УДК 004.056

ЦИФРОВАЯ ИДЕНТИЧНОСТЬ И РАСПРЕДЕЛЁННЫЕ РЕЕСТРЫ В E-GOVERNMENT СИСТЕМАХ

Ахметшин В.Р.
специалист, Кубанский государственный технологический университет (Краснодар, Россия)

Тумашев А.Г.
специалист, Кубанский государственный технологический университет (Краснодар, Россия)

DIGITAL IDENTITY AND DISTRIBUTED LEDGERS IN E-GOVERNMENT SYSTEMS

Akhmetshin V.R.
specialist degree, Kuban state technological university (Krasnodar, Russia)

Tumashev A.G.
specialist degree, Kuban state technological university (Krasnodar, Russia)

Аннотация

Цифровая идентичность, основанная на технологиях распределённых реестров (DLT), становится фундаментом для построения доверенных e-government-систем нового поколения. Эффективное внедрение таких решений требует учёта архитектурных, нормативных и инфраструктурных факторов. Проведён сравнительный анализ зрелости внедрения цифровых удостоверений личности в международной практике, а также технических характеристик ключевых DLT-платформ. Обоснована значимость самоуправляемой идентичности (SSI) как механизма повышения приватности и пользовательского контроля. Предложен подход к выбору технологической архитектуры, учитывающий баланс между производительностью, нормативной совместимостью и требованиями к масштабируемости. Полученные результаты могут быть использованы при разработке национальных стратегий цифровой трансформации.

Ключевые слова: цифровая идентичность, DLT, SSI, e-government, блокчейн, масштабируемость, архитектура, приватность.

Abstract

Digital identity built on distributed ledger technologies (DLT) is emerging as a foundational component of next-generation e-government infrastructures. Successful implementation depends on a combination of architectural design, regulatory frameworks, and technical interoperability. This paper presents a comparative assessment of global maturity levels in DLT-based identity systems and evaluates core platform characteristics. The relevance of self-sovereign identity (SSI) is emphasized as a means to enhance user control and privacy. A methodological approach is proposed for selecting technological architectures that align performance, scalability, and compliance objectives. The findings provide practical guidance for national digital transformation strategies and public sector implementation.

Keywords: digital identity, DLT, SSI, e-government, blockchain, architecture, scalability, privacy.

Введение

Современные цифровые трансформации в государственном управлении обусловлены необходимостью повышения прозрачности, эффективности и доверия в отношениях между гражданами, бизнесом и государством. Одним из ключевых элементов этих преобразований становится развитие электронного правительства (e-government), ориентированного на автоматизацию административных процессов, цифровизацию сервисов и интеграцию распределённых информационных систем.

Важнейшим компонентом e-government-инфраструктуры выступает цифровая идентичность - совокупность уникальных цифровых признаков, позволяющих однозначно идентифицировать субъекта в виртуальной среде. Безопасность, устойчивость и управляемость цифровых идентичностей напрямую влияют на качество предоставляемых государственных услуг, включая регистрацию граждан, доступ к медицинским и образовательным системам, участие в выборах и распределение социальных выплат. В условиях растущих угроз приватности и фальсификации данных особое значение приобретают подходы, основанные на распределённых реестрах (distributed ledgers), в том числе на технологии блокчейн.

Цель данной статьи - проанализировать потенциал интеграции цифровой идентичности с распределёнными реестрами в рамках e-government-систем. Рассматриваются технические, правовые и организационные аспекты внедрения распределённых идентификационных моделей, оцениваются преимущества и ограничения подхода, а также предлагается концептуальная модель архитектуры государственной системы цифровой идентификации, основанной на децентрализованных технологиях.

Основная часть. Эволюция цифровой идентичности в контексте электронного государства

Развитие электронного правительства сопровождалось последовательной трансформацией моделей идентификации пользователей. На ранних этапах цифровизации основное внимание уделялось централизованным системам аутентификации, в которых государственные органы или доверенные провайдеры удостоверяли личность пользователя на основе традиционных документов и закрытых реестров [1]. Такие подходы обеспечивали базовый уровень надёжности, однако оставались уязвимыми к утечкам данных, техническим сбоям и ограничениям масштабируемости.

С переходом к более зрелым e-government-платформам возникла необходимость в создании самостоятельных и гибко управляемых цифровых идентичностей, которые могли бы использоваться повторно в различных административных и межведомственных сценариях. Это привело к распространению моделей федеративной идентификации, в которых несколько ведомств или сервисов признают одну и ту же цифровую сущность. Однако и такие решения сохраняют зависимость от центральных регистраторов и не устраняют риски, связанные с единым центром отказа.

Современные концепции цифровой идентичности всё чаще ориентированы на децентрализованные и пользовательско-ориентированные модели. Примером такой парадигмы выступает концепция самоуправляемой идентичности (self-sovereign identity, SSI), согласно которой субъект сам контролирует доступ к своим данным, а их верификация осуществляется через распределённые реестры с использованием криптографических механизмов доверия. В рамках SSI доверие строится не на инфраструктуре централизованных удостоверяющих центров, а на сетевом консенсусе и цифровых подписях, записываемых в неизменяемые блоки данных.

Таким образом, эволюция цифровой идентичности в e-government-среде демонстрирует переход от централизованного управления к распределённым и суверенным моделям, где безопасность, приватность и прозрачность определяются архитектурными особенностями цифровой экосистемы, а не исключительно институциональным доверием.

Архитектурные модели цифровой идентичности в e-government-среде

Выбор архитектуры цифровой идентичности в системах электронного правительства предопределяет не только технологическую реализацию, но и нормативные аспекты взаимодействия между государством, гражданином и сторонними сервисами [2]. Современные подходы к проектированию таких систем можно условно разделить на три категории: централизованная, федеративная и децентрализованная (на основе распределённых реестров).

Централизованная архитектура предполагает наличие единого удостоверяющего органа, отвечающего за регистрацию, хранение и верификацию идентификационных данных. Этот подход широко применялся на ранних этапах цифровизации, но характеризуется высокой уязвимостью к атакам, а также рисками злоупотребления полномочиями.

Федеративные модели позволяют объединять несколько поставщиков удостоверяющих услуг в рамках доверенной сети. Верификация может осуществляться с использованием протоколов, таких как SAML или OAuth2, при этом данные пользователя могут циркулировать между различными ведомствами. Несмотря на более высокую гибкость, федеративные решения всё ещё полагаются на центральную инфраструктуру и требуют строгой координации между участниками.

Децентрализованные архитектуры, реализуемые на базе распределённых реестров, принципиально изменяют модель доверия. В системе SSI каждый субъект (гражданин, организация, государственное учреждение) может создавать и управлять собственными идентификаторами, а проверки подлинности осуществляются через цифровые доказательства и записи в блокчейне. Такие системы повышают прозрачность и устойчивость, снижая зависимость от централизованных доверенных сторон.

На рисунке 1 представлена сравнительная схема трёх архитектур цифровой идентичности, применяемых в e-government-системах.

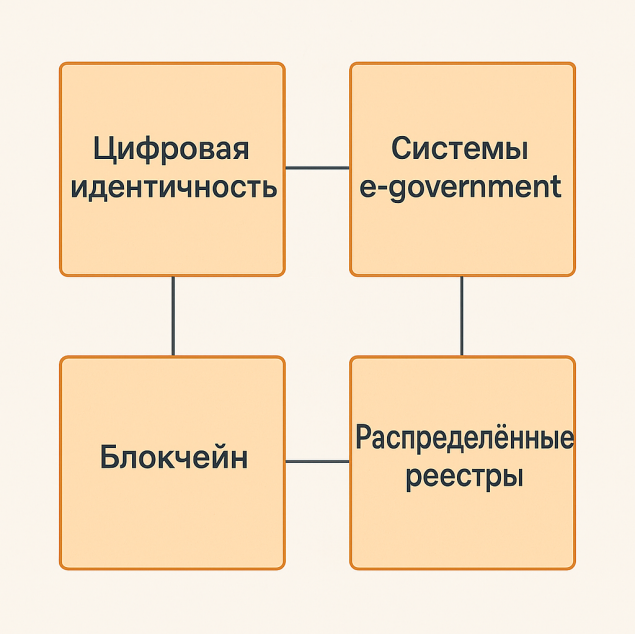

Рисунок 1. Сравнение архитектур цифровой идентичности: централизованная, федеративная и децентрализованная модель

Сравнительный анализ архитектур цифровой идентичности, представленных на рисунке, демонстрирует, что централизованные модели, несмотря на простоту реализации, уступают по уровню отказоустойчивости и контролю со стороны пользователей. Федеративные решения обеспечивают более высокий уровень взаимодействия между ведомствами, но сохраняют зависимость от доверенных посредников. Наиболее перспективной в контексте цифрового суверенитета граждан и устойчивости инфраструктуры представляется децентрализованная модель, реализуемая с использованием распределённых реестров. Она обеспечивает наибольшую степень прозрачности, масштабируемости и криптографической надёжности, что особенно актуально для современных e-government-систем [3].

Сравнительный анализ решений цифровой идентификации на базе DLT

Внедрение технологий распределённых реестров (Distributed Ledger Technology, DLT) в государственные идентификационные системы сопровождается ростом интереса к конкретным технологическим платформам. На сегодняшний день существует несколько зрелых решений, адаптированных под нужды e-government: Hyperledger Indy, Ethereum, Sovrin, Quorum и другие. Каждое из них обладает специфическими характеристиками, влияющими на уровень доверия, масштабируемость, приватность и юридическую совместимость.

В таблице 1 приведено подробное сравнение ключевых DLT-платформ, применяемых для построения систем цифровой идентичности, включая их технологические характеристики, уровень приватности, совместимость с государственными системами и другие важные параметры.

Таблица 1

Сравнение ключевых DLT-платформ для построения систем цифровой идентичности: особенности и ограничения

Платформа	**Тип реестра и поддержка SSI**	**Приватность и масштабируемость**	**Применимость в e-government**
Hyperledger indy	Разрешённый, полная поддержка самоуправляемой идентичности	Высокий уровень приватности, средняя масштабируемость	Рекомендуется для интеграции с госреестрами и удостоверяющими центрами
Ethereum	Публичный, ограниченная поддержка концепции идентичности	Низкая приватность, высокая масштабируемость	Ограниченная применимость, требует доработки под госстандарты
Sovrin	Публично-разрешённый, полная поддержка самоуправляемой идентичности	Высокая приватность, средняя масштабируемость	Подходит для национальных проектов, интегрируется с DID и VC
Quorum	Разрешённый, частичная поддержка пользовательского контроля	Средняя приватность, высокая масштабируемость	Может использоваться в ведомственных системах с настройкой приватности
Corda	Разрешённый, ограниченная поддержка через плагины и настройки	Высокая приватность, высокая масштабируемость	Частично применима, требует адаптации для идентификационных задач

Анализ представленных в таблице платформ показывает, что наибольший потенциал для внедрения в государственные идентификационные системы демонстрируют решения Hyperledger Indy и Sovrin, ориентированные на поддержку концепции самоуправляемой идентичности и обеспечение высокого уровня приватности. Платформы общего назначения, такие как Ethereum и Quorum, хотя и обладают высокой масштабируемостью, в базовой конфигурации недостаточно адаптированы к требованиям защиты персональных данных и нормативной совместимости. Решения на базе Corda могут быть применимы в межведомственных сценариях, но требуют доработки механизмов идентификации. Следовательно, выбор технологии должен базироваться на комплексной оценке приватности, масштабируемости и соответствия регуляторным требованиям конкретной юрисдикции.

Важным аспектом выбора DLT-платформы также становится уровень зрелости экосистемы, наличие поддержки со стороны разработчиков и соответствие национальным стандартам информационной безопасности [4]. Так, Hyperledger Indy уже адаптирован для

интеграции с национальными идентификационными системами в ряде стран, включая пилотные проекты в Канаде и Индии, что делает его привлекательным для масштабируемых решений в сфере государственного управления.

Кроме того, при проектировании идентификационных систем на базе DLT особое внимание должно уделяться интероперабельности. Возможность обмена данными между платформами и ведомствами без потери доверия критически важна для построения единой цифровой идентичности, пригодной для использования в различных сферах - от налоговых сервисов до электронного здравоохранения. Такие механизмы, как DID (Decentralized Identifier) и VC (Verifiable Credentials), становятся ключевыми стандартами, способствующими совместимости между системами, независимо от выбранной базовой инфраструктуры.

Наконец, не менее значимым фактором является гибкость лицензирования и модели управления платформой. Платформы с открытым исходным кодом, управляемые консорциумами или фондами (например, Hyperledger Foundation), обеспечивают большую прозрачность и возможность адаптации к локальным требованиям. В то время как проприетарные решения могут ограничивать развитие за счёт зависимости от конкретного вендора и стоимости владения.

Уровни зрелости внедрения цифровой идентичности с DLT в международной практике

Внедрение цифровой идентичности с использованием распределённых реестров в e-government-системах находится на разных стадиях зрелости в зависимости от политико-экономического контекста, нормативного регулирования и цифровой зрелости страны. По состоянию на текущий этап развития можно выделить несколько уровней зрелости, отражающих глубину интеграции DLT в государственную инфраструктуру:

Начальный уровень - страны, исследующие возможности применения блокчейн-технологий, но не приступившие к пилотным внедрениям (например, Аргентина, Казахстан).

Пилотный уровень - реализуются ограниченные проекты в отдельных ведомствах или регионах, как правило, без масштабной нормативной базы (например, Индия, Украина).

Интеграционный уровень - платформа цифровой идентичности на базе DLT включена в e-government-экосистему, охватывая несколько сфер: здравоохранение, налоги, голосование (например, Эстония, Канада).

Стабильный уровень - устойчиво работающая, проверенная временем и регулированием архитектура, способная масштабироваться и соответствовать международным стандартам (например, Южная Корея, Сингапур) [5].

Правовые и этические аспекты применения DLT в системах цифровой идентичности

Внедрение цифровой идентичности с использованием распределённых реестров в государственные информационные системы требует тщательного учета правовых, этических и регуляторных аспектов. Особую актуальность эти вопросы приобретают в контексте хранения, обработки и верификации персональных данных, а также в условиях трансграничного взаимодействия.

С точки зрения законодательства, основным ориентиром для большинства стран остаются положения GDPR (General Data Protection Regulation), а также национальные законы о защите персональных данных. Использование неизменяемых и публичных блокчейнов может противоречить праву на удаление информации («право быть забытым»), что создаёт противоречие между принципами децентрализации и нормативными требованиями [6].

Одним из путей решения данной проблемы становится применение off-chain-хранилищ или хешированных ссылок, где сами персональные данные не записываются в реестр, а используются ссылки на зашифрованные внешние хранилища. Это позволяет сохранить преимущества блокчейн-модели (прозрачность и неизменяемость) без нарушения конфиденциальности.

Кроме правового регулирования, значимую роль играют этические вопросы, связанные с цифровым неравенством и возможным навязыванием технологий уязвимым группам

населения. Обязательное использование цифровой идентичности на основе DLT может создавать барьеры для лиц с ограниченным доступом к цифровым устройствам или интернету.

Не менее важным является обеспечение институциональной подотчётности. Применение самоуправляемой цифровой идентичности требует наличия доверенной инфраструктуры: агентств по выпуску идентификаторов, органов аудита, а также механизмов разрешения споров. Без этих элементов любые децентрализованные архитектуры рискуют потерять легитимность в глазах пользователей и регуляторов.

Таким образом, разработка цифровой идентичности на базе DLT должна основываться не только на технологической состоятельности, но и на чётком соблюдении правовых норм, принципов справедливости и социального баланса. Это требует междисциплинарного подхода с участием технологов, юристов, представителей государства и гражданского общества.

Модели доверия и распределение ответственности в DLT-системах цифровой идентичности

В архитектуре цифровой идентичности на основе распределённых реестров важнейшую роль играет модель распределения доверия и ответственности между участниками системы. В отличие от централизованных решений, где вся логика и ответственность сосредоточены в одном органе, распределённые модели предполагают координацию между несколькими ролями:

Issuer (Эмитент) - организация, уполномоченная на выпуск идентификаторов или аттестатов (например, налоговая служба, университет).

Holder (Держатель) - субъект идентичности (гражданин, юридическое лицо), хранящий свои идентификационные данные и управляющий доступом к ним.

Verifier (Проверяющий) - сторона, запрашивающая подтверждение тех или иных атрибутов личности (например, работодатель или банк).

Registry node (Узел реестра) - участник сети, поддерживающий инфраструктуру DLT, обеспечивая неизменяемость и доступность записей.

Governance authority (Регулятор) - надзорный орган, устанавливающий технические и юридические рамки функционирования всей системы.

На рисунке 2 представлена схема распределения этих ролей и потока доверия между ними.

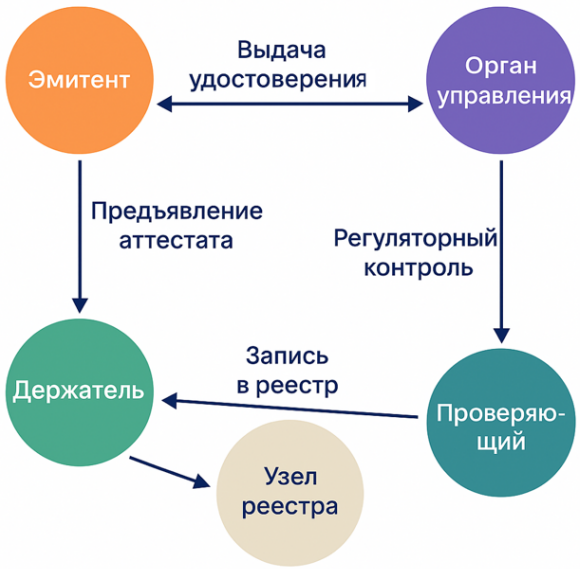

Рисунок 2. Распределение ролей и потоков данных в системе цифровой идентичности на основе DLT

Представленная схема демонстрирует ключевое распределение ролей и взаимодействий между участниками децентрализованной системы цифровой идентичности. В отличие от централизованных моделей, архитектура на основе DLT предусматривает передачу ответственности от единого оператора к множеству доверенных сторон: эмитентов, держателей и проверяющих [7]. Такая модель повышает прозрачность, масштабируемость и

устойчивость системы, однако требует строгой координации между ролями и наличия регулирующей инфраструктуры. Потоки данных между участниками организованы на принципах избирательного доступа и криптографической верификации, что обеспечивает баланс между приватностью и достоверностью.

Технологические ограничения и проблемы масштабируемости DLT в системах цифровой идентичности

Несмотря на широкое обсуждение преимуществ DLT в контексте цифровой идентичности, их внедрение в государственные системы сталкивается с рядом технологических ограничений, способных существенно замедлить или усложнить масштабное применение.

Одним из ключевых вызовов является низкая пропускная способность и ограниченная масштабируемость большинства DLT-платформ. При большом количестве транзакций - например, при массовом обращении граждан к электронным сервисам - система может испытывать задержки или перегрузку. Особенно это актуально для публичных блокчейнов, где все узлы должны достичь консенсуса, что увеличивает время обработки.

Другой критический аспект - энергопотребление и производительность. Хотя некоторые платформы (например, Tezos, Algorand) уже реализуют энергоэффективные протоколы, большая часть существующих решений всё ещё базируется на ресурсоёмких алгоритмах, не соответствующих принципам устойчивого развития и «зелёных» ИТ [8].

Также остаётся нерешённой проблема интероперабельности между различными DLT-платформами. В условиях, когда государственная система должна взаимодействовать с коммерческими, банковскими и международными сервисами, отсутствие стандартов затрудняет обмен данными, а также усложняет аудит и миграцию между платформами.

Дополнительные риски возникают в связи с обновлением и модификацией данных, что критично для цифровой идентичности. Технология блокчейн по своей природе неизменяема, а это затрудняет реализацию механизмов отзыва удостоверений, внесения исправлений или удаления данных в соответствии с нормативными требованиями.

Наконец, важно учитывать сложность интеграции DLT-решений с устаревшими государственными ИС, где отсутствует единый протокол или интерфейс взаимодействия. Это требует вложений в адаптационные слои, шлюзы и API, что увеличивает стоимость и сроки внедрения.

Таким образом, внедрение DLT в e-government-системы цифровой идентичности требует не только нормативной и организационной готовности, но и серьёзной технической адаптации, ориентированной на устойчивость, совместимость и производительность.

Сравнение DLT-платформ по критериям применимости в e-government

Выбор технологической платформы для реализации цифровой идентичности в системах электронного правительства определяется набором ключевых критериев, от которых зависит не только производительность, но и юридическая совместимость, устойчивость и масштабируемость архитектуры. Среди таких критериев выделяются:

- Производительность и пропускная способность - способность системы обрабатывать большое количество транзакций в секунду без снижения стабильности.
- Энергоэффективность - важный показатель устойчивости и экосоциальной совместимости технологии.
- Интероперабельность - возможность взаимодействия с другими платформами и стандартами цифровой идентичности.
- Поддержка SSI (Self-Sovereign Identity) - наличие встроенных механизмов управления удостоверениями со стороны пользователей.
- Гибкость и адаптируемость - возможность настройки архитектуры под нормативные и организационные особенности разных стран [9].

Анализ доступных DLT-платформ показывает, что ни одна из них не обладает абсолютным превосходством по всем критериям. Ethereum, как одна из наиболее распространённых публичных блокчейн-платформ, обеспечивает высокую совместимость с

децентрализованными приложениями, однако страдает от ограниченной масштабируемости и высокой энергозатратности в своей классической реализации (до перехода на алгоритм консенсуса Proof-of-Stake). При этом адаптация Ethereum для нужд цифровой идентичности требует внедрения дополнительных протоколов и надстроек.

Hyperledger Indy и связанная с ней экосистема Sovrin изначально ориентированы на реализацию концепции самоуправляемой идентичности (SSI). Эти платформы демонстрируют высокий уровень соответствия требованиям приватности, управления доступом и децентрализованной верификации, но уступают в гибкости и интеграционной совместимости с другими системами, а также требуют более сложной настройки инфраструктуры.

Quorum и Corda, разработанные для корпоративных и межведомственных сценариев, показывают хорошие результаты в части масштабируемости, управляемости и регуляторной совместимости. Тем не менее, в базовой конфигурации эти решения не содержат встроенной поддержки SSI и требуют дополнительной настройки для реализации пользовательского контроля над удостоверениями.

Таким образом, выбор DLT-платформы должен осуществляться не только на основании технических характеристик, но и с учётом требований конкретной юрисдикции, уровня зрелости ИТ-инфраструктуры, сценариев использования и политико-правовой среды [10]. В некоторых случаях оправдано применение гибридных моделей, где один уровень системы функционирует на основе публичного блокчейна, а другой - на приватной или разрешённой сети, что позволяет достичь компромисса между открытостью, контролем и безопасностью.

Заключение

Развитие цифровой идентичности на основе DLT представляет собой важнейшее направление цифровой трансформации государственного управления. Такие технологии позволяют повысить уровень доверия, прозрачности и пользовательского контроля в системах идентификации, что особенно актуально в условиях растущих требований к защите персональных данных, обеспечению киберустойчивости и международной совместимости.

В статье был проведён анализ архитектурных моделей, технологических платформ и практик внедрения цифровой идентичности в различных странах. Показано, что наибольшую зрелость в этом направлении демонстрируют государства с развитой цифровой инфраструктурой, нормативной базой и стратегией внедрения самоуправляемых удостоверений.

Ключевые технологические ограничения - масштабируемость, интероперабельность, энергоэффективность и сложность интеграции - остаются значимыми барьерами. Их преодоление возможно через применение гибридных архитектур, развитие стандартов и институциональную поддержку со стороны государства. Важно подчеркнуть, что универсального решения не существует: каждая страна должна разрабатывать собственную модель цифровой идентичности с учётом локального контекста, при этом опираясь на международный опыт и открытые технологии.

В перспективе именно DLT может стать основой для построения по-настоящему доверенных, распределённых и самоуправляемых цифровых удостоверений личности, способных трансформировать не только e-government, но и всю экосистему цифровых услуг.

References

1. Elisa N., Yang L., Chao F., Cao Y. A framework of blockchain-based secure and privacy-preserving E-government system // Wireless networks. 2023. Vol. 29. No. 3. P. 1005-1015.
2. Sung C.S., Park J.Y. Understanding of blockchain-based identity management system adoption in the public sector // Journal of Enterprise Information Management. 2021. Vol. 34. No. 5. P. 1481-1505.
3. Ranjith Kumar M.V., Bhalaji N. Blockchain based chameleon hashing technique for privacy preservation in E-governance system // Wireless Personal Communications. 2021. Vol. 117. No. 2. P. 987-1006.

4. Mustafa G., Rafiq W., Jhamat N., Arshad Z., Rana F.A. Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations // International Journal of Law and Management. 2025. Vol. 67. No. 1. P. 37-55.
5. Kuperberg M., Kemper S., Durak C. Blockchain usage for government-issued electronic IDs: A survey // International Conference on Advanced Information Systems Engineering. Cham: Springer International Publishing. 2019. P. 155-167.
6. Elisa N., Yang L., Chao F., Naik N., Boongoen T. A secure and privacy-preserving e-government framework using blockchain and artificial immunity // IEEE Access. 2023. Vol. 11. P. 8773-8789.
7. Al-Ameri H.H., Ayvaz S. A Blockchain-Based Secure Mutual Authentication System for E-Government Services // 2023 3rd International Scientific Conference of Engineering Sciences (ISCES). IEEE. 2023. P. 19-24.
8. Datta A. Blockchain enabled digital government and public sector services: A survey // Blockchain and the Public Sector: Theories, Reforms, and Case Studies. 2021. P. 175-195.
9. Gao Y., Pan Q., Liu Y., Lin H., Chen Y., Wen Q. The notarial office in E-government: a blockchain-based solution // IEEE Access. 2021. Vol. 9. P. 44411-44425.
10. Fajar A., Trialih R., Ramlan F.W. A Decentralized File Storage for Effective E-Government // Indonesia Post-Pandemic Outlook: Environment and Technology Role for Indonesia Development. 2022. P. 279.