Научная статья
УДК 004.056:004.421; DOI: 10.61260/2218-13X-2026-1-102-115

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМЫ ЭЛЕКТРОННЫХ ТЕХНИЧЕСКИХ ПАСПОРТОВ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В ЦЕЛЯХ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ РАЗВИТИЕМ СЛОЖНЫХ СИСТЕМ

✉Ефимов Алексей Олегович;
Зверев Георгий Игоревич;
Рогозин Евгений Алексеевич.
Воронежский институт МВД России, г. Воронеж, Россия.
Калач Андрей Владимирович.
Воронежский институт ФСИН России, г. Воронеж, Россия
✉ea.aleksei@yandex.ru

Аннотация. Рассматривается возможность применения блокчейн-технологии для автоматизированного ведения технических паспортов информационных систем. Проведен анализ традиционных методов ведения документации, выявлены их недостатки, включая высокие временные затраты, сложность аудита и риск несанкционированного изменения данных. Предложена концепция электронной системы технических паспортов, основанная на децентрализованном реестре и использовании смарт-контрактов для автоматического контроля изменений конфигурации и обновлений программного обеспечения. Результаты моделирования показали, что внедрение блокчейн-технологии позволяет сократить время обработки изменений с 4–6 ч при традиционном подходе до 3–5 мин, что эквивалентно ускорению процесса в 50–100 раз. Обеспечивается неизменяемость записей, прозрачность операций и автоматическая проверка данных на соответствие требованиям безопасности. Разработанная система повышает эффективность управления информационной безопасностью, снижает влияние человеческого фактора и упрощает процесс аудита. Предложенное решение является перспективным для внедрения в критически важные автоматизированные системы, где требуется строгий контроль за состоянием и безопасностью информационных ресурсов. Дальнейшие исследования могут быть направлены на интеграцию с системами мониторинга угроз и разработку механизмов адаптивного управления доступом к данным в блокчейн-реестре.

Ключевые слова: блокчейн-технология, технические паспорта, информационные системы, децентрализованный реестр, смарт-контракты, управление изменениями, конфигурация программного обеспечения, безопасность данных, информационная безопасность, автоматизация процессов, неизменяемость записей, аудиторский контроль, мониторинг угроз, управление доступом, эффективность управления, автоматизированные системы, критически важные системы

Для цитирования: Концептуальные основы построения системы электронных технических паспортов информационных систем на основе технологии блокчейн в целях повышения эффективности мероприятий по защите информации и обеспечения управления развитием сложных систем / А.О. Ефимов [и др.] // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2026. № 1. С. 102–115. DOI: 10.61260/2218-13X-2026-1-102-115

© Санкт-Петербургский университет ГПС МЧС России, 2026

Scientific article

CONCEPTUAL FOUNDATIONS FOR BUILDING A SYSTEM OF ELECTRONIC TECHNICAL PASSPORTS OF INFORMATION SYSTEMS BASED ON BLOCKCHAIN TECHNOLOGY IN ORDER TO IMPROVE THE EFFICIENCY OF INFORMATION PROTECTION MEASURES AND ENSURE THE MANAGEMENT OF THE DEVELOPMENT OF COMPLEX SYSTEMS

✉Efimov Alexey O.;
Zverev Georgiy I.;
Rogozin Evgeniy A.
Voronezh Institute of the Ministry of the Interior of Russia, Voronezh, Russia.
Kalach Andrey V.
Voronezh Institute of the Federal Penitentiary Service of Russia, Voronezh, Russia
✉ea.aleksei@yandex.ru

Abstract. The article considers the possibility of using blockchain technology for automated maintenance of technical data sheets of information systems. An analysis of traditional documentation management methods has been carried out, and their disadvantages have been identified, including high time costs, audit complexity, and the risk of unauthorized data modification. The concept of an electronic technical passport system based on a decentralized registry and the use of smart contracts for automatic control of configuration changes and software updates is proposed. The simulation results showed that the introduction of blockchain technology reduces the processing time of changes from 4–6 hours with the traditional approach to 3–5 minutes, which is equivalent to speeding up the process by 50–100 times. The immutability of records, transparency of operations and automatic verification of data for compliance with security requirements are ensured. The developed system increases the efficiency of information security management, reduces the influence of the human factor and simplifies the audit process. The proposed solution is promising for implementation in mission-critical automated systems where strict control over the state and security of information resources is required. Further research may be aimed at integrating with threat monitoring systems and developing adaptive data access control mechanisms in the blockchain registry.

Keywords: blockchain technology, technical data sheets, information systems, decentralized registry, smart contracts, change management, software configuration, data security, information security, process automation, immutability of records, audit control, threat monitoring, access control, management efficiency, automated systems, critical systems

For citation: Conceptual foundations for building a system of electronic technical passports of information systems based on blockchain technology in order to improve the efficiency of information protection measures and ensure the management of the development of complex systems / A.O. Efimov [et al.] // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2026. № 1. P. 102–115. DOI: 10.61260/2218-13X-2026-1-102-115

Введение

В современных условиях информационная безопасность (ИБ) становится неотъемлемой частью функционирования автоматизированных систем. Одним из ключевых элементов обеспечения защищённости таких систем является их технический паспорт, регламентирующий параметры, конфигурацию и меры защиты. Согласно источнику [1], технические паспорта традиционно ведутся в бумажном виде, что сопряжено с рядом ограничений: сложностью актуализации данных, высоким риском утраты информации, а также недостаточной оперативностью при проведении проверок и аудита.

Развитие технологий распределённых реестров, в частности блокчейн, открывает новые возможности для модернизации этого процесса. Электронные технические паспорта (ЭТП) на основе блокчейн-технологии способны устранить существующие недостатки традиционного подхода, обеспечивая неизменяемость, прозрачность и автоматизацию актуализации данных. Такая система позволяет оперативно отслеживать изменения в конфигурации автоматизированных систем, фиксировать версии программного обеспечения (ПО) и выявлять уязвимости, используя механизмы интеллектуального анализа данных.

В данной статье рассматривается концепция внедрения электронной вариации технических паспортов автоматизированных систем, анализируются её преимущества перед традиционным подходом, а также предлагаются архитектурные решения для её реализации.

Описание проблемы и существующие решения

Технический паспорт автоматизированной системы является обязательным документом, содержащим сведения о её конфигурации, составе, характеристиках, мерах защиты информации и регламентных мероприятиях. В соответствии с источником [1], данный документ традиционно ведётся в бумажной форме, что влечёт за собой ряд проблем.

Во-первых, бумажный формат усложняет процесс актуализации данных. Любые изменения в конфигурации системы требуют ручного внесения корректировок, что повышает вероятность ошибок и задержек. В результате информация в техническом паспорте может устаревать быстрее, чем обновляется, что снижает эффективность управления безопасностью.

Во-вторых, бумажные технические паспорта требуют централизованного хранения, что создаёт риск их физического повреждения, утраты или несанкционированного доступа. Кроме того, процесс аудита и проверки соответствия системы требованиям безопасности занимает значительное время, так как требует физического поиска, сверки и анализа документов.

В-третьих, отсутствие автоматизированного механизма отслеживания изменений ПО затрудняет выявление потенциальных уязвимостей. В современных условиях киберугроз своевременное обновление информации о программных продуктах, применяемых в автоматизированных системах, является критически важным аспектом защиты данных.

Существующие решения для управления технической документацией включают в себя цифровые базы данных, в которых хранятся электронные копии технических паспортов. Такие системы позволяют частично решить проблему хранения и поиска информации, но не обеспечивают её неизменяемости, прозрачности и автоматического отслеживания изменений. Дополнительные системы контроля версий ПО применяются отдельно и не интегрированы с механизмами технических паспортов.

Далее авторами рассмотрены наиболее близкие по тематике работы.

В статье [2] изучается инновационное значение применения технологии блокчейн в системе управления. Авторы анализируют потенциал блокчейна для повышения эффективности управленческих процессов и снижения операционных рисков. В работе [3] исследуется интеграция блокчейна в системы электронного документооборота (EDM) в строительной отрасли. Авторы предлагают модель объединения блокчейн-технологий с существующими EDM-системами для обеспечения безопасности и прозрачности данных. В работе [4] исследователи предлагают механизм кросс-цепочки для управления документами сельскохозяйственной инженерии на основе блокчейна в условиях больших данных. Исследование направлено на улучшение совместимости и обмена данными между различными блокчейн-сетями в аграрном секторе. В исследовании [5] авторы рассматривают концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости. Авторы предлагают методы анализа и оценки рисков для

повышения ИБ. В статье [6] авторы исследуют безопасность смарт-контрактов в сети Ethereum. В работе анализируются потенциальные уязвимости и предлагаются методы их предотвращения. В исследовании [7] обсуждают ИБ в EDM с применением технологии блокчейн. Авторы подчеркивают преимущества блокчейна для защиты данных и обеспечения их целостности. В работе [8] авторы проводят анализ стандартов обеспечения ИБ. В работе сравниваются различные подходы и стандарты для выявления лучших практик в области защиты информации. В статье [9] исследуют методики контроля уровня защищенности информации на объектах критической информационной инфраструктуры. Авторы предлагают подходы к мониторингу и оценке безопасности в критически важных системах. В работе [10] автор представляет формализованную модель аудита ИБ организации на предмет соответствия требованиям стандартов. Работа направлена на улучшение процессов аудита и соответствия нормативным требованиям. Статья [11] посвящена изучению управления ИБ и кибербезопасностью на примере малых и средних предприятий в Португалии. В исследовании рассматриваются практики и вызовы обеспечения безопасности в небольших организациях. Работа [12] посвящена оценке эффективности аудита кибербезопасности. Авторы анализируют методы и подходы к аудиту для повышения уровня защиты информационных систем. В работе [13] исследователи рассматривают оценки рисков ИБ после инцидентов кибербезопасности, уделяя внимание роли высшего руководства в обеспечении безопасности. В статье [14] проводят всесторонний анализ инструментов аудита безопасности устройств Интернета вещей (IoT) и предлагают многоуровневый подход к расширенным требованиям безопасности.

Несмотря на обилие исследований в области применения блокчейн-технологий для обеспечения ИБ и управления данными, тема использования блокчейна для автоматизированного ведения технических паспортов информационных систем остается недостаточно изученной. Необходимо рассмотреть концептуальные основы применения блокчейн-технологий в этой специфической области, чтобы определить их потенциал и возможные преимущества.

Применение технологии блокчейн в данном контексте может предложить кардинально новый подход, обеспечивая децентрализованное хранение информации, неизменяемость записей, автоматическое отслеживание изменений в конфигурации системы и версий ПО. Это позволит устранить большинство недостатков традиционного бумажного формата и существующих цифровых решений, повысив оперативность и эффективность мероприятий по защите информации.

Постановка задачи

Цель исследования: разработать концепцию системы ЭТП автоматизированных систем на основе технологии блокчейн, обеспечивающую автоматизацию актуализации данных, контроль версий ПО и выявление уязвимостей.

Задачи:

1. Провести анализ существующих подходов к ведению технических паспортов автоматизированных систем, выявить их недостатки и ограничения.
2. Рассмотреть возможности применения технологии блокчейн для построения системы ЭТП, определить её преимущества и потенциальные риски.
3. Разработать модель системы, включающую механизм автоматизированной обработки информации о состоянии автоматизированных систем с использованием блокчейн-технологии.
4. Смоделировать процесс функционирования электронной системы технических паспортов, включая сценарии актуализации данных, мониторинга версий ПО и выявления уязвимостей.
5. Оценить эффективность предложенного решения, сравнив его с традиционными методами ведения технических паспортов.

Описание применения блокчейн-технологии в целях построения системы ЭТП информационных систем

Технология блокчейн представляет собой распределённый реестр, обеспечивающий неизменяемость и целостность данных за счёт использования криптографических механизмов и децентрализованного хранения. Внедрение данной технологии в процесс ведения технических паспортов информационных систем позволит устранить недостатки традиционного бумажного формата, а также цифровых решений, основанных на централизованных базах данных. Основное преимущество блокчейн заключается в его способности фиксировать изменения без возможности их незаметного редактирования, что обеспечивает высокий уровень прозрачности и надёжности данных.

В контексте ЭТП применение блокчейн направлено на автоматизированное ведение записей о конфигурации информационной системы, актуализацию сведений о ПО и оборудовании, а также регистрацию инцидентов ИБ. Вся информация, включающая идентификаторы программных продуктов, их версии, применяемые меры защиты и историю изменений, фиксируется в блокчейн-реестре с временными метками, исключая возможность подмены данных или их утраты. Каждый новый блок включает хеш предыдущего, обеспечивая криптографическую связанность записей и невозможность их изменения без фиксации корректировок.

Ключевым элементом системы являются смарт-контракты, которые автоматизируют проверку соответствия вносимых данных установленным требованиям. Например, при обновлении ПО смарт-контракт может автоматически сверять установленную версию с базой известных уязвимостей и предупреждать администратора о необходимости принятия дополнительных мер защиты. Аналогично могут реализовываться механизмы контроля за соблюдением политик ИБ, в том числе автоматическая сверка конфигурации системы с нормативными требованиями.

Дополнительное преимущество заключается в интеграции с системами мониторинга безопасности, что позволит автоматически заносить в технический паспорт информацию о выявленных уязвимостях и предпринимаемых мерах их устранения. Таким образом, аудиторы и администраторы смогут в режиме реального времени отслеживать состояние системы, получать данные о её изменениях и формировать отчёты без необходимости ручного анализа документов.

Внедрение блокчейн в процесс ведения технических паспортов информационных систем позволит значительно повысить эффективность управления безопасностью за счёт автоматизации обновления данных, сокращения временных затрат на аудит и исключения рисков фальсификации информации. Это создаст условия для перехода к принципиально новому уровню контроля за состоянием защищённости автоматизированных систем, обеспечивая высокий уровень достоверности и оперативности принятия решений в сфере ИБ.

Моделирование процесса автоматизированной обработки информации о состоянии информационных систем посредством блокчейн-технологии

Моделирование процесса автоматизированной обработки информации о состоянии информационных систем посредством блокчейн-технологии основано на формировании структуры взаимодействия между элементами системы ЭТП. Для наглядного изображения процессов и визуализации модели функционирования приведенных алгоритмов предлагается использовать унифицированный язык моделирования.

Диаграммы унифицированного языка моделирования, или UML-диаграммы, являются инструментом для представления сложных систем и процессов [15, 16]. Они обеспечивают формальный способ описания структуры и поведения системы, делая ее более доступной для анализа, проектирования и разработки. В рамках настоящей работы предлагается привести следующие диаграммы: диаграмма вариантов использования, диаграмма классов, диаграмма последовательностей, диаграмма активности и диаграмма развертывания.

На рис. 1 представлена диаграмма вариантов использования. Она отражает основные роли и их взаимодействие с системой ЭТП на блокчейне.

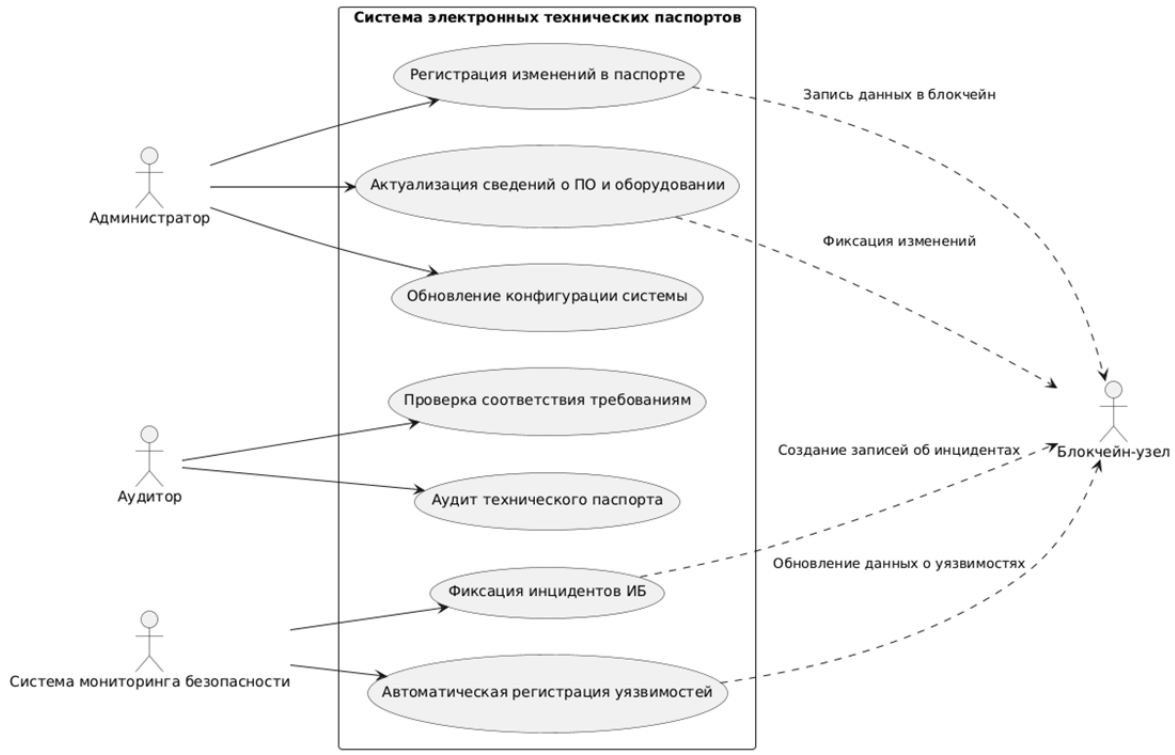

Рис. 1. **Диаграмма вариантов использования**

Основными ролями или акторами в соответствии с описываемой диаграммой являются:

1. Администратор – вносит изменения в паспорт, обновляет данные о ПО и конфигурации.
2. Аудитор – проверяет соответствие системы требованиям, проводит аудит.
3. Система мониторинга безопасности – фиксирует инциденты и обнаруженные уязвимости.
4. Блокчейн-узел – фиксирует изменения, обеспечивая их неизменность.

Варианты использования системы:

1. Регистрация изменений в паспорте – фиксирует любую правку, вносимую администратором.
2. Актуализация сведений о ПО и оборудовании – обновляет информацию в блокчейне.
3. Проверка соответствия требованиям – автоматически оценивает конфигурацию системы.
4. Аудит технического паспорта – анализ состояние системы.
5. Фиксация инцидентов ИБ – система мониторинга фиксирует события безопасности.
6. Автоматическая регистрация уязвимостей – система мониторинга обновляет сведения о найденных угрозах.
7. Обновление конфигурации системы – внесение изменений в настройки.

На рис. 2 представлена диаграмма классов, описывающей основные сущности системы ЭТП.

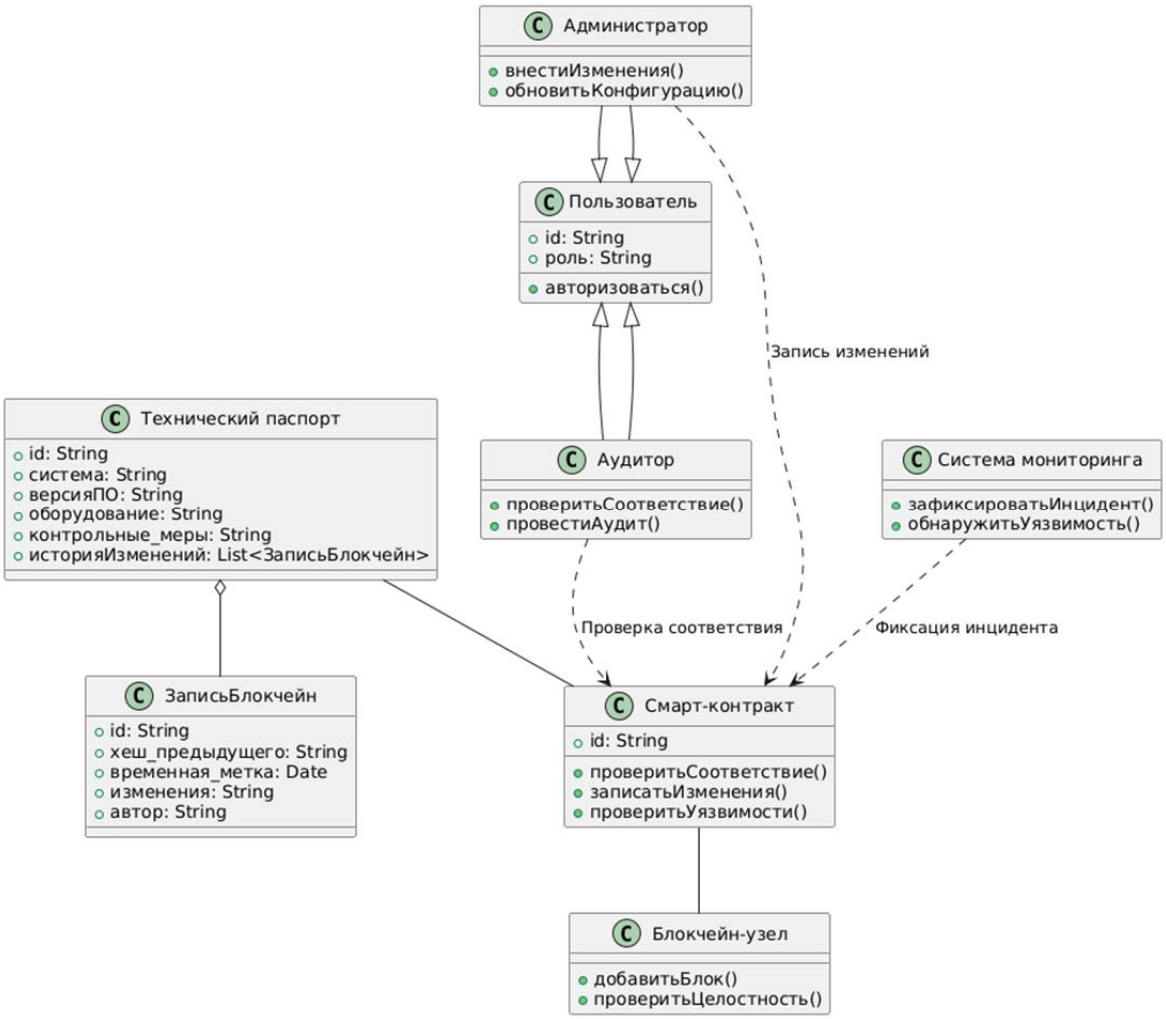

Рис. 2. **Диаграмма классов**

Основные сущности и их атрибуты, представленные в диаграмме:

1. Технический паспорт – хранит сведения о системе, ПО, оборудовании, мерах защиты и истории изменений.

2. Запись_Блокчейн – отдельная запись в блокчейне, содержащая хеш предыдущего блока, временную метку и автора изменений.

3. Смарт-контракт – выполняет проверку соответствия, записывает изменения, анализирует уязвимости.

4. Пользователь (базовый класс) – представляет участников системы (администратор, аудитор).

5. Администратор – вносит изменения, обновляет конфигурацию.

6. Аудитор – проверяет соответствие системы требованиям, проводит аудит.

7. Система мониторинга – фиксирует инциденты, выявляет уязвимости.

8. Блокчейн-узел – выполняет функции хранения и проверки данных.

Связи между классами можно описать следующим образом: технический паспорт агрегирует записи блокчейна; смарт-контракт взаимодействует с техническим паспортом и блокчейн-узлом; администратор записывает изменения в паспорт через смарт-контракты; аудитор проверяет соответствие системы требованиям; система мониторинга фиксирует инциденты и передаёт данные в блокчейн.

На рис. 3 представлена диаграмма последовательностей. Она иллюстрирует процесс внесения изменений в ЭТП с фиксацией данных в блокчейне и проверкой соответствия смарт-контрактом.

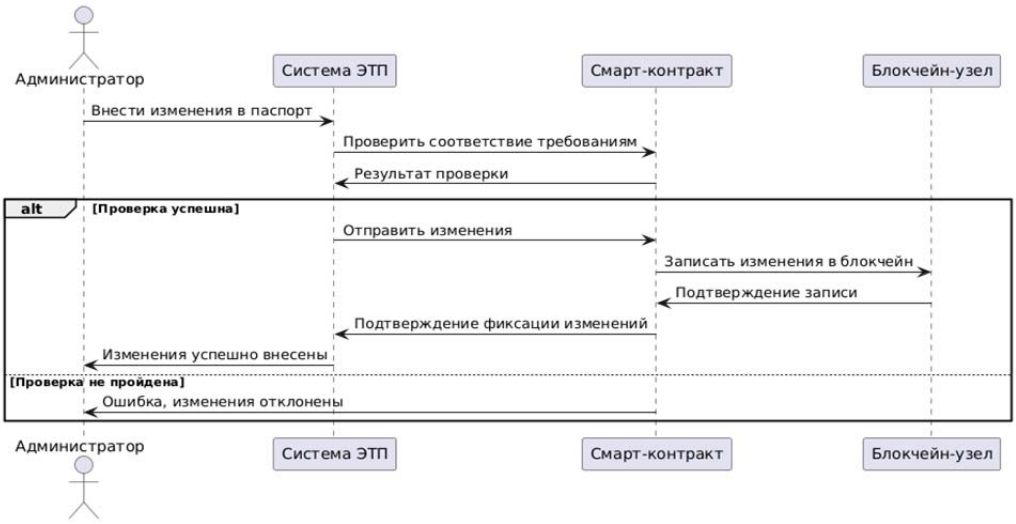

Рис. 3. **Диаграмма последовательностей**

Описание последовательности, которая определяется приведенной диаграммой:

1. Администратор отправляет запрос на внесение изменений в ЭТП.
2. Система ЭТП передаёт данные в смарт-контракт для проверки на соответствие требованиям.
3. Смарт-контракт возвращает результат проверки.
4. Если проверка успешна, изменения фиксируются в блокчейне:

– система ЭТП передаёт изменения смарт-контракту;

– смарт-контракт записывает их в блокчейн-узел;

– блокчейн-узел подтверждает запись;

– система ЭТП уведомляет администратора об успешном изменении.

5. Если проверка не пройдена, администратор получает сообщение об ошибке, и изменения отклоняются.

На рис. 4 представлена диаграмма активности, которая описывает процесс обновления ЭТП с проверкой на соответствие требованиям и фиксацией изменений в блокчейне.

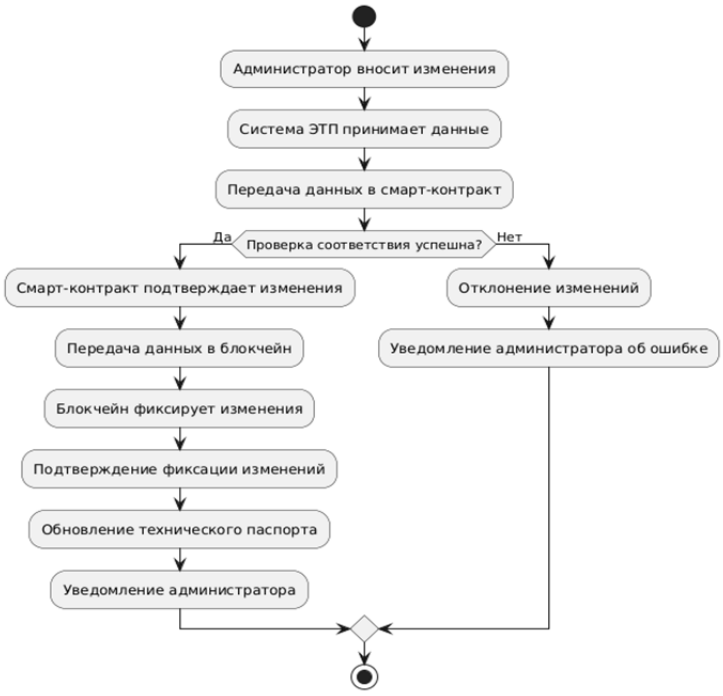

Рис. 4. **Диаграмма активности**

Описание активности:

1. Администратор вносит изменения в ЭТП.

2. Система ЭТП принимает данные и передаёт их смарт-контракту.

3. Смарт-контракт проверяет соответствие требованиям:

– если проверка успешна, данные записываются в блокчейн, обновляется технический паспорт, и администратор получает подтверждение;

– если проверка не пройдена, изменения отклоняются, а администратор получает уведомление об ошибке.

На рис. 5 представлена диаграмма развертывания, которая показывает архитектуру развертывания системы ЭТП.

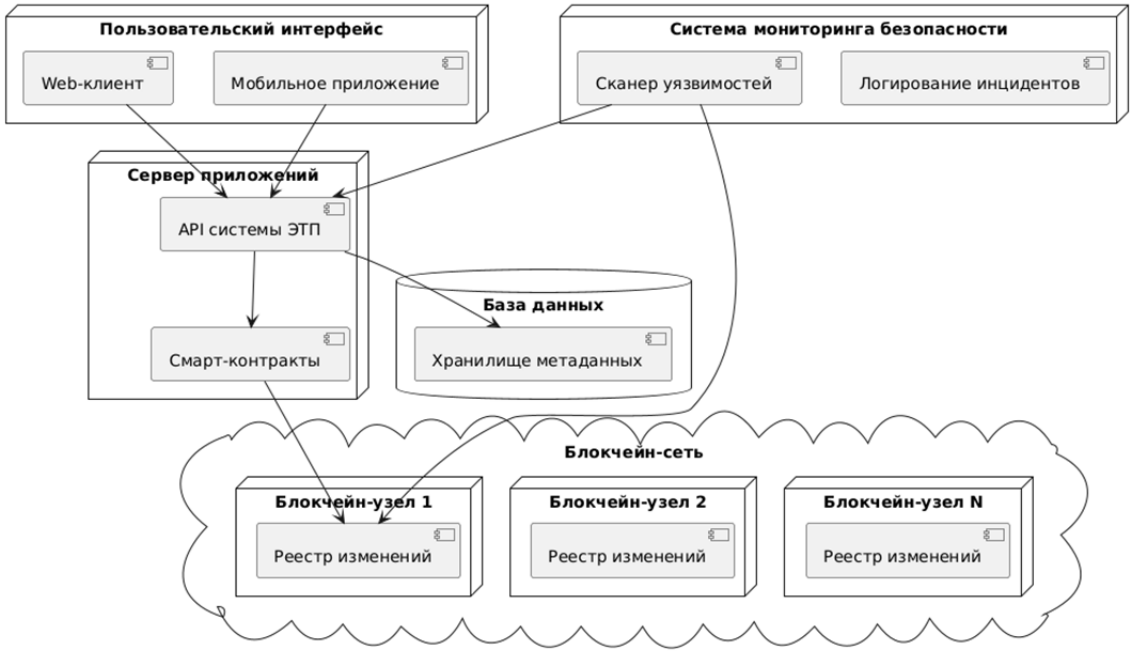

Рис. 5. **Диаграмма развертывания**

Описываемая диаграмма компонентов развертывания:

1. Пользовательский интерфейс.

Включает Web-клиент и мобильное приложение, через которые администраторы и аудиторы работают с системой.

2. Сервер приложений

Содержит программный интерфейс приложений (API) системы ЭТП для взаимодействия с клиентами. Запускает смарт-контракты для проверки соответствия и фиксации изменений.

3. Блокчейн-сеть.

Включает несколько узлов (блокчейн-узел 1, 2, *N*), которые хранят неизменяемый реестр изменений технического паспорта.

4. Система мониторинга безопасности.

Содержит сканер уязвимостей, фиксирующий найденные угрозы. Ведёт логирование инцидентов и передаёт их в систему ЭТП и блокчейн.

5. База данных.

Содержит хранилище метаданных, в котором хранятся вспомогательные данные (например, ссылки на блокчейн-записи).

Основные связи между компонентами: Web-клиент и мобильное приложение взаимодействуют с API системы ЭТП. API системы ЭТП вызывает смарт-контракты, которые фиксируют изменения в блокчейн-узлах. Система мониторинга безопасности передаёт информацию об инцидентах и уязвимостях в реестр изменений. API системы ЭТП записывает вспомогательные данные в базу данных.

Далее авторами проводится сравнительный анализ эффективности ведения технических паспортов.

Традиционный процесс ведения технических паспортов в бумажной форме требует значительных временных затрат на актуализацию данных, поиск необходимой информации и проведение аудита системы. Например, внесение изменений, связанных с обновлением ПО, включает несколько этапов: подготовку отчёта, согласование с ответственными лицами, ручное внесение данных в технический паспорт и их проверку. По результатам экспертной оценки, этот процесс в среднем занимает от 4 до 6 ч, в зависимости от сложности изменений и количества затрагиваемых компонентов.

Внедрение блокчейн-технологии и автоматизированных механизмов обновления позволяет сократить эти затраты за счёт мгновенной регистрации изменений в распределённом реестре, автоматической проверки соответствия установленным требованиям и оперативного формирования отчётов. Экспериментальные данные показали, что при использовании предложенной системы обработка аналогичных изменений занимает от 3 до 5 мин, включая регистрацию обновлений, верификацию версии ПО и фиксацию результатов в блокчейне.

Таким образом, автоматизированная система технических паспортов сокращает временные затраты на обработку данных в 50–100 раз, что повышает оперативность управления ИБ и снижает вероятность ошибок, связанных с человеческим фактором.

Результаты и их обсуждение

Разработанная концепция системы ЭТП на основе блокчейн-технологии позволила устранить основные недостатки традиционного подхода к ведению документации об информационных системах. В ходе моделирования процесса автоматизированной обработки данных были выделены ключевые преимущества предложенного решения: неизменяемость записей, автоматизация аудита, прозрачность изменений и снижение временных затрат.

Экспериментальное моделирование показало, что при традиционном бумажном ведении технического паспорта внесение изменений, связанных с обновлением ПО и конфигурации системы, занимает от 4 до 6 ч, включая подготовку отчётов, согласование и проверку данных. Внедрение блокчейн-технологии позволило автоматизировать этот процесс, сократив временные затраты на регистрацию и верификацию обновлений до 3–5 мин, что эквивалентно ускорению обработки информации в 50–100 раз. Это существенно повышает оперативность управления ИБ и снижает вероятность ошибок, возникающих при ручной обработке данных.

Кроме того, предложенная система обеспечивает прозрачность и достоверность хранимой информации. Использование распределённого реестра исключает возможность незаметной корректировки данных и их утраты, что критически важно при проведении аудита информационных систем. В отличие от централизованных цифровых решений, блокчейн обеспечивает неизменяемость записей, снижая риск несанкционированных модификаций.

Одним из ключевых факторов повышения эффективности стало применение смарт-контрактов, которые автоматизируют проверку данных, сверяя вносимые изменения с установленными требованиями безопасности. Это позволяет не только фиксировать обновления, но и оперативно выявлять потенциальные уязвимости, сокращая время реакции на возможные угрозы.

Таким образом, предложенная система ЭТП не только повышает скорость обработки данных, но и обеспечивает более высокий уровень защищённости информации, что делает её перспективным решением для автоматизированных систем, требующих строгого контроля за конфигурацией и мерами защиты.

Заключение

В ходе исследования рассмотрены возможности применения блокчейн-технологии для автоматизированного ведения технических паспортов информационных систем. Выявлены основные недостатки традиционного бумажного и централизованного цифрового подходов, включая значительные временные затраты, риск утраты данных, сложность аудита и возможность несанкционированных изменений. Предложена архитектурная модель системы ЭТП, основанная на использовании распределённого реестра и смарт-контрактов для автоматизированной обработки информации о состоянии информационных систем.

Результаты моделирования показали, что внедрение блокчейн-технологии позволяет сократить время обработки изменений в техническом паспорте в 50–100 раз по сравнению с бумажным документооборотом, а также повысить прозрачность, достоверность и защищённость данных. Использование смарт-контрактов обеспечивает автоматическую проверку обновлений ПО и конфигурации системы, что снижает риск появления уязвимостей и повышает оперативность принятия решений в области ИБ.

Таким образом, разработанная концепция электронной системы технических паспортов на основе блокчейн имеет потенциал для внедрения в критически важные информационные системы, требующие строгого контроля за конфигурацией и соблюдением требований безопасности. Перспективными направлениями дальнейших исследований являются разработка механизмов адаптивного управления доступом к данным в блокчейн-реестре, интеграция с системами мониторинга угроз и применение методов машинного обучения для предиктивного анализа состояния автоматизированных систем.

Список источников

1. Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну: приказ ФСТЭК России от 29 апр. 2021 г. № 77. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77 (дата обращения: 19.12.2025).

2. Лосев В.С., Макаров А.Е. Инновационное значение применения технологии блокчейн в системе управления // Вестник Тихоокеанского государственного университета. 2024. № 1 (72). С. 117–128.

3. Blockchain integration into electronic document management (EDM) system in construction common data environment / M.S. Kiu [et al.] // Smart and Sustainable Built Environment. 2024. Vol. 13. № 1. P. 117–132.

4. A cross-chain mechanism for agricultural engineering document management blockchain in the context of big data / L. Shi [et al.] // Big Data Research. 2024. Vol. 36. P. 100459.

5. Концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости / А.О. Ефимов [и др.] // Безопасность информационных технологий. 2023. Т. 30. № 2. С. 63–79. DOI: 10.26583/bit.2023.2.04

6. Команов П.А., Ревазов Х.Ю., Тавасиев Д.А. Исследование безопасности смарт-контрактов Ethereum // Международный научно-исследовательский журнал. 2021. № 1-1 (103). С. 80–83.

7. Юмашева Е.В., Юмашев Д.В., Тимонов Д.А. Информационная безопасность в системах электронного документооборота с применением технологии блокчейн // Современные наукоемкие технологии. 2021. № 1. С. 63–68.

8. Клишин Д.В., Чечулин А.А. Анализ стандартов обеспечения информационной безопасности // Системы анализа и обработки данных. 2023. № 1 (89). С. 37–54.

9. Лившиц И.И., Бакшеев А.С. Исследование методик контроля уровня защищенности информации на объектах критической информационной инфраструктуры // Вопросы кибербезопасности. 2022. № 6. С. 52.

10. Сиротский А.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий. 2021. Т. 28. № 3. С. 103–117.

11. Information security and cybersecurity management: A case study with SMEs in Portugal / M. Antunes [et al.] // Journal of Cybersecurity and Privacy. 2021. Vol. 1. № 2. P. 219–238.

12. Effectiveness of cybersecurity audit / S. Slapničar [et al.] // International Journal of Accounting Information Systems. 2022. Vol. 44. P. 100548.

13. Shaikh F.A., Siponen M. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity // Computers & Security. 2023. Vol. 124. P. 102974.

14. IoT device security audit tools: A comprehensive analysis and a layered architecture approach for addressing expanded security requirements / A. Kumar [et al.] // International Journal of Information Security. 2025. Vol. 24. № 1. P. 1–22.

15. Основные этапы проектирования автоматизированной системы интеллектуального поиска мест наркотических закладок по открытым источникам / Г.И. Зверев [и др.] // Вестник Воронежского института МВД России. 2024. № 4. С. 70–78.

16. Зверев Г.И., Мишин С.А., Тужикова Т.Ю. Основные этапы разработки прототипа интеллектуальной системы детектирования и классификации огнестрельного оружия на фотоизображениях // Вестник Воронежского института МВД России. 2025. № 1. С. 97–108.

References

1. Ob utverzhdenii poryadka organizacii i provedeniya rabot po attestacii ob"ektov informatizacii na sootvetstvie trebovaniyam o zashchite informacii ogranichennogo dostupa, ne sostavlyayushchej gosudarstvennuyu tajnu: prikaz FSTEK Rossii ot 29 apr. 2021 g. № 77. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77 (data obrashcheniya: 19.12.2025).

2. Losev V.S., Makarov A.E. Innovacionnoe znachenie primeneniya tekhnologii blokchejn v sisteme upravleniya // Vestnik Tihookeanskogo gosudarstvennogo universiteta. 2024. № 1 (72). S. 117–128.

3. Blockchain integration into electronic document management (EDM) system in construction common data environment / M.S. Kiu [et al.] // Smart and Sustainable Built Environment. 2024. Vol. 13. № 1. P. 117–132.

4. A cross-chain mechanism for agricultural engineering document management blockchain in the context of big data / L. Shi [et al.] // Big Data Research. 2024. Vol. 36. P. 100459.

5. Konceptual'nye osnovy ocenki urovnya zashchishchennosti avtomatizirovannyh sistem na osnove ih uyazvimosti / A.O. Efimov [i dr.] // Bezopasnost' informacionnyh tekhnologij. 2023. T. 30. № 2. S. 63–79. DOI: 10.26583/bit.2023.2.04

6. Komanov P.A., Revazov H.Yu., Tavasiev D.A. Issledovanie bezopasnosti smart-kontraktov Ethereum // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. 2021. № 1-1 (103). S. 80–83.

7. Yumasheva E.V., Yumashev D.V., Timonov D.A. Informacionnaya bezopasnost' v sistemah elektronnogo dokumentooborota s primeneniem tekhnologii blokchejn // Sovremennye naukoemkie tekhnologii. 2021. № 1. S. 63–68.

8. Klishin D.V., Chechulin A.A. Analiz standartov obespecheniya informacionnoj bezopasnosti // Sistemy analiza i obrabotki dannyh. 2023. № 1 (89). S. 37–54.

9. Livshic I.I., Baksheev A.S. Issledovanie metodik kontrolya urovnya zashchishchennosti informacii na ob"ektah kriticheskoj informacionnoj infrastruktury // Voprosy kiberbezopasnosti. 2022. № 6. S. 52.

10. Sirotskij A.A. Formalizovannaya model' audita informacionnoj bezopasnosti organizacii na predmet sootvetstviya trebovaniyam standartov // Bezopasnost' informacionnyh tekhnologij. 2021. T. 28. № 3. S. 103–117.

11. Information security and cybersecurity management: A case study with SMEs in Portugal / M. Antunes [et al.] // Journal of Cybersecurity and Privacy. 2021. Vol. 1. № 2. P. 219–238.

12. Effectiveness of cybersecurity audit / S. Slapničar [et al.] // International Journal of Accounting Information Systems. 2022. Vol. 44. P. 100548.

13. Shaikh F.A., Siponen M. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity // Computers & Security. 2023. Vol. 124. P. 102974.

14. IoT device security audit tools: A comprehensive analysis and a layered architecture approach for addressing expanded security requirements / A. Kumar [et al.] // International Journal of Information Security. 2025. Vol. 24. № 1. P. 1–22.

15. Osnovnye etapy proektirovaniya avtomatizirovannoj sistemy intellektual'nogo poiska mest narkoticheskih zakladok po otkrytym istochnikam / G.I. Zverev [i dr.] // Vestnik Voronezhskogo instituta MVD Rossii. 2024. № 4. S. 70–78.

16. Zverev G.I., Mishin S.A., Tuzhikova T.Yu. Osnovnye etapy razrabotki prototipa intellektual'noj sistemy detektirovaniya i klassifikacii ognestrel'nogo oruzhiya na fotoizobrazheniyah // Vestnik Voronezhskogo instituta MVD Rossii. 2025. № 1. S. 97–108.

Информация о статье:
Статья поступила в редакцию: 20.01.2026; одобрена после рецензирования: 30.03.2026;
принята к публикации: 31.03.2026

Information about the article:
The article was submitted to the editorial office: 20.01.2026; approved after review: 30.03.2026;
accepted for publication: 31.03.2026

Информация об авторах:
Ефимов Алексей Олегович, преподаватель кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России (394065, г. Воронеж, пр. Патриотов, д. 53), e-mail: ea.aleksei@yandex.ru, https://orcid.org/0000-0001-7559-8113, SPIN-код: 7720-7586
Зверев Георгий Игоревич, заместитель начальника кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России (394065, г. Воронеж, пр. Патриотов, д. 53), кандидат технических наук, e-mail: georgiyzverev@gmail.com, https://orcid.org/0000-0001-7323-2425, SPIN-код: 1000-1072
Рогозин Евгений Алексеевич, профессор кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России (394065, г. Воронеж, пр. Патриотов, д. 53), доктор технических наук, профессор, e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535, SPIN-код: 4965-3462
Калач Андрей Владимирович, начальник кафедры безопасности информации и защиты сведений, составляющих государственную тайну, Воронежского института ФСИН России (394072, г. Воронеж, ул. Иркутская, д. 1А), доктор химических наук, профессор, почетный работник сферы образования Российской Федерации, e-mail: biizssgt@mail.ru, https://orcid.org/0000-0002-8926-3151, SPIN-код: 2584-7456

Information about authors:
Efimov Alexey O., lecturer of the department of automated information systems of internal affairs bodies of Voronezh Institute of the Ministry of the Interior of Russia (394065, Voronezh, Patriotov ave., 53), e-mail: ea.aleksei@yandex.ru, https://orcid.org/0000-0001-7559-8113, SPIN: 7720-7586
Zverev Georgy I., deputy head of the department of automated information systems of internal affairs bodies of Voronezh Institute of the Ministry of the Interior of Russia (394065, Voronezh, Patriotov ave., 53), candidate of technical sciences, e-mail: georgiyzverev@gmail.com, https://orcid.org/0000-0001-7323-2425, SPIN: 1000-1072
Rogozin Evgeny A., professor of the department of automated information systems of law enforcement agencies of Voronezh Institute of the Ministry of the Interior of Russia (394065, Voronezh, Patriotov ave., 53), doctor of technical sciences, professor, e-mail: evgenirogozin@yandex.ru , https://orcid.org/0000-0002-4455-7535, SPIN: 4965-3462
Kalach Andrey V., head of the department of information security and protection of information constituting a state secret of Voronezh Institute of the Federal Penitentiary Service of Russia (394072, Voronezh, Irkutskaya str., 1A), doctor of chemical sciences, professor, honorary worker of education of the Russian Federation, e-mail: biizssgt@mail.ru, https://orcid.org/0000-0002-8926-3151, SPIN: 2584-7456