



РЕСПУБЛИКА КАЗАХСТАН

(19) KZ (13) U (11) 11895
(51) G06F 17/00 (2006.01)
H04L 9/06 (2006.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(21) 2025/1561.2

(22) 14.10.2025

(45) 13.03.2026, бюл. №10

(72) Прокопович-Ткаченко Дмитрий Игоревич (UA); Адилжанова Салтанат Альмуханбетовна (KZ); Амирханова Гульшат Аманжоловна (KZ); Амирханов Алихан Бауыржанұлы (KZ)

(73) Амирханов Алихан Бауыржанұлы (KZ)

(56) UA 132302 U, 25.02.2019

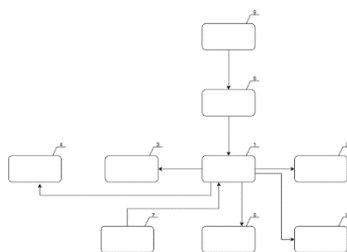
(54) **МОДУЛЬ АУТЕНТИФИКАЦИИ ЦИФРОВОГО ДВОЙНИКА НА ОСНОВЕ ХЕШ-ИДЕНТИФИКАТОРОВ ПРОИЗВОДСТВЕННЫХ ЦИКЛОВ**

(57) Полезная модель относится к области цифровых информационных технологий, промышленной автоматизации и защиты информации и может быть использована в составе киберфизических систем для аутентификации цифровых двойников технологических линий, в частности линий выпечки хлебобулочных изделий.

Модуль включает микроконтроллер, криптографический сопроцессор, сетевой интерфейс, блок сбора технологических параметров, подсистему синхронизации времени,

энергонезависимую память и блок питания. Микроконтроллер принимает параметры производственного цикла (замес, брожение, выпечка, охлаждение), формирует структурированный набор признаков, вычисляет хеш-идентификатор по алгоритму SHA-256, подписывает его криптографическим сопроцессором и передаёт в облачный реестр для проверки подлинности и регистрации данных цифрового двойника.

Технический результат заключается в повышении достоверности, целостности и прослеживаемости производственных данных за счёт криптографической фиксации каждой итерации технологического процесса, обеспечении защиты от подмены телеметрии и повышении прозрачности мониторинга. Основные признаки, обеспечивающие указанный результат, включают использование криптографического сопроцессора, подсистемы синхронизации времени и алгоритма SHA-256 в составе микроконтроллера, выполняющего аутентификацию и передачу данных по защищённому каналу связи.



Фиг. 1 - Модуль аутентификации цифрового двойника на основе хеш-идентификаторов производственных циклов

(19) KZ (13) U (11) 11895

Область техники

Полезная модель относится к области цифровых информационных технологий, промышленной автоматизации и защиты информации и может быть использована в составе киберфизических систем для аутентификации цифровых двойников технологических линий, в частности линий выпечки хлебобулочных изделий.

Уровень техники

Известны устройства и программные комплексы для сбора и передачи производственных данных на базе промышленных контроллеров и систем SCADA/IIoT. Такие решения обеспечивают мониторинг параметров (температуры, влажности, времени, скорости конвейера и т. д.), однако не предусматривают криптографической фиксации каждой итерации производственного цикла, что создаёт риск искажения или подмены данных.

Известен способ и устройство вычисления хэш-функции (патент РФ № 2666303, кл. G06F 17/10, H04L 9/06, 2018 г.), включающее блок предварительной подготовки, модуль конвейерного вычисления и блок объединения. Недостатком данного устройства является отсутствие механизмов аутентификации источника данных и невозможность применения в реальном времени в составе технологической линии.

Наиболее близким аналогом (прототипом) является устройство хеширования цифровых данных по патенту Украины № 132302, в котором микроконтроллер формирует хэш-код данных по алгоритму SHA-256. Недостатком данного устройства является отсутствие структурной связи между хэш-идентификаторами и конкретными итерациями производственного процесса, а также невозможность сверки данных с цифровым двойником.

Сущность полезной модели

Технический результат, достигаемый полезной моделью, заключается в повышении достоверности, целостности и прослеживаемости данных цифрового двойника технологической линии путём формирования уникального хэш-идентификатора для каждой итерации производственного цикла (замес, брожение, выпечка, охлаждение) и их аутентификации в облачном реестре.

Модуль включает микроконтроллер с сетевым интерфейсом, криптографический сопроцессор, блок сбора технологических параметров, подсистему синхронизации времени, энергонезависимую память и блок питания. Микроконтроллер принимает параметры текущего этапа технологического цикла, формирует структурированный набор признаков, вычисляет хэш-значение по алгоритму SHA-256, подписывает его криптографическим сопроцессором и передаёт в облачный реестр для проверки подлинности и регистрации.

Краткое описание чертежа

Фиг.1 — структурная схема модуля аутентификации цифрового двойника, где:

- 1 — микроконтроллер;
- 2 — криптографический сопроцессор;
- 3 — блок ввода и сбора данных;

- 4 — подсистема синхронизации времени;
- 5 — энергонезависимая память;
- 6 — сетевой интерфейс;
- 7 — блок питания;
- 8 — индикаторы состояния;
- 9 — облачный реестр цифрового двойника.

Подробное описание реализации

На Фиг.1 представлена структурная схема модуля аутентификации цифрового двойника.

Модуль содержит микроконтроллер (1), выполняющий обработку технологических параметров, вычисление хэш-идентификатора и управление сетевым обменом; криптографический сопроцессор (2) для аппаратного хранения ключей и формирования подписи; блок ввода данных (3), обеспечивающий приём параметров производственного процесса через промышленные интерфейсы RS-485, CAN, OPC UA, MQTT; подсистему синхронизации времени (4) для фиксации точных временных меток; энергонезависимую память (5) для хранения конфигурации и журналов событий; сетевой интерфейс (6) для передачи данных по защищённому протоколу TLS; блок питания (7) с фильтрацией и стабилизацией напряжения; индикаторы состояния (8) для визуального контроля работы.

В процессе работы модуль получает технологические параметры каждого этапа производственного цикла, нормализует их по заданным диапазонам, формирует структурированный набор признаков (идентификатор линии, номер партии, временные метки, параметры температуры, влажности и скорости). Для этого набора вычисляется хэш-значение алгоритмом SHA-256, формируется сообщение с цифровой подписью, которое передаётся в облачный реестр (9). Реестр проверяет подпись, сверяет данные с эталонными параметрами цифрового двойника и сохраняет результат проверки.

При потере связи модуль сохраняет неподтверждённые сообщения в энергонезависимой памяти и автоматически передаёт их после восстановления канала связи. Защита данных обеспечивается аппаратной изоляцией ключей, аутентификацией по сертификату и контролем целостности прошивки.

Реализация устройства позволяет надёжно фиксировать каждую итерацию производственного процесса и предотвращать фальсификацию данных при передаче и хранении в цифровой модели.

Технический результат

Применение полезной модели обеспечивает:

- аутентификацию источника данных на уровне производственного узла;
- формирование уникальных хэш-идентификаторов производственных циклов;
- контроль целостности цифрового двойника;
- защиту от подмены и повторного воспроизведения телеметрии;
- совместимость с существующими системами SCADA, PLC и IIoT без изменения их структуры;

— повышение надёжности и прозрачности технологического мониторинга.

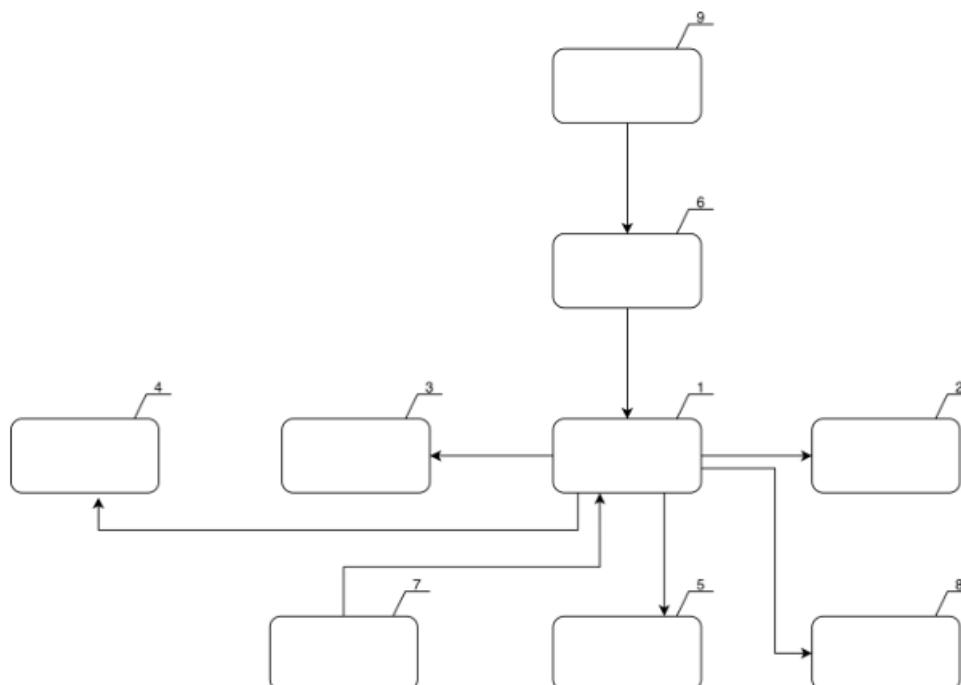
Перечень условных обозначений

- 1 — микроконтроллер;
- 2 — криптографический сопроцессор;
- 3 — блок ввода и сбора данных;
- 4 — подсистема синхронизации времени;
- 5 — энергонезависимая память;
- 6 — сетевой интерфейс;
- 7 — блок питания;
- 8 — индикаторы состояния;
- 9 — облачный реестр цифрового двойника.

ФОРМУЛА ПОЛЕЗНОЙ МОДЕЛИ

Модуль аутентификации цифрового двойника на основе хеш-идентификаторов производственных

циклов, содержащий микроконтроллер, сетевой интерфейс, энергонезависимую память, криптографический сопроцессор, подсистему синхронизации времени и блок ввода технологических параметров, *отличающийся* тем, что он дополнительно содержит блок питания и индикаторы состояния, при этом микроконтроллер выполнен с возможностью приема и нормализации параметров технологического цикла, формирования структурированного набора признаков, вычисления хеш-идентификатора по алгоритму SHA-256, создания аутентифицированного сообщения с цифровой подписью и передачи его в облачный реестр по защищенному протоколу связи для проверки подлинности и регистрации данных цифрового двойника.



Фиг. 1 - Модуль аутентификации цифрового двойника на основе хеш-идентификаторов производственных циклов