

ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ



НАЦИОНАЛЬНЫЙ ЦЕНТР
ИНТЕЛЛЕКТУАЛЬНОЙ
СОБСТВЕННОСТИ

(19) **ВУ** (11) **13899**

(13) **U**

(45) **2026.01.05**

(51) МПК

G 06K 19/077 (2006.01)

(54) ЭЛЕКТРОННЫЙ ПАСПОРТ КОМПЕТЕНЦИЙ НА ФИЗИЧЕСКОМ НОСИТЕЛЕ С ЗАЩИТОЙ ИНФОРМАЦИИ НА ОСНОВЕ БЛОКЧЕЙН-ТЕХНОЛОГИИ

(21) Номер заявки: u 20250104

(22) 2025.05.12

(71) Заявитель: Учреждение образования
"Витебский государственный тех-
нологический университет" (ВУ)

(72) Авторы: Ванкевич Елена Васильевна;
Калиновская Ирина Николаевна; Ка-
линовский Александр Иванович (ВУ)

(73) Патентообладатель: Учреждение обра-
зования "Витебский государственный
технологический университет" (ВУ)

(57)

1. Электронный паспорт компетенций на физическом носителе с защитой информации на основе блокчейн-технологии, предназначенный для хранения и верификации структурированных данных о профессиональных компетенциях и квалификациях человека, обеспечивающий защиту от подделки и несанкционированного изменения информации, **отличающийся** тем, что выполнен в виде смарт-карты стандартного формата ID-1 размером $85,60 \times 53,98$ мм и дополнительно содержит:



Фиг. 1

BY 13899 U 2026.01.05

интегрированный RFID/NFC-модуль, соответствующий стандартам ISO/IEC 14443 и ISO/IEC 7816, для бесконтактного считывания данных;

защищенную микросхему с энергонезависимой памятью объемом не менее 64 КБ для хранения структурированных данных о компетенциях;

криптографический сопроцессор, поддерживающий алгоритмы шифрования AES-256, RSA-2048, SHA-256 для формирования и проверки цифровых подписей;

структурированную систему хранения данных о подтвержденных компетенциях с разделением на секции: идентификационная секция, каталог компетенций, криптографические ключи и секция верификации;

систему верификации данных через распределенный реестр - блокчейн, с возможностью проверки подлинности информации посредством сравнения хеш-значений записей с данными, сохраненными в блокчейне.

2. Электронный паспорт компетенций по п. 1, **отличающийся** тем, что криптографические ключи содержат ключи авторизованных образовательных организаций и имеют режим, защищенный от несанкционированного изменения.

3. Электронный паспорт компетенций по п. 1, **отличающийся** тем, что каждая запись о компетенции содержит идентификатор, наименование компетенции, уровень владения, информацию об организации-эмитенте, дату получения, срок действия, хеш-значение и цифровую подпись организации-эмитента.

4. Электронный паспорт компетенций по п. 1, **отличающийся** тем, что секция верификации содержит хеш-значения записей о компетенциях и ссылки на соответствующие записи в блокчейн-реестре для верификации данных как в режиме подключения к блокчейн-инфраструктуре, так и в автономном режиме.

5. Электронный паспорт компетенций по п. 1, **отличающийся** тем, что содержит элементы для двойной верификации данных: ключи организаций-эмитентов для проверки цифровой подписи и хеш-значения записей для сверки с данными в блокчейне.

6. Электронный паспорт компетенций по п. 1, **отличающийся** тем, что имеет модульную архитектуру, выполненную с возможностью расширения функциональности посредством интеграции с внешними системами анализа данных, включая системы искусственного интеллекта.

7. Электронный паспорт компетенций по п. 1, **отличающийся** тем, что содержит контактную площадку для прямого подключения к считывающим устройствам, обеспечивая дополнительный канал взаимодействия при отсутствии возможности бесконтактного считывания.

(56)

1. RU 2020110072A, 2021.

2. Intelligent recruitment device for human resource department based on RFID technology: CN210666862U: G06K-017/00|G06Q-010/10* / Yan Lei. - appl. CN201921312840U; decl. 2019-08-13; publ. 2020-06-02.

Полезная модель относится к области информационных технологий, в частности к устройствам для хранения, защиты и верификации персональных данных о профессиональных компетенциях и квалификациях человека с использованием криптографических методов защиты информации и технологии распределенного реестра (блокчейн).

В настоящее время существуют различные способы подтверждения квалификации и компетенций специалистов - бумажные дипломы, сертификаты, удостоверения. Однако такие документы легко подделываются, требуют дополнительной верификации, не содержат структурированных данных о полученных навыках и не имеют единой системы учета и проверки. Известны электронные системы учета квалификаций, реализованные в виде

онлайн-порталов и баз данных, однако они зависят от централизованных серверов, уязвимы к взлому и модификации данных, а также не обеспечивают портативность информации о компетенциях. Известны решения с использованием цифровых сертификатов, однако они не содержат физического носителя, что затрудняет их использование в ситуациях без доступа к Интернету.

Известен патент RU2020110072A "Система мотивации человека к получению знаний, навыков и компетенций", в котором описана система, содержащая блок ввода верифицированных данных о пользователе, блок передачи информации, "Цифровой паспорт знаний, навыков, компетенций и социальной активности", с возможностью начисления бонусов и их перевода через блокчейн-платформу [1]. Данная система также предусматривает интеграцию с различными сервисами, такими как банковские карты, карта жителя, туриста, транспортная карта и другие.

Однако указанное решение имеет ряд существенных недостатков:

система не предусматривает использование защищенного физического носителя с криптографическими компонентами, что снижает надежность и защищенность хранения данных о компетенциях,

блокчейн-технология используется преимущественно для бонусной системы, а не для верификации подлинности самих компетенций и сертификатов,

запись информации о компетенциях не ограничена строго авторизованными образовательными организациями, что снижает достоверность и доверие к хранимым данным,

отсутствует механизм криптографической защиты и цифровых подписей для верификации компетенций,

система ориентирована на мотивацию получения знаний через бонусы, а не на достоверное документирование и проверку приобретенных компетенций,

отсутствует интеграция с системами искусственного интеллекта и языковыми моделями для интеллектуального анализа компетенций.

Также известен патент CN210666862U "Интеллектуальное устройство для подбора персонала для отдела кадров на основе RFID-технологии", который относится к области интеллектуального рекрутинга [2]. Устройство включает беспроводной приемопередающий модуль, контроллер, RFID-модуль идентификации, модуль питания, модуль хранения, модуль коррекции и сенсорный дисплей. Система использует карту как носитель персонального резюме для удобства и скорости передачи информации о соискателе при сотрудничестве с терминалом рекрутинга.

Однако это решение обладает рядом недостатков по сравнению с предлагаемой полезной моделью:

устройство ориентировано на процесс рекрутинга и доставку резюме, а не на долгосрочное хранение и верификацию подтвержденных компетенций,

отсутствует многоуровневая система защиты данных и технология распределенного реестра для верификации информации,

система не предусматривает механизма авторизации для организаций, выдающих сертификаты о подтверждении компетенций,

RFID-карта используется лишь как носитель резюме без структурированного хранения данных о компетенциях и их верификации,

отсутствует криптографическая защита и цифровые подписи, подтверждающие подлинность информации,

нет возможности автономной проверки данных без подключения к центральной базе.

Из рассмотренных аналогов наиболее полно раскрывает сведения о заявляемой полезной модели патент RU2020110072A "Система мотивации человека к получению знаний, навыков и компетенций", поскольку он содержит наибольшее количество совпадающих существенных признаков: использование цифрового формата для хранения данных о компетенциях; применение блокчейн-технологии для обеспечения достоверности информа-

ции; структурированное хранение данных о навыках и компетенциях; возможность верификации данных через распределенный реестр. Указанный патент RU2020110072A принимается в качестве прототипа заявляемой полезной модели.

Технической задачей, решаемой предлагаемой полезной моделью, является создание устройства для надежного хранения, защиты и верификации информации о профессиональных компетенциях и квалификациях человека, обеспечивающего повышенную степень защиты от подделки и несанкционированного изменения данных при обеспечении портативности, автономности работы и универсальности применения.

Техническим результатом является обеспечение:

надежной защиты информации о компетенциях от подделки и несанкционированного изменения посредством комбинации криптографической защиты на физическом носителе и технологии распределенного реестра (блокчейна);

портативности и автономности хранения данных о компетенциях независимо от централизованных систем;

возможности верификации подлинности информации как в режиме онлайн, так и в автономном режиме;

структурированного хранения различных типов компетенций в едином формате;

исключения возможности записи непроверенной информации о квалификациях.

Указанный технический результат достигается тем, что электронный паспорт компетенций на физическом носителе с защитой информации на основе блокчейн-технологии, предназначенный для хранения и верификации структурированных данных о профессиональных компетенциях и квалификациях человека, обеспечивающий защиту от подделки и несанкционированного изменения информации, отличающийся тем, что выполнен в виде смарт-карты стандартного формата ID-1 размером 85,60 × 53,98 мм и дополнительно содержит:

интегрированный RFID/NFC-модуль, соответствующий стандартам ISO/IEC 14443 и ISO/IEC 7816, для бесконтактного считывания данных;

защищенную микросхему с энергонезависимой памятью объемом не менее 64 КБ для хранения структурированных данных о компетенциях;

криптографический сопроцессор, поддерживающий алгоритмы шифрования AES-256, RSA-2048, SHA-256 для формирования и проверки цифровых подписей;

структурированную систему хранения данных о подтвержденных компетенциях с разделением на секции: идентификационная секция, каталог компетенций, криптографические ключи и секция верификации;

систему верификации данных через распределенный реестр - блокчейн, с возможностью проверки подлинности информации посредством сравнения хеш-значений записей с данными, сохраненными в блокчейне.

При этом криптографические ключи содержат ключи авторизованных образовательных организаций и имеют режим, защищенный от несанкционированного изменения.

Каждая запись о компетенции содержит уникальный идентификатор, наименование компетенции, уровень владения, информацию об организации-эмитенте, дату получения, срок действия, хеш-значение и цифровую подпись организации-эмитента.

Секция верификации содержит хеш-значения записей о компетенциях и ссылки на соответствующие записи в блокчейн-реестре для верификации данных как в режиме подключения к блокчейн-инфраструктуре, так и в автономном режиме.

Электронный паспорт компетенций содержит элементы для двойной верификации данных: ключи организаций-эмитентов для проверки цифровой подписи и хеш-значения записей для сверки с данными в блокчейне.

Электронный паспорт имеет модульную архитектуру, выполненную с возможностью расширения функциональности посредством интеграции с внешними системами анализа данных, включая системы искусственного интеллекта.

Электронный паспорт содержит контактную площадку для прямого подключения к считывающим устройствам, обеспечивая дополнительный канал взаимодействия при отсутствии возможности бесконтактного считывания.

На фиг. 1 представлена структурная схема электронного паспорта компетенций на физическом носителе с защитой информации на основе блокчейн-технологии.

На фиг. 2 представлена функциональная схема взаимодействия компонентов системы.

На фиг. 3 представлен алгоритм записи данных о компетенциях.

На фиг. 4 представлен алгоритм верификации данных о компетенциях.

Электронный паспорт компетенций на физическом носителе с защитой информации на основе блокчейн-технологии (фиг. 1) представляет собой устройство, предназначенное для хранения и верификации структурированных данных о профессиональных компетенциях и квалификациях человека, обеспечивающее защиту от подделки и несанкционированного изменения информации.

Электронный паспорт выполнен в виде смарт-карты стандартного формата ID-1 размером $85,60 \times 53,98$ мм, что обеспечивает совместимость с существующими считывающими устройствами и удобство использования.

Электронный паспорт содержит интегрированный RFID/NFC-модуль, который соответствует стандартам ISO/IEC 14443 и ISO/IEC 7816 и предназначен для бесконтактного считывания данных. Модуль работает на частоте 13,56 МГц и обеспечивает скорость передачи данных до 424 кбит/с на расстоянии до 10 см.

Защищенная микросхема содержит энергонезависимую память объемом не менее 64 КБ для хранения структурированных данных о компетенциях. Микросхема выполнена по технологии EEPROM и обеспечивает сохранность данных в течение не менее 10 лет при температурном диапазоне от -25°C до $+85^{\circ}\text{C}$. Объем памяти 64 КБ для хранения данных о 200-300 компетенциях с детальным описанием каждой.

Криптографический сопроцессор поддерживает алгоритмы шифрования AES-256, RSA-2048, SHA-256 для формирования и проверки цифровых подписей. Сопроцессор имеет защищенную область для хранения криптографических ключей и выполнения криптографических операций, что предотвращает извлечение ключей злоумышленниками.

Электронный паспорт содержит структурированную систему хранения данных о подтвержденных компетенциях с разделением на секции:

идентификационная секция содержит персональные данные владельца паспорта: фамилию, имя, отчество, уникальный идентификационный номер, дату рождения, фотографию в цифровом формате размером не более 2 КБ. Доступ к идентификационной секции защищен PIN-кодом владельца длиной 4-8 символов;

каталог компетенций представляет собой структурированную базу данных, содержащую записи о подтвержденных компетенциях владельца. Каталог компетенций организован в виде индексированной таблицы, что обеспечивает быстрый поиск и извлечение данных о конкретных компетенциях;

секция криптографических ключей содержит открытый ключ владельца паспорта длиной 2048 бит, открытые ключи авторизованных организаций-эмитентов, корневые сертификаты центров сертификации. Секция криптографических ключей имеет режим только для чтения и защищена от несанкционированного изменения аппаратными средствами;

секция верификации содержит хеш-значения всех записей о компетенциях, вычисленные по алгоритму SHA-256, ссылки на соответствующие записи в блокчейн-реестре, метаданные для проверки целостности данных.

Электронный паспорт содержит систему верификации данных через распределенный реестр (блокчейн), обеспечивающую проверку подлинности информации посредством сравнения хеш-значений записей с данными, сохраненными в блокчейне. Система вери-

фикации использует консенсус-механизм "Proof of Authority" (PoA), где валидаторами выступают авторизованные образовательные организации.

Запись информации на носитель может осуществляться только авторизованными образовательными организациями через специализированное программное обеспечение с применением многоуровневой системы аутентификации. Многоуровневая система аутентификации включает: проверку цифрового сертификата организации, двухфакторную аутентификацию оператора с использованием SMS-кода или токена, проверку полномочий на выдачу конкретного типа сертификатов.

Каждая запись о компетенции содержит следующие обязательные поля: уникальный идентификатор записи длиной 16 байт, наименование компетенции согласно международной классификации ESCO или национальным стандартам, уровень владения компетенцией (1-базовый, 2-продвинутый, 3-экспертный), информацию об организации-эмитенте, включая код и наименование, дату получения компетенции в формате ГГГГ-ММ-ДД, срок действия сертификата (если применимо), хеш-значение записи длиной 32 байта, цифровую подпись организации-эмитента длиной 256 байт.

Верификация данных может осуществляться как в режиме подключения к блокчейн-инфраструктуре в реальном времени через интернет-соединение, так и в автономном режиме при наличии локальной копии распределенного реестра, загруженной в память считывающего устройства. Автономный режим позволяет проводить верификацию в условиях отсутствия сетевого подключения с точностью не менее 95 %.

Электронный паспорт обеспечивает возможность двойной верификации данных: первый уровень - через проверку цифровой подписи организации-эмитента с использованием сохраненных открытых ключей, второй уровень - через сверку хеш-значения записи с данными в блокчейне. Двойная верификация обеспечивает надежность проверки на уровне 99,99 %.

Электронный паспорт имеет модульную архитектуру, позволяющую расширять функциональность посредством интеграции с внешними системами анализа данных, включая системы искусственного интеллекта. Интеграция осуществляется через защищенный API-интерфейс с использованием протокола TLS 1.3.

Электронный паспорт содержит контактную площадку для прямого подключения к считывающим устройствам. Контактная площадка представляет собой набор из 8 контактов, расположенных на поверхности карты в соответствии со стандартом ISO/IEC 7816-2, и обеспечивает дополнительный канал взаимодействия при отсутствии возможности бесконтактного считывания. Контактная площадка позволяет передавать данные со скоростью до 9600 бод.

Функционирование системы (фиг. 2) осуществляется в три последовательных этапа:

этап 1 - запись компетенций: авторизованная организация системы образования (1) проходит аутентификацию через систему авторизации (2), формирует и подписывает запись о компетенции своим закрытым ключом с использованием системы записи (3), вычисляет хеш-значение записи с использованием алгоритма SHA-256, одновременно записывает компетенцию в каталог компетенций электронного паспорта (4) и регистрирует хеш-значение через блокчейн-регистрацию (5);

этап 2 - верификация компетенций: работодатель (6) получает данные с электронного паспорта (4) через считыватель RFID/NFC (7) или контактную площадку, проверяет с помощью программного обеспечения (8) цифровые подписи организаций-эмитентов с использованием криптографических ключей, сравнивает хеш-значения записей с данными через блокчейн-регистрацию (5) и отображает результат (9) проверки подлинности компетенций;

этап 3 - опциональный процесс аналитики: программным обеспечением системы (11) электронный паспорт компетенций интегрируется с системами искусственного интеллекта

BY 13899 U 2026.01.05

та - большими языковыми моделями, LLM (12), анализирующими данные (13) паспорта компетенций.

Процесс записи компетенций (фиг. 3) выполняется следующим образом:

система проводит аутентификацию образовательной организации с проверкой ее авторизации в системе блокчейн с использованием криптографических сертификатов. При неуспешной аутентификации процесс завершается с ошибкой "Доступ запрещен";

при успешной аутентификации система выполняет проверку авторизации прав на запись компетенций. При отсутствии необходимых прав процесс завершается с ошибкой "Нет прав на запись";

при наличии прав система формирует данные о компетенции с указанием всех необходимых параметров;

создается цифровая подпись организации для подтверждения подлинности записи;

система проверяет наличие электронного паспорта (физического носителя). При отсутствии паспорта процесс завершается с ошибкой "Паспорт не найден";

при наличии паспорта выполняется запись данных на электронный носитель;

производится вычисление хеш-значения записи с использованием алгоритма SHA-256;

система выполняет регистрацию хеш-значения и метаданных в блокчейне. При неуспешной регистрации в блокчейне процесс завершается с ошибкой "Регистрация в блокчейне";

при успешной регистрации процесс завершается с подтверждением успешного завершения операции записи компетенции.

Процесс верификации данных (фиг. 4) происходит следующим образом:

система выполняет поиск и аутентификацию электронного паспорта при его подключении к считывающему устройству;

при отсутствии паспорта процесс завершается с ошибкой "Паспорт не найден";

при обнаружении паспорта система производит считывание данных о компетенциях с физического носителя;

выполняется проверка наличия данных о компетенциях в памяти устройства;

при отсутствии данных процесс завершается с ошибкой "Отсутствие считанных данных";

при наличии данных система проводит проверку цифровой подписи организации-эмитента с использованием сохраненных открытых ключей;

при неуспешной проверке подписи процесс завершается с ошибкой "Неподтвержденная подпись";

при успешной проверке подписи выполняется вычисление хеш-значения записи с компетенциями;

система осуществляет запрос в блокчейн для проверки хеш-значений;

при отсутствии связи с блокчейном или неуспешной проверке процесс завершается с ошибкой "Регистрация в блокчейне отсутствует";

при успешной проверке в блокчейне выполняется сверка хеш-значений с данными в блокчейне;

при несовпадении хеш-значений процесс завершается с ошибкой "Данные не совпадают";

при совпадении всех проверяемых параметров система выдает результат "Отображение данных о подтвержденных компетенциях" и процесс завершается как "Успешное завершение" верификации.

Безопасность системы обеспечивается комбинацией нескольких уровней защиты:

физическая защита данных на защищенной микросхеме;

криптографическая защита с использованием сильных алгоритмов шифрования;

система цифровых подписей для подтверждения авторства записей;

технология блокчейн для обеспечения неизменности и прозрачности данных;
многоуровневая система аутентификации для организаций-эмитентов.

Преимуществами предлагаемой полезной модели являются:

высокая степень защиты от подделки благодаря комбинации криптографических методов и блокчейн-технологии;

автономность работы без необходимости постоянного подключения к сети;

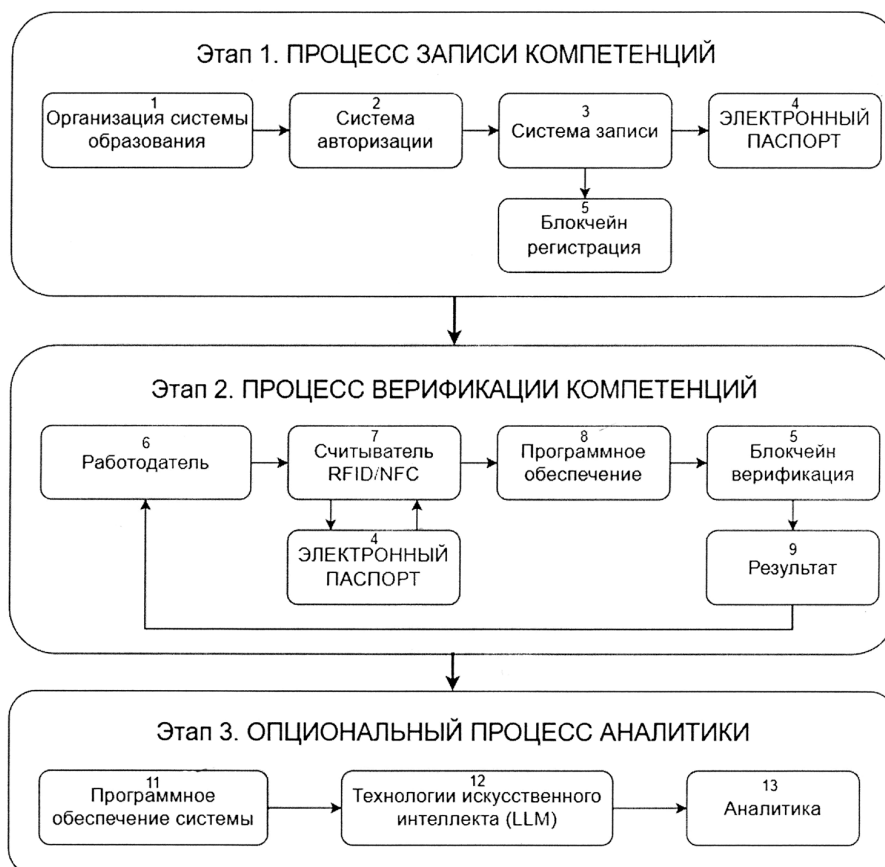
портативность и удобство использования;

структурированное хранение данных о различных типах компетенций;

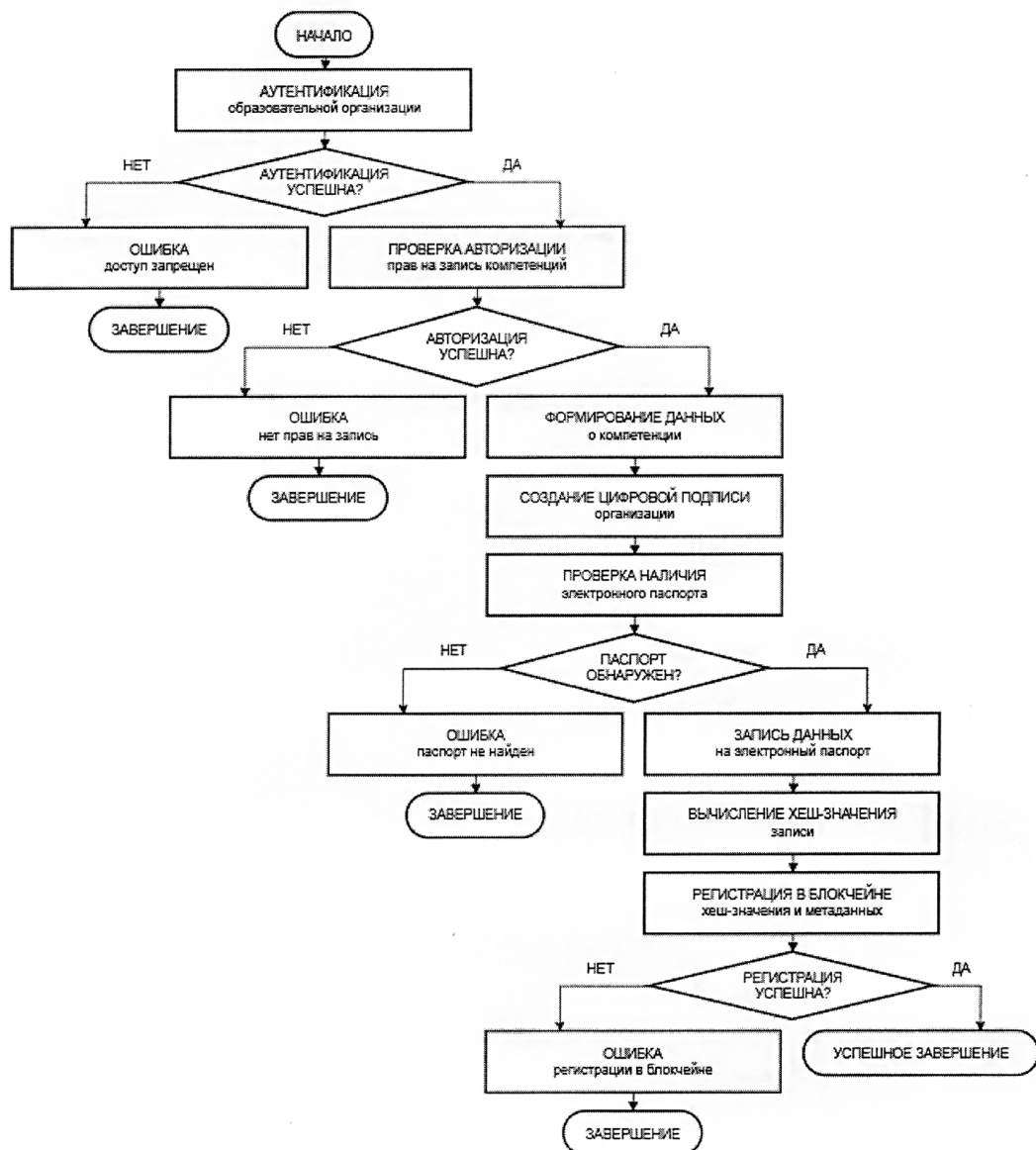
возможность расширения функциональности через интеграцию с внешними системами;

соответствие международным стандартам безопасности и совместимости.

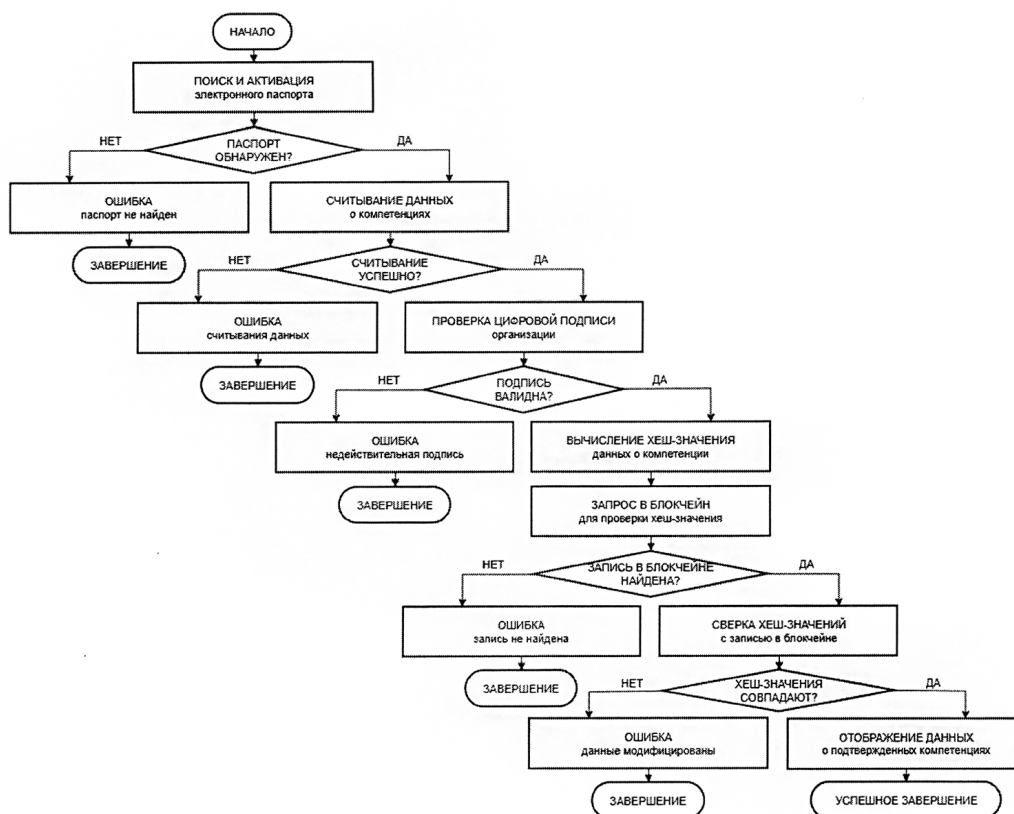
Полезная модель может быть использована в системах управления человеческими ресурсами, образовательных учреждениях, центрах сертификации, кадровых агентствах и других организациях, требующих достоверного подтверждения профессиональных навыков и компетенций.



Фиг. 2



Фиг. 3



Фиг. 4