутствующие метаданные в энергонезависимой памяти с режимом WORM-логики;

• сверяет подписи при чтении/экспорте, формирует отчеты о целостности и подлинности;

• управляет визуальной/релейной индикацией статуса;

• использует отказоустойчивое питание и фильтрацию электромагнитных помех.

Отличительные признаки: наличие аппаратного криптомодуля с защищенным хранилищем ключей, доверенного источника времени, алгоритма хеш-сцепления записей (chain-of-hash) с канонизацией, а также автономных средств индикации и аудита.

Краткое описание чертежей

Фиг.1 — Структурная схема интеллектуального контроллера.

На схеме изображены: 1 — микроконтроллерный узел; 2 — криптографический модуль безопасного хранения ключей; 3 — модуль доверенного времени (RTC с батареей и/или NTP-синхронизацией); 4 — модуль сетевого интерфейса (Ethernet/Wi-Fi); 5 — интерфейс к цифровому двойнику/SCADA (OPC UA/MQTT/HTTP-API); 6 — интерфейсы к датчикам температуры/влажности; 7 — блок канонизации и нормализации записей; 8 — блок вычисления хеш-подписи и хеш-сцепления; 9 — энергонезависимая память журналов с WORM-логикой; 10 — модуль индикации состояния (световая/релейная); 11 — сервисный/audit-порт (только чтение); 12 — блок отказоустойчивого питания и фильтрации ЭМП; 13 — датчик вскрытия/тампер-контроль.

Подробное описание реализации

Микроконтроллерный узел (1) управляет обменом данными, криптографическими операциями и логикой контроля. К нему аппаратно подключены: криптографический модуль (2) с защищенным хранилищем ключевого материала и реализацией аппаратных примитивов; модуль доверенного времени (3), включающий высокостабильный RTC с автономным питанием и, при наличии связи, модуль синхронизации по NTP с верификацией источника; сетевой интерфейс (4) и протокольный интерфейс к цифровому двойнику/SCADA (5).

Интерфейсы к датчикам (6) обеспечивают прием первичных технологических параметров либо принимают уже агрегированные записи от цифрового двойника через (5). Блок канонизации (7) выполняет нормализацию полей записи: сортировку ключ-значений по предопределенному реестру, унификацию единиц измерения, фиксированный формат времени (UTC+метка RTC), удаление избыточных полей, квантование значений до установленной точности и вычисление контрольного идентификатора партии/смены.

Блок хеширования (8) формирует канонизированное представление записи и вычисляет контрольную хеш-подпись, например по алгоритму SHA-256; для аутентифицированного контроля целостности может использоваться HMAC-SHA-256 с ключом из модуля (2). Для предотвращения незаметного удаления или перестановки записей реализуется хеш-сцепление: в хеш текущей записи включается хеш предыдущей, метка времени (3) и одноразовое значение (nonce), генерируемое контроллером. По требованию, модуль (2) может выполнять заверение сводных блоков (например, конца смены) аппаратной электронной подписью с использованием закрытого ключа, недоступного микроконтроллеру.

Энергонезависимая память (9) хранит журнал и метаданные в режиме WORM-логики (без возможности перезаписи существующих записей на уровне прошивки; физически реализуется за счет фрагментированного выделения областей и запрета операций стирания без сервисного аппаратного ключа). Модуль индикации (10) реализует отображение статуса: «целостность подтверждена», «обнаружено несоответствие», «ошибка времени», «ошибка подписи», а также выдает управляющий сигнал (сухой контакт/реле) для блокировки применения спорных данных в уровне управления процессом.

Сервисный/audit-порт (11) предоставляет режим только чтения для выгрузки журналов и отчетов о целостности в машиночитаемом формате, сопровождаемых сводными хеш-идентификаторами и аттестатом времени. Питание (12) включает первичный источник, резервный аккумулятор/суперконденсатор, стабилизацию, фильтры и защиту от выбросов/переполюсовки; обеспечивается корректная дозапись критических структур при внезапном пропадании энергии. Датчик вскрытия (13) регистрирует попытки несанкционированного доступа к корпусу, формируя отдельную запись журнала и индикацию.

Алгоритм проверки при чтении/экспорте: контроллер последовательно рекомбинирует хеш-цепочку от первой записи к последней, сверяет рассчитанные значения с сохраненными, валидирует метки времени (3) и, при наличии заверения пакетов, проверяет подпись через модуль (2). При любом несоответствии формируется событие нарушения целостности и активируется индикация (10).

Технический результат

Реализация модели обеспечивает:

• криптографически обоснованный контроль целостности и подлинности технологических журналов (устойчивость к подмене, удалению и перестановке записей);

• локальную, не зависящую от внешних сервисов верификацию с доверенным временем;

• повышение достоверности прослеживаемости в рамках процедур HACCP и ISO 22000;

• автономную работу и корректное завершение операций при сбоях питания;

• оперативную визуальную и релейную индикацию состояния целостности для предотвращения использования недостоверных данных в управлении технологическим процессом.

Перечень условных обозначений (Фиг.1)

1 — микроконтроллерный узел;

2 — криптографический модуль безопасного хранения ключей;

3 — модуль доверенного времени (RTC/NTP);

4 — модуль сетевого интерфейса (Ethernet/Wi-Fi);

5 — интерфейс к цифровому двойнику/SCADA (OPC UA/MQTT/HTTP-API);

6 — интерфейсы к датчикам температуры/влажности;

7 — блок канонизации и нормализации записей;

8 — блок вычисления хеш-подписи и хеш-сцепления;

9 — энергонезависимая память журналов с WORM-логикой;

10 — модуль индикации состояния (световая/релейная);

11 — сервисный/audit-порт (только чтение);

12 — блок отказоустойчивого питания и фильтрации ЭМП;

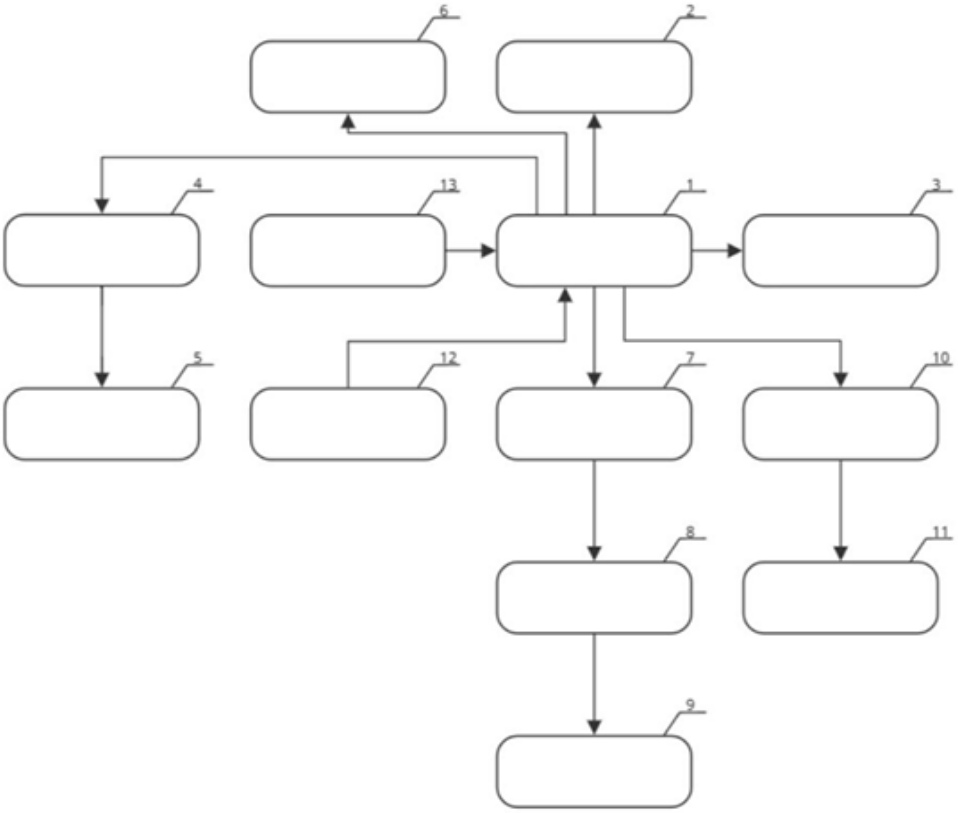
13 — датчик вскрытия/тампер-контроль.

ФОРМУЛА ПОЛЕЗНОЙ МОДЕЛИ

1. Интеллектуальный контроллер проверки цифровой подписи технологических журналов, содержащий микроконтроллерный узел, модуль сетевого интерфейса, интерфейс к цифровому двойнику, интерфейсы к датчикам технологических параметров, модуль индикации состояния и блок отказоустойчивого питания, ***отличающийся*** тем, что он дополнительно содержит криптографический модуль с защищенным хранением ключей, модуль доверенного времени, блок канонизации и нормализации записей, блок вычисления хеш-подписи и хеш-сцепления, энергонезависимую память журналов с WORM-логикой, сервисный порт, выполненный в режиме только чтения, и датчик вскрытия, при этом микроконтроллерный узел соединен с криптографическим модулем, модулем доверенного времени, модулем сетевого интерфейса, интерфейсом к цифровому двойнику, интерфейсами к датчикам технологических параметров, блоком канонизации и нормализации записей, блоком вычисления хеш-подписи и хеш-сцепления, энергонезависимой памятью журналов с WORM-логикой, модулем индикации состояния, сервисным портом и датчиком вскрытия и выполнен с возможностью приема записей технологического журнала, канонизации полей каждой записи, вычисления хеш-подписи текущей записи с включением метки времени, одноразового значения и хеша предыдущей записи, записи указанных данных в энергонезависимую память и последовательной верификации хеш-сцепления при чтении и экспорте журнала.

2. Контроллер по п.1, ***отличающийся*** тем, что криптографический модуль выполнен с возможностью формирования электронной подписи сводных пакетов записей технологического журнала.

3. Контроллер по п.1, ***отличающийся*** тем, что модуль индикации состояния содержит световой индикатор и релейный выход.



Фиг. 1 - Интеллектуальный контроллер проверки цифровой подписи технологических журналов

Верстка Д. Женысова
Корректор Г. Косанова