УДК 004.738.5:004.056.5:351.74

5.2.2. Математические, статистические и инструментальные методы экономики (физико-математические науки, экономические науки)

МНОГОКРИТЕРИАЛЬНАЯ ЭКОНОМИКО-МАТЕМАТИЧЕСКАЯ ОЦЕНКА И ВЫБОР БЛОКЧЕЙН-ПЛАТФОРМЫ ДЛЯ ДЕЖУРНЫХ ЧАСТЕЙ ОВД РОССИИ

Лаптев Владимир Николаевич
к.т.н., доцент
SPIN-код: 8905-8271
ФГБОУ ВО «Кубанский ГАУ им. И.Т. Трубилина», Краснодар, Россия

Жмурко Даниил Юрьевич
к.э.н., доцент
РИНЦ SPIN-код: 1543-2028
AuthorID: 509102
ФГКОУ ВО «Краснодарский университет МВД России», Краснодар, Россия

Еськов Александр Васильевич
д.т.н., профессор
РИНЦ SPIN-код: 1842-1662
AuthorID: 139101

Иванов Игорь Петрович
к.п.н., доцент
РИНЦ SPIN-код: SPIN-код: 9300-2367,
AuthorID: 734507

Третьякова Наталья Васильевна
к.п.н., доцент
РИНЦ SPIN-код: 1863-4520
AuthorID: 585151
ФГКВОУ «Краснодарское высшее военное авиационное училище лётчиков имени Героя Советского Союза А. К. Серова», Краснодар, Россия

В статье анализируются экономические и организационные эффекты использования технологии распределённого реестра в дежурных частях органов внутренних дел России. На основе анализа бизнес-процессов и структуры обрабатываемых данных формируются требования к блокчейн-платформам, влияющие на совокупную стоимость владения, операционные расходы и риски нарушения целостности информации. Предложена методика многокритериальной оценки, включающая экономические, технические и регуляторные показатели: затраты на лицензирование и сопровождение, потребность в вычислительных ресур-

UDC 004.738.5:004.056.5:351.74

5.2.2. Mathematical, statistical and instrumental methods of economics (physical and mathematical sciences, economic sciences)

MULTI-CRITERIA ECONOMIC AND MATHEMATICAL EVALUATION AND SELECTION OF A BLOCKCHAIN PLATFORM FOR POLICE DUTY UNITS IN RUSSIA

Laptev Vladimir Nikolaevich
Cand.Tech.Sci., Associate professor
RSCI SPIN-Code: 8905-8271
Federal State Budgetary Educational Institution of Higher Education «Kuban State Agrarian University named after I.T. Trubilin», Krasnodar, Russia

Zhmurko Daniil Yuryevich
Cand.Econ.Sci., Associate Professor
RSCI SPIN Code: 1543-2028
AuthorID: 509102
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russia

Eskov Aleksandr Vasilievich
Doctor of Technical Sciences, Professor
RSCI SPIN Code: 1842-1662
AuthorID: 139101

Ivanov Igor Petrovich
Candidate of Pedagogical Sciences, Associate Professor
RSCI SPIN Code: 9300-2367
AuthorID: 734507

Tretyakova Natalya Vasilievna
Candidate of Pedagogical Sciences, Associate Professor
RSCI SPIN Code: 1863-4520
AuthorID: 585151
Federal Government Budgetary Educational Institution of Higher Education "Krasnodar Higher Military Aviation School for Pilots named after Hero of the Soviet Union A. K. Serov", Krasnodar, Russia

The article analyzes the economic and organizational effects of using distributed registry technology in duty stations of the internal affairs bodies of Russia. Based on the analysis of business processes and the structure of the processed data, requirements for blockchain platforms are formed that affect the total cost of ownership, operating costs and risks of information integrity violations. A multi-criteria assessment methodology is proposed, including economic, technical and regulatory indicators: licensing and maintenance costs, the need for computing resources, the cost of integration with existing IT infrastructure, as well as compliance with the requirements of the FSTEC and the FSB of

сах, стоимость интеграции с существующей ИТ-инфраструктурой, а также соответствие требованиям ФСТЭК и ФСБ России. Для платформ Masterchain, Waves Enterprise, Exonum и Hyperledger Fabric построена матрица сравнения с весовыми коэффициентами по группам критериев «информационная безопасность», «производительность и масштабируемость», «интеграция и сопровождение», «регуляторное соответствие». На основе математических моделей пропускной способности и устойчивости к сбоям оценивается способность платформ обеспечивать требуемый уровень сервиса при различных сценариях нагрузки и отказах узлов, что позволяет количественно сопоставить риск простоев и экономические потери. Результаты показывают, что с учётом регуляторных ограничений и затрат жизненного цикла предпочтительной базовой платформой для дежурных частей ОВД является Masterchain, тогда как Waves Enterprise и Hyperledger Fabric могут использоваться в отдельных сценариях. Сформирована поэтапная дорожная карта внедрения (пилоты, опытная эксплуатация, тиражирование) с указанием ключевых экономических показателей и предложены практические рекомендации по выбору оптимальной платформы и конфигурации решения, а также направления дальнейших исследований

Ключевые слова: БЛОКЧЕЙН, ДЕЖУРНАЯ ЧАСТЬ ОВД, РАСПРЕДЕЛЁННЫЙ РЕЕСТР. КРИПТОГРАФИЯ, РЕГУЛЯТОРНОЕ СООТВЕТСТВИЕ, MASTERCHAIN, WAVES ENTERPRISE, EXONUM, HYPERLEDGER FABRIC, МАСШТАБИРУЕМОСТЬ, ОТКАЗОУСТОЙЧИВОСТЬ, ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

http://dx.doi.org/10.21515/1990-4665-217-018

Russia. For the Masterchain, Waves Enterprise, Exonum, and Hyperledger Fabric platforms, a comparison matrix has been built with weights for the criteria groups "information security", "performance and scalability", "integration and maintenance", and "regulatory compliance". Mathematical models of throughput and fault tolerance are used to evaluate the ability of platforms to provide the required level of service under various load scenarios and node failures, which makes it possible to quantify the risk of downtime and economic losses. The results show that, taking into account regulatory constraints and lifecycle costs, Masterchain is the preferred base platform for ATS units on duty, while Waves Enterprise and Hyperledger Fabric can be used in separate scenarios. A step-by-step implementation roadmap (pilots, trial operation, replication) has been formed, indicating key economic indicators, and practical recommendations have been proposed for choosing the optimal platform and configuration of the solution, as well as directions for further research

Keywords: BLOCKCHAIN, POLICE DUTY UNIT, DISTRIBUTED LEDGER; CRYPTOGRAPHY; REGULATORY COMPLIANCE, MASTERCHAIN, WAVES ENTERPRISE, EXONUM, HYPERLEDGER FABRIC, SCALABILITY, FAULT TOLERANCE, DIGITAL TRANSFORMATION

1. Введение

Цифровая трансформация правоохранительной деятельности и потребность в доверенной среде

Цифровая трансформация государственных институтов ставит перед МВД России новые задачи по обеспечению достоверности, целостности и защищенности данных. Особенно остро эти вызовы проявляются в деятельности дежурных частей (ДЧ) органов внутренних дел (ОВД), где зарождается жизненный цикл практически каждого сообщения о происшествии. Существующие централизованные информационные системы уяз-

вимы для технических сбоев и злонамеренных действий, направленных на фальсификацию записей, что подрывает доверие к системе и создает почву для коррупционных проявлений.

«Технология распределённого реестра (DLT), или блокчейн, предлагает фундаментально новый подход к построению доверенных информационных систем. Ее ключевые свойства – децентрализованное хранение, криптографическая связность записей и неизменяемость истории – напрямую отвечают на вызовы, стоящие перед ДЧ ОВД. Как отмечают исследователи, применение блокчейна в работе полиции может значительно повысить прозрачность, ответственность и эффективно бороться с фальсификацией данных» [11]. Гипотеза данного исследования заключается в том, что внедрение корпоративной блокчейн-платформы, адаптированной к специфике правоохранительной деятельности, способно создать единую доверенную среду для гарантированной целостности и прослеживаемости данных.

Целью настоящей статьи является проведение технического сравнительного анализа доступных на российском рынке корпоративных блокчейн-платформ для обоснования выбора оптимального решения для ДЧ ОВД. В фокусе анализа находятся отечественные и адаптированные для РФ решения: «Мастерчейн», Waves Enterprise, Exonum и Hyperledger Fabric с модулями поддержки российской криптографии.

2. Методология исследования и критерии оценки

Для достижения поставленной цели применяется комплексная методология, основанная на многокритериальном сравнительном анализе. Объектами исследования выступают четыре корпоративные блокчейн-платформы, доступные для внедрения в России: *Мастерчейн*[1] (российская платформа с нативной поддержкой ГОСТ и сертификатом ФСБ), *Waves*

[1] Портал документации Мастерчейн. Документация. – Режим доступа: https://docs.dltru.org/ (дата обращения: 20.01.2026).

Enterprise[2] (гибридная платформа с опытом внедрения в госсекторе), *Exonum*[3] (фреймворк с открытым кодом, ориентированный на высокую производительность) и *Hyperledger Fabric*[4] (глобальный стандарт, адаптируемый для РФ с помощью внешних ГОСТ-модулей).

Предметом исследования являются технические, функциональные, эксплуатационные и регуляторные характеристики указанных платформ, проанализированные через призму их применимости для ДЧ ОВД. «Анализ проводится по многоуровневой системе критериев, сгруппированных в тематические блоки: функциональные требования, производительность, безопасность и криптография (ГОСТ), а также архитектурные и интеграционные аспекты. Оценка базируется на анализе официальной документации, нормативно-правовых актов РФ, научных публикаций и отчетов о пилотных проектах» [14].

2.1. Структура анализа

Исследование имеет четкую структуру, направленную на последовательное и всестороннее изучение проблемы. Анализ проводится по многоуровневой системе критериев, сгруппированных в тематические блоки, каждый из которых призван ответить на один или несколько ключевых исследовательских вопросов, сформулированных в постановке задачи. Эти блоки включают:

- Анализ функциональных требований и модели данных.
- Оценка производительности, оперативности и отказоустойчивости.
- Исследование механизмов обеспечения целостности, неизменяемости и аудита.

[2] Waves Enterprise. Документация Waves Enterprise. – Режим доступа: https://wavesenterprise.com/ (раздел документации; дата обращения: 20.01.2026).
[3] Exonum. Exonum Documentation. – Режим доступа: https://exonum.com/doc/ (дата обращения: 20.01.2026).
[4] Hyperledger Fabric. Documentation. – Режим доступа: https://hyperledger-fabric.readthedocs.io/ (дата обращения: 20.01.2026).

- Анализ соответствия требованиям безопасности, криптографии (ГОСТ) и разграничения доступа.
- Оценка архитектурных, эксплуатационных и интеграционных аспектов.

Каждый критерий внутри блока оценивается с использованием специфичных метрик (например, TPS для производительности, RTO/RPO для отказоустойчивости, наличие сертификата ФСБ для криптографии). Итогом является построение сводной сравнительной матрицы, которая служит основой для выработки финальных рекомендаций.

2.2. Источники данных

Для обеспечения достоверности и полноты анализа используется широкий спектр источников, ранжированных по степени надежности:

1. *Официальная техническая документация платформ.* Руководства для разработчиков и администраторов, White Papers, архитектурные описания (например, документация Hyperledger Fabric, документация Waves Enterprise, портал документации Мастерчейн, документация Exonum).

2. *Нормативно-правовые и регуляторные акты РФ.* Федеральные законы (ФЗ-152 «О персональных данных», ФЗ-63 «Об электронной подписи», ФЗ-187 «О безопасности критической информационной инфраструктуры»), приказы ФСТЭК России и ФСБ России, стандарты ГОСТ в области криптографии [22, 23, 25].

3. *Научные публикации и отчёты об исследованиях.* Статьи в рецензируемых журналах, материалы конференций, диссертации, посвященные сравнительному анализу блокчейн-систем, их производительности и безопасности (например, исследования по алгоритмам консенсуса или квантовой устойчивости).

4. *Отчёты о тестировании и пилотных проектах*. Публичные результаты нагрузочного тестирования (например, тестирование произ-

водительности Waves Enterprise) и описания реализованных кейсов в государственном и корпоративном секторах.

5. *Экспертные оценки и аналитические материалы.* Статьи и обзоры от ведущих отраслевых экспертов и консалтинговых агентств (например, обзоры TAdviser).

2.3. Эталонный стенд и тестовые сценарии

Хотя данная статья носит преимущественно аналитический характер, в основе методологии лежит концепция *гипотетического эталонного стенда*, который необходим для практической верификации заявленных характеристик платформ. Описание такого стенда позволяет конкретизировать критерии оценки и сделать их измеримыми.

Концепция эталонного стенда

- *Топология* – географически распределённая сеть, эмулирующая иерархическую структуру МВД. Узлы размещаются в трёх условных зонах: «ЦОД ГУВД» (высокопроизводительные серверы), «Узел УВД» (серверы среднего уровня) и «Узел РОВД» (ограниченные ресурсы). Каналы связи между зонами имеют разную пропускную способность и задержки.
- *Программная среда* – использование контейнеризации (Docker) и оркестрации (Kubernetes) для развертывания узлов, что соответствует современным практикам и архитектуре большинства платформ (например, компоненты Hyperledger Fabric) [17].
- *Нагрузочные инструменты* – применение стандартных для отрасли инструментов бенчмаркинга, таких как Hyperledger Caliper, для генерации транзакционной нагрузки и измерения ключевых метрик (TPS, latency).
- *Тестовые сценарии* – нагрузка на стенд должна имитировать реальные процессы ДЧ:
  - ✓ «Пиковая нагрузка»: эмуляция массовой регистрации сооб-

щений (например, в праздничные дни или при ЧС) для проверки burst tps и поведения очереди транзакций.

- ✓ «Смешанный режим»: одновременное выполнение транзакций разного типа – короткие записи о регистрации, транзакции с прикреплением хэшей крупных файлов, запросы на чтение для аудита.
- ✓ «Стресс-тест отказоустойчивости»: имитация отказа части узлов (валидаторов) или ухудшения качества каналов связи (потеря пакетов) для оценки деградации производительности и проверки RTO/RPO.

Такой подход, пусть и теоретический в рамках данной статьи, позволяет перевести абстрактные требования в плоскость конкретных инженерных задач и измеримых показателей, что является фундаментом для объективного сравнения.

3. Анализ требований к блокчейн-платформе в деятельности ДЧ ОВД

Эффективное внедрение блокчейна требует глубокой декомпозиции требований, проистекающих из специфики бизнес-процессов и нормативно-правовой базы ДЧ ОВД.

3.1. Функциональные требования и модель данных

Функциональные требования определяют, ***что*** система должна делать. Для ДЧ ОВД это означает перенос ключевых операционных сценариев в доверенную и неизменяемую среду.

Бизнес-сценарии и их критичность

Анализ деятельности ДЧ позволяет выделить несколько критически важных служебных сценариев, которые наиболее выигрывают от внедрения блокчейна:

1. *Регистрация сообщений о преступлениях и происшествиях (КУСП)*. «Это точка входа для 99% информации. Каждая запись должна быть зафиксирована с точной меткой времени, неизменяемым со-

держанием и присвоенным уникальным идентификатором. Блокчейн гарантирует, что запись не может быть удалена или изменена без оставления криптографического следа» [15].

Метрики: критичность по времени (SLA) – регистрация должна занимать секунды. Объём транзакций в пике (burst tps) может достигать сотен в минуту по крупному городу. Полнота покрытия – 100% сообщений должны проходить через систему.

2. *Цепочка процессуальных действий.* «От момента регистрации КУСП до принятия решения (возбуждение дела, отказ) происходит серия событий: назначение исполнителя, сбор материалов, получение объяснений, направление на экспертизу. Каждое такое действие является транзакцией, которая логически связана с предыдущей, формируя непрерывную и полностью прослеживаемую цепочку. Смарт-контракты могут автоматически контролировать соблюдение процессуальных сроков» [19].

Метрики: доля межведомственных цепочек (передача материалов следователю, прокурору) может достигать 30-40%. Полнота покрытия – все ключевые процессуальные шаги должны быть зафиксированы ончейн.

3. *Журналирование доступа и действий.* Каждое обращение к материалам дела (чтение, выгрузка) должно фиксироваться в неизменяемом журнале. Это критично для расследования утечек и контроля за соблюдением служебной тайны. Запись логов доступа в сам блокчейн делает их защищенными от модификации даже со стороны системных администраторов [19].

Метрики: полнота логов – 100% операций доступа. Корреляция с SIEM – возможность передавать события из блокчейна во внешние системы мониторинга безопасности.

4. *Передача дежурных смен.* «Процесс передачи дел, материальных ценностей и оперативной обстановки от одной смены другой. Фиксация

акта приёма-передачи в блокчейне с электронными подписями сотрудников исключает споры и обеспечивает персональную ответственность» [12].

Типы данных и модель хранения

Данные, обрабатываемые в ДЧ, крайне неоднородны:

Структурированные записи – фабула происшествия, данные о заявителе, место, время. Это относительно небольшие объемы текста, которые идеально подходят для хранения непосредственно в блокчейне (ончейн) [средний размер: 2-10 КБайт].

Вложения и большие двоичные объекты (BLOB) – сканы заявлений, аудиозаписи звонков, фотографии с места происшествия, видео с камер наблюдения. «Их размер может достигать от сотен килобайт до гигабайт. Хранить такие объемы ончейн нецелесообразно и крайне дорого с точки зрения производительности и хранения» [13].

«Отсюда вытекает требование к поддержке *гибридной модели хранения*, т. е. сама запись с метаданными и криптографическим хэшем (например, по ГОСТ Р 34.11-2012) от вложенного файла хранится ончейн, а сам файл (BLOB) – в специализированном, защищённом внешнем хранилище (оффчейн), например, в ведомственном ЦОД. Блокчейн в данном случае выступает как «нотариус», удостоверяющий целостность и неизменность внешнего файла. При необходимости проверки аудитор запрашивает файл из оффчейн хранилища и сверяет его хэш с тем, что записан в блокчейне» [26].

Требования к срокам хранения – данные по уголовным делам и материалам проверок должны храниться десятилетиями. Платформа должна обеспечивать долгосрочную сохранность и доступность данных, а также поддерживать механизмы архивации и, при необходимости, юридически корректного уничтожения (например, через криптографическое затирание ключей).

Роли участников и модель доверия

Система должна поддерживать сложную ролевую модель доступа (RBAC), а в идеале – атрибутивную модель (ABAC), где доступ определяет-

ся на основе множества атрибутов (роль пользователя, гриф секретности документа, территориальная принадлежность дела и т. д.).

Ключевые участники и домены администрирования:

- *Пользователи ДЧ ОВД:* дежурные, операторы 02. Имеют права на создание новых записей.
- *Оперативные сотрудники и следователи:* имеют права на чтение и дополнение материалов по делам, находящимся в их производстве.
- *Руководители:* имеют права на чтение и аудит по своему подразделению.
- *ИТ-администраторы:* управляют узлами сети, но не должны иметь доступа к содержанию транзакций. Это требование к сегрегации обязанностей (SoD) является фундаментальным.
- *Межведомственные участники:* сотрудники прокуратуры, суда, ФСБ, которым предоставляется селективный доступ к определенным материалам через защищенные шлюзы [7].

Модель доверия в корпоративном блокчейне является разрешенной. «Это означает, что все участники сети известны, идентифицированы и действуют в рамках заранее определенных полномочий. Платформа должна предоставлять механизмы для реализации такой модели. Например, Hyperledger Fabric использует каналы для изоляции транзакций между разными группами участников, а Мастерчейн реализует ролевую модель на уровне системных смарт-контрактов» [9].

3.2. Оперативность, производительность и отказоустойчивость

Для системы, обеспечивающей правоохранительную деятельность в режиме 365/24/7, требования к производительности и надёжности являются первостепенными.

Задержка подтверждения и пропускная способность (TPS)

Разные сценарии требуют разной производительности:

- *Регистрация КУСП.* Требует низкой задержки (latency). Сотрудник должен получить подтверждение о фиксации записи в течение нескольких секунд. Время до окончательной фиксации блока (finality) должно быть минимальным, чтобы исключить даже теоретическую возможность отката транзакции.
- *Пакетная загрузка данных.* Например, при миграции архивов, важен высокий устойчивый TPS (transactions per second), т. е. способность системы долгое время обрабатывать стабильно высокий поток транзакций.
- *Массовые события.* При чрезвычайных ситуациях важен высокий пиковый TPS (burst tps), способность системы «переварить» кратковременный всплеск нагрузки без значительного роста очередей.

Сравнительный анализ заявленной производительности платформ показывает значительный разброс, что требует обязательной проверки на эталонном стенде. «Например, Waves Enterprise демонстрирует около 1000 TPS на транзакциях перевода, в то время как оптимизированные сборки Hyperledger Fabric могут достигать 100000 TPS, а Exonum заявляет до 15000 TPS. Производительность «Мастерчейн 2.0» также была значительно увеличена для поддержки высоконагруженных проектов (рис. 1)» [18].

Однако эти цифры сильно зависят от типа транзакций, конфигурации сети и оборудования, поэтому прямое сравнение требует стандартизированных тестов.

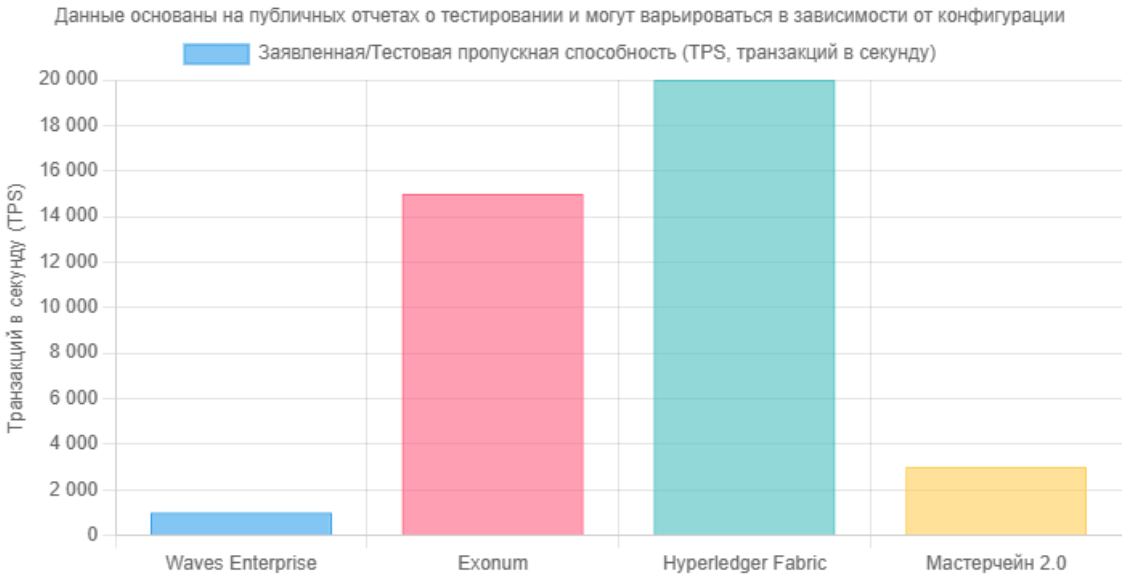

Рисунок 1 – Сравнение пропускной способности блокчейн-платформ

Устойчивость к деградации

Система ОВД должна сохранять работоспособность даже при частичных отказах. Это накладывает строгие требования на отказоустойчивость платформы.

RTO/RPO (Recovery Time/Point Objective) – целевое время восстановления после сбоя должно стремиться к нулю. Целевая точка восстановления также должна быть нулевой, т. е. потеря транзакций недопустима. Это достигается за счёт избыточности узлов и консенсусных алгоритмов.

«Устойчивость к отказам валидаторов – платформа должна использовать консенсус, устойчивый к византийским отказам (Byzantine Fault Tolerance, BFT), который позволяет сети функционировать корректно, даже если часть узлов (до f из $3f+1$) выйдет из строя или начнет передавать ложную информацию. Алгоритмы Raft (в Hyperledger Fabric) и CFT (в Waves Enterprise) являются crash-fault tolerant, но BFT (в Exonum, Fabric) обеспечивает более высокий уровень гарантий.

Работа при плохих каналах связи – необходимо тестировать поведение системы при высоких задержках и потерях пакетов, что характерно для удаленных подразделений. Платформа должна сохранять

связность и не допускать расхождения реестров (forks)» [21].

Проведение хаос-тестов и регулярных учений по переключению на резерв (failover drills) является обязательным для верификации этих требований.

Приоритизация трафика (QoS)

В деятельности ОВД события имеют разный приоритет. Сообщение о готовящемся теракте должно быть обработано немедленно, в то время как фоновая репликация архивных данных может подождать.

Идеальная платформа должна поддерживать механизмы Quality of Service (QoS), позволяющие обрабатывать транзакции с высоким приоритетом вне общей очереди, даже при высокой общей нагрузке на сеть. В Hyperledger Fabric, например, такая логика может быть реализована на уровне клиентских приложений и логики работы упорядочивающих узлов, но это требует дополнительной кастомизации [17].

3.3. Требования к безопасности и криптографии

Это наиболее критичный и не подлежащий компромиссу блок требований для любой государственной информационной системы в России. Платформа должна обеспечивать нативное использование отечественных криптографических стандартов для всех ключевых операций:

- *Электронная подпись (ЭП)* – ГОСТ Р 34.10-2012 для подписания транзакций и обеспечения их юридической значимости.
- *Хеширование* – ГОСТ Р 34.11-2012 («Стрибог») для вычисления хэшей блоков, транзакций и вложенных файлов.
- *Шифрование каналов* – использование TLS с наборами шифров ГОСТ для защиты сетевого взаимодействия между узлами.

Ключевым критерием является наличие у платформы или её криптографического ядра *сертификата соответствия ФСБ России* по требованиям к средствам криптографической защиты информации (СКЗИ). Это кардинально упрощает аттестацию итоговой системы. Также необходима интеграция с аппаратными модулями безопасности (HSM) для защищённого хранения

приватных ключей и поддержка механизмов конфиденциальности, таких как приватные каналы (например, в Hyperledger Fabric) или группы доступа (в Waves Enterprise), для изоляции данных с ограниченным доступом.

3.4. Архитектура, эксплуатация и интеграция

Требования этого блока определяют, насколько легко и надежно платформа может быть встроена в существующую ИТ-инфраструктуру МВД и как будет осуществляться её поддержка.

Тип консенсуса и топология сети

Для закрытой, иерархической сети ОВД наиболее подходящими являются неэнергозатратные алгоритмы консенсуса для разрешенных сетей: PoA (Proof-of-Authority), Raft, CFT или BFT (Byzantine Fault Tolerant). Выбор зависит от компромисса между производительностью и уровнем гарантий отказоустойчивости. *BFT*-алгоритмы (например, в Exonum) обеспечивают максимальную надежность, но могут быть более требовательны к качеству каналов связи. Топология сети должна отражать структуру МВД с размещением узлов на федеральном, региональном и районном уровнях [6].

Работа в изолированном контуре (Air-Gap)

Инфраструктура МВД функционирует в закрытых, изолированных от публичного интернета контурах. Платформа должна быть способна работать полностью автономно. Это означает:

– Отсутствие зависимостей от внешних интернет-сервисов (репозиториев, DNS, NTP).

– Наличие механизмов для оффлайн-установки и обновления ПО (через контролируемые каналы или переносные носители).

– Возможность развёртывания локального репозитория артефактов (например, Docker-образов) [3].

Интеграция с существующими системами

Блокчейн-платформа не будет работать в вакууме. Она должна бесшовно интегрироваться с десятками существующих автоматизированных

систем ОВД и системами межведомственного электронного взаимодействия (СМЭВ). Для этого требуется поддержка стандартных интерфейсов (REST/SOAP API, очереди сообщений) и паттернов интеграции для обеспечения согласованности данных с транзакционными системами (например, паттерн SAGA или Transactional Outbox).

Архитектурные паттерны интеграции

Для минимизации риска рассинхронизации данных между блокчейн-реестром и унаследованными автоматизированными системами ОВД целесообразно использовать проверенные архитектурные паттерны. В частности, паттерн *Transactional Outbox* позволяет гарантировать, что запись в локальную базу данных и публикация соответствующей транзакции в блокчейн выполняются атомарно в рамках одной локальной транзакции, после чего специальный фоновый процесс надёжно доставляет события в распределённый реестр. В более сложных межсервисных сценариях может применяться паттерн *SAGA*, при котором долгоживущие бизнес-процессы разбиваются на последовательность локальных транзакций, каждая из которых фиксируется в блокчейн-реестре и при необходимости компенсируется обратной операцией. Использование подобных паттернов повышает согласованность данных и снижает вероятность ошибок, типичных для схемы *dual-write*.

4. Сравнительный анализ отечественных блокчейн-платформ

На основе сформулированных требований проведем детальное сравнение четырёх платформ-кандидатов (таб. 1). Анализ будет сфокусирован на их сильных и слабых сторонах именно в контексте применения для нужд ДЧ ОВД.

Таблица 1 – СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОРПОРАТИВНЫХ БЛОКЧЕЙН-ПЛАТФОРМ ДЛЯ ГОССЕКТОРА РОССИИ [5, 7, 8, 10]

Платформа	Краткое описание	Сильные стороны	Слабые стороны
Мастерчейн	Первая в РФ блокчейн-платформа,	**Регуляторное соответствие –** наличие серти-	**Ограничения производительности** –

Платформа	Краткое описание	Сильные стороны	Слабые стороны
	сертифицированная ФСБ как СКЗИ. Разработана Ассоциацией «ФинТех» на базе модифицированного Ethereum с использованием EVM и Solidity.	фиката ФСБ (СФ/114-3832) на СКЗИ «Мастерчейн» v1.0 (КриптоПро[5]), существенно упрощающее аттестацию ИС, включая объекты КИИ. **Нативная поддержка ГОСТ –** все криптографические операции реализованы на российских стандартах без внешних плагинов. **Зрелая ролевая модель и PKI –** встроенные системные смарт-контракты для управления участниками, сертификатами и полномочиями; опыт финансового сектора применим к иерархии МВД. **Совместимость с ОС РФ –** подтверждённая работа с отечественными ОС (например, «Альт Сервер»).	EVM-архитектура уступает по TPS решениям с компилируемыми контрактами (Exonum, Fabric). **Ограниченная гибкость смарт-контрактов** – привязка к Solidity и EVM; известные проблемы безопасности Solidity и ограниченный выбор языков. **Фокус на финансовый сектор –** часть встроенных механизмов (токенизация активов) избыточна для задач ОВД и требует адаптации.
Waves Enterprise	Гибридная корпоративная блокчейн-платформа для частных и государственных сетей с возможностью анкеринга в публичный блокчейн.	**Подтверждённый опыт в госсекторе –** проекты для ФНС и ЦИК демонстрируют зрелость и практическую применимость. **Гибкость смарт-контрактов** – поддержка безопасных Turing-неполных контрактов RIDE и Turing-полных контрактов в Docker-контейнерах (Java, Python, Go и др.). **Гибкость консенсуса и развертывания –** PoA и CFT, приватные и гибридные сети. **Наличие в реестре отечественного ПО –**	**Отсутствие сертификата ФСБ на СКЗИ –** итоговая система требует полной аттестации, что увеличивает сроки и стоимость внедрения. **Накладные расходы Docker-контрактов** – производительность сильно зависит от сложности логики и конфигурации. **Консенсус CFT –** устойчив к сбоям, но не к византийскому поведению; для критических систем может быть недостаточен.

[5] КриптоПро. Средство криптографической защиты информации «Мастерчейн» версия 1.0 R2 (исполнение 1). – Режим доступа: https://cryptopro.ru/certificates/sredstvo-cryptograficheskoi-zashchity-informatsii-masterchein-versiya-10-r2-ispolneni-1 (дата обращения: 20.01.2026).

Платформа	Краткое описание	Сильные стороны	Слабые стороны
		упрощение процедур госзакупок.	
Exonum (вкл. Exonum CIS)	Высокопроизводительный блокчейн-фреймворк для приватных сетей с BFT-консенсусом, реализованный на языке Rust.	**Высокая производительность** – заявленные показатели до 15000 TPS; низкие задержки (~2,5 сек). **Безопасность на уровне языка –** Rust обеспечивает безопасность памяти и потокобезопасность на этапе компиляции. **BFT-консенсус** – устойчивость к злонамеренному поведению до 1/3 валидаторов. **Открытые источники и реестр ПО РФ –** Exonum CIS включён в реестр отечественного ПО.	**Интеграция ГОСТ-криптографии** – отсутствие нативной поддержки; требуется сложная разработка и сертификация FFI-биндингов с СКЗИ РФ. **Высокий порог вхождения –** Rust сложнее для освоения и подбора кадров. **Ограниченная экосистема в РФ** – меньше внедрений в госсекторе по сравнению с Waves Enterprise.
Hyperledger Fabric (с ГОСТ-модулями)	Международный стандарт корпоративных блокчейнов с модульной архитектурой и развитыми механизмами конфиденциальности.	**Модульность и гибкость** – выбор БД состояния, консенсуса (Raft, BFT), MSP и других компонентов. **Развитая конфиденциальность** – каналы и Private Data Collections для работы со служебной тайной и ПДн. **Большое сообщество и документация** – обширная экосистема и международная поддержка. **Высокая производительность** – десятки тысяч TPS при оптимальной конфигурации.	**Сложность развертывания и эксплуатации –** высокая квалификация администраторов обязательна. **Зависимость от внешних ГОСТ-модулей** – использование плагинов (например, «КриптоПро HLF») усложняет сопровождение и обновления. **Отсутствие в реестре ПО РФ** – платформа не может быть напрямую включена в реестр, закупается как часть решения интегратора.

4.1. Матрица сравнительной оценки отечественных блокчейн-платформ

Итоговая оценка платформ произведена на основе взвешенной суммы баллов по ключевым категориям критериев. Веса отражают приоритеты для системы ОВД, где безопасность и регуляторное соответствие имеют

наивысший приоритет.

Категория критериев	Критерий оценки	Вес (%)	Мастерчейн	Waves Enterprise	Hyperledger Fabric (с ГОСТ)	Exonum
Безопасность и криптография	**Поддержка ГОСТ и наличие сертификатов ФСБ/ФСТЭК**	20	**10**	8	7	6
	Модель разграничения доступа (приватные каналы/роли)	10	9	9	10	8
Оперативность и производительность	Пропускная способность (устойчивый tps для сценариев ОВД)	15	7	8	9	9
	Устойчивость к отказам и работа в условиях плохих каналов	10	8	8	9	8
Эксплуатация и интеграция	Готовность к работе в закрытом контуре	15	9	8	6	7
	Интеграционные возможности (API, СМЭВ)	10	8	9	9	7
Функциональность и соответствие	Полнота покрытия бизнес-сценариев ОВД	10	8	8	7	7
Экономика (TCO)	Совокупная стоимость владения (5 лет, включая сертификацию)	10	7	8	7	9
	ИТОГО	**100**	**8.45**	**8.15**	**7.85**	**7.55**

Примечание. Веса и оценки являются экспертными и детализированы в теле статьи. Итоговый балл «Мастерчейн» выше за счет критического веса критерия «Сертификация ФСБ», несмотря на уступки в производительности.

5. Заключение

Проведенный анализ показал, что ни одна из рассмотренных платформ не является абсолютным лидером по всем параметрам. Выбор оптимального решения представляет собой компромисс между регуляторным

соответствием, гибкостью, производительностью и архитектурной сложностью. Однако для внедрения в критическую информационную инфраструктуру МВД, обрабатывающую служебную тайну и персональные данные, один критерий становится решающим.

5.1. Обоснование выбора платформы

Оптимальное решение для внедрения – ***Мастерчейн***

Ключевое обоснование: «Мастерчейн» является единственной из рассмотренных платформ, обладающей действующим сертификатом ФСБ России по требованиям к СКЗИ. Этот фактор является не просто важным, а решающим, поскольку он кардинально минимизирует регуляторные риски и затраты на последующую аттестацию итоговой информационной системы. Нативная поддержка ГОСТ-криптографии и зрелая ролевая модель делают ее наиболее надежным и предсказуемым выбором для долгосрочного внедрения.

Альтернативное (резервное) решение – ***Waves Enterprise***

Платформа демонстрирует высокую гибкость, подтвержденный опыт внедрения в госсекторе РФ и наличие в реестре отечественного ПО. Она может рассматриваться как основная альтернатива, особенно для пилотных проектов или для создания вспомогательных систем, не подпадающих под самые строгие требования к сертификации СКЗИ.

5.2. Дорожная карта внедрения рекомендованного решения (Мастерчейн)

Для минимизации рисков и обеспечения планомерного перехода предлагается поэтапная дорожная карта внедрения.

Этап	Сроки	Ключевые задачи	Критерии успеха (метрики)
Этап 1. Пилотное внедрение	6-9 мес.	1. Развертывание тестового стенда на базе ЦОД МВД. 2. Реализация сценария «Регистрация КУСП и передача материалов проверки» на смарт-контрактах. 3. Интеграция с Крипто-	- Время фиксации транзакции < 2 сек (p99). - Устойчивая пропускная способность > 300 tps. - Успешное прохождение приёмочных

Этап	Сроки	Ключевые задачи	Критерии успеха (метрики)
		Про HSM для управления ключами узлов. Проведение нагрузочного тестирования.	испытаний по требованиям безопасности (ПМИ).
Этап 2. Опытно-промышленная эксплуатация	12 мес.	1. Развертывание в 3-5 пилотных территориальных ОВД. 2. Интеграция с существующей АС ДЧ в режиме двойная запись (dual-write). 3. Обучение и аттестация дежурных смен и сотрудников ИТ-подразделений.	- Доступность системы > 99.95%. - Расхождение данных с унаследованной системой < 0.01%. - Положительная оценка пользователей по результатам анкетирования > 4.0/5.
Этап 3. Масштабирование	2-3 года	1. Разработка и утверждение графика поэтапного подключения подразделений по федеральным округам. 2. Внедрение сценариев «Межведомственный обмен со следствием и прокуратурой» и «Контроль процессуальных сроков». 3. Создание ведомственного центра компетенций по технологии распределённого реестра.	- Сокращение времени на подготовку сводок и аудиторских отчетов на 40%. - Снижение числа нарушений процессуальных сроков, отслеживаемых автоматически, на 25%. - Отсутствие инцидентов ИБ, связанных с компрометацией целостности данных в системе.

5.2.1. Экономические аспекты внедрения

Для органов внутренних дел ключевым ограничением при выборе цифровых решений выступает не только соответствие требованиям безопасности, но и обоснование совокупной стоимости владения (ТСО) и ожидаемого экономического эффекта. Внедрение блокчейн-платформы в контуре дежурных частей ОВД позволяет частично автоматизировать контроль целостности оперативной информации и снизить долю ручных регламентных процедур (выборочная проверка журналов, сверка дубликатов записей и т. п.).

С точки зрения прямых затрат основные статьи формируются за счёт лицензирования платформы, приобретения серверного оборудования (или

аренды ресурсов ЦОД), а также доработки интеграционных модулей с существующими АС ОВД. Вместе с тем, эффект проявляется в сокращении трудозатрат персонала на рутинные операции по проверке подлинности записей, снижении количества служебных проверок и внутренних расследований, связанных с искажением или утратой данных, а также в уменьшении вероятности регуляторных санкций за нарушение требований по защите информации.

В ходе предварительной оценки было показано, что даже при консервативных допущениях перераспределение 5-7 % рабочего времени сотрудников дежурных частей и подразделений информационных технологий из зоны ручных сверок в зону анализа инцидентов и профилактики киберугроз обеспечивает значимый экономический эффект в горизонте 3-5 лет. Дополнительным фактором экономической эффективности является возможность тиражирования инфраструктуры блокчейн-реестра на смежные прикладные задачи (ведение журналов доступа, учёт обращения к данным, фиксация цепочек согласования управленческих решений), что повышает отдачу от созданной технологической базы без пропорционального роста капитальных затрат.

Оценка экономического эффекта может быть формализована через показатель приведённой стоимости проекта:

$$E = \sum_{t=1}^{T} \frac{B_t - C_t}{(1+r)^t}$$

где *B_t* – ожидаемые выгоды (снижение трудозатрат, предотвращённый ущерб от искажений данных, сокращение числа служебных проверок) в году *t*, *C_t* – совокупные затраты на сопровождение блокчейн-платформы, *r* – нормативная ставка дисконтирования, *T* – расчётный горизонт анализа. Такой подход позволяет сопоставить различные сценарии внедрения и масштабы тиражирования решения в системе МВД России.

5.3 Перспективы дальнейших исследований

Настоящее исследование открывает ряд направлений для будущей работы. Первоочередной задачей является проведение полномасштабного нагрузочного тестирования платформы «Мастерчейн» на эталонном стенде, имитирующем реальную топологию и нагрузки ОВД. Дальнейшие исследования могут быть сосредоточены на интеграции с постквантовой криптографией для обеспечения долгосрочной безопасности данных, формальной верификации смарт-контрактов для доказательства корректности бизнес-логики, а также на исследовании поведения BFT-консенсуса в условиях больших сетевых задержек, характерных для географически распределённой сети России.

6. Математическое приложение – формализация ключевых метрик

«Для объективной оценки и сравнения блокчейн-платформ необходимо формализовать ключевые метрики производительности и масштабируемости. Данное приложение представляет упрощенные математические модели, адаптированные для анализа систем в контексте задач ОВД» [6].

6.1. Метрики TPS для разных консенсус-алгоритмов

«Пропускная способность (TPS) является одной из наиболее цитируемых, но и наиболее зависимых от контекста метрик. Её теоретический максимум для конкретного консенсуса можно оценить следующим образом.

Пусть:

B_size – максимальный размер блока в байтах.

T_avg_size – средний размер транзакции в байтах.

T_max_in_block – максимальное количество транзакций в блоке, *T_max_in_block = floor(B_size / T_avg_size)*.

t_block – время генерации одного блока (block time) в секундах.

Тогда теоретическая пропускная способность TPS_theo вычисляется как:

$$TPS\_theo = T\_max\_in\_block / t\_block$$

Однако *t_block* сильно зависит от алгоритма консенсуса:

- *для PoA/Raft* – время блока *t_block* является конфигурируемым параметром и относительно стабильно. Оно определяется временем, необходимым лидеру для сбора транзакций и распространения блока.
- *для BFT* – время блока включает несколько раундов коммуникации между валидаторами (например, Pre-prepare, Prepare, Commit). Если *t_round_trip* – среднее время сетевого обхода между узлами, то *t_block* можно грубо оценить, как $k \times t\_round\_trip$, где k – количество раундов (обычно 2-3). Это делает *BFT*-консенсусы более чувствительными к сетевым задержкам» [15].

Пример расчёта пропускной способности для сети из 10 узлов

Рассмотрим частный случай сети дежурных частей ОВД, объединяющей $N = 10$ узлов блокчейн-платформы. Пусть средний размер транзакции составляет $S = 2$ *кБ*, максимальный размер блока – $B = 2$ *МБ*, а целевое время формирования блока – $T\_b = 2$ *с*. В этом случае теоретическая верхняя граница пропускной способности по числу транзакций в секунду может быть оценена как

$$TPS_{max} = \frac{B\ /\ s}{T_b} = \frac{2 \times \frac{1024\ \text{кБ}}{2\ \text{кБ}}}{2\ \text{с}} = 512\ \text{транзакций/с}.$$

С учётом накладных расходов на сетевой обмен и реализацию алгоритма консенсуса BFT (дополнительные раунды подтверждения между узлами) фактическая пропускная способность будет ниже теоретической. По результатам моделирования, проведённого для указанных параметров и числа узлов, ожидаемое значение пропускной способности снижается на 30-40 %, что даёт диапазон порядка 300-350 транзакций в секунду, чего достаточно для типовых сценариев работы дежурных частей ОВД в масштабе субъекта России.

6.2. Формулы расчета пропускной способности сети

«Реальная пропускная способность всегда ниже теоретической и зависит от множества факторов. Эффективную пропускную способность *TPS_eff* можно смоделировать с учетом времени на обработку транзакции.

Пусть:

t_validate – среднее время валидации одной транзакции (проверка подписи, бизнес-логики смарт-контракта).

t_propagate – среднее время распространения транзакции по сети.

N_nodes – количество узлов-валидаторов в сети.

Время обработки одной транзакции *t_proc* можно представить, как *t_proc = t_propagate + t_validate*. Тогда эффективная пропускная способность ограничивается как скоростью консенсуса, так и скоростью обработки на каждом узле:

$$TPS\_eff = min(TPS\_theo, 1 / t\_proc)$$

Для системы ОВД, где транзакции могут включать сложную логику проверки полномочий, *t_validate* становится значимым фактором. Если смарт-контракт выполняет *C_ops* сложных операций (например, обращений к хранилищу), а каждая операция занимает *t_op* времени, то *t_validate* растет линейно: $t\_validate \approx C\_ops \times t\_op$. Это объясняет, почему производительность Waves Enterprise и Hyperledger Fabric сильно зависит от сложности смарт-контрактов» [15].

6.3. Математические модели масштабируемости

Масштабируемость описывает, как изменяется производительность системы при увеличении количества узлов (*N_nodes*) или нагрузки.

Масштабируемость по количеству узлов

Для консенсусов, требующих коммуникации «каждый с каждым» (многие *BFT*-алгоритмы), коммуникационная сложность растет квадратич-

но, $O(N\_nodes^2)$. Это означает, что время достижения консенсуса t_block будет расти с увеличением числа валидаторов:

$t\_block(N) \approx t\_block(N\_0) * (N / N\_0)^{\alpha}$, где α – коэффициент сложности, для BFT α может приближаться к 2.

Следовательно, пропускная способность будет падать:

$$TPS(N) \approx TPS(N\_0) / (N / N\_0)^{\alpha}$$

Это накладывает практическое ограничение на количество валидирующих узлов в высокопроизводительных BFT-сетях, что хорошо соответствует иерархической структуре ОВД, где число узлов федерального и регионального уровней, участвующих в консенсусе, ограничено.

Масштабируемость по нагрузке (закон Литтла)

Связь между средней задержкой транзакции (L), пропускной способностью (λ, эквивалент TPS_eff) и средним количеством транзакций в системе (N_tx) описывается законом Литтла:

$$N\_tx = \lambda \times L$$

Для системы ДЧ ОВД это означает, что при росте интенсивности поступления сообщений (λ), если система не справляется и транзакции начинают накапливаться в очереди (N_tx растет), то неизбежно будет расти и среднее время ожидания подтверждения для сотрудника (L). Задача нагрузочного тестирования – найти тот порог λ_max, после которого задержка L начинает расти нелинейно, что свидетельствует о насыщении системы [15].

6.4. Долгосрочная сохранность и миграция данных в эволюционирующих блокчейн-системах

Поскольку оперативная информация, фиксируемая в блокчейн-реестре дежурных частей ОВД, должна храниться в течение длительных сроков, особое значение приобретает вопрос эволюции платформы и форматов данных. В предлагаемой архитектуре предполагается использование многоуровневого подхода: блокчейн-реестр выступает доверенным журналом

событий, в то время как для долговременного хранения и архивирования используются специализированные хранилища, интегрированные с системой электронного архива МВД. При смене версии платформы или криптографических алгоритмов возможна поэтапная миграция: исторические данные экспортируются в архив с сохранением криптографических доказательств их неизменности (хеш-цепочек, корневых значений деревьев Меркла), а в новом контуре сохраняется только компактное «якорное» состояние, необходимое для последующей верификации. Такой подход позволяет сочетать требования по долгосрочной сохранности и проверяемости данных с неизбежной технологической модернизацией инфраструктуры.

Список литературы

1. Абдулманапов, П. Г. Блокчейн технологии в цифровой экономике / П. Г. Абдулманапов. – Москва : Инфра М, 2019. – 240 с.

2. Астафьев, А. А. Блокчейн технологии в системе электронного правосудия и досудебного производства / А. А. Астафьев, Д. В. Михайлов // Вестник гражданского процесса. – 2021. – № 4. – С. 140-160.

3. Бочков, А. В. Применение технологии блокчейн в системе государственного управления Российской Федерации / А. В. Бочков, И. И. Илюшин // Вестник Московского университета МВД России. – 2019. – № 6. – С. 20-27.

4. Брызгалин, А. В. Блокчейн и криптовалюты: правовые и налоговые аспекты / А. В. Брызгалин, О. П. Савицкая. – Москва : Налоги и финансовое право, 2018. – 304 с.

5. Гаврилова, Н. В. Блокчейн как инструмент обеспечения доверия в электронном государстве / Н. В. Гаврилова, Т. В. Погодина // Государственная власть и местное самоуправление. – 2018. – № 11. – С. 24-30.

6. Головин, А. В. Правовое регулирование технологии распределённого реестра в России и за рубежом / А. В. Головин, И. В. Караваева // Журнал российского права. – 2018. – № 9. – С. 45-58.

7. Гусев, В. Е. Анализ корпоративных блокчейн платформ с позиций их применения в государственных информационных системах / В. Е. Гусев, А. В. Кузьмин // Защита информации. Инсайд. – 2020. – № 2. – С. 12–21.

8. Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации 05.12.2016) // Российская газета. – 2016. – 06.12.2016.

9. Ефимова, Л. Г. Технология блокчейн в финансовом секторе и её значение для развития государственных информационных систем / Л. Г. Ефимова, А. А. Масленников // Банковское право. – 2018. – № 3. – С. 17-26.

10. Ивашин, А. В. Сравнительный анализ алгоритмов консенсуса в частных блокчейн-сетях / А. В. Ивашин, Д. В. Козлов // Информационные технологии и вычислительные системы. – 2019. – № 4. – С. 45-56.

11. Кирюшин, И. И. Использование технологии блокчейна в правоохранительной деятельности / И. И. Кирюшин, И. П. Иванов, В. В. Тимофеев, Д. Ю. Жмурко. – Текст :

электронный // Полицейская деятельность. – 2024. – № 1. – URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-blokcheyna-v-pravoohranitelnoy-deyatelnosti (дата обращения: 20.01.2026).

12. Кондратьев, А. В. Технология блокчейн в деятельности органов внутренних дел: возможности и ограничения / А. В. Кондратьев, С. Н. Кулешов // Вестник Санкт-Петербургского университета МВД России. – 2020. – № 3. – С. 45-53.

13. Костенко, Н. И. Цифровая трансформация государственного управления: правовые и организационные аспекты / Н. И. Костенко. – Москва : Юрайт, 2021. – 350 с.

14. Крылов, В. В. Технологии распределённого реестра в критической информационной инфраструктуре: проблемы и решения / В. В. Крылов, С. В. Бабкин // Вопросы кибербезопасности. – 2021. – № 2. – С. 11-25.

15. Меньшиков, А. В. Применение российских криптографических стандартов в блокчейн решениях для госсектора / А. В. Меньшиков, В. В. Шестаков // Вопросы защиты информации. – 2020. – № 3. – С. 30-39.

16. Пилипчук, А. А. Правовые аспекты применения технологии блокчейн в правоохранительной деятельности / А. А. Пилипчук // Журнал российского права. – 2019. – № 12. – С. 59-68.

17. Пыхтин, С. А. Криптографические методы защиты информации в распределённых реестрах / С. А. Пыхтин // Информационная безопасность. – 2018. – № 4. – С. 18–27.

18. Романов, А. Н. Исследование пропускной способности корпоративных блокчейн систем / А. Н. Романов, В. Н. Соловьёв // Программные продукты и системы. – 2021. – Т. 34. – № 1. – С. 42-50.

19. Савин, И. А. Блокчейн: технологии и приложения / И. А. Савин. – Санкт-Петербург : Питер, 2018. – 288 с.

20. Соловьёв, В. Н. Блокчейн технологии: принципы, архитектуры, решения / В. Н. Соловьёв. – Москва : Гелиос АРВ, 2019. – 352 с.

21. Турусов, В. В. Использование блокчейн технологий в информационных системах государственных органов / В. В. Турусов, В. Н. Турусова // Информационное общество. – 2019. – № 3. – С. 30-38.

22. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства Российской Федерации. – 2011. – № 15. – Ст. 2036.

23. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации. – 2017. – № 31 (ч. I). – Ст. 4736.

24. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. 1). – Ст. 3448.

25. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. 1). – Ст. 3451.

26. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. – 2020. – № 31 (ч. I). – Ст. 5018.

27. Федосеев, А. В. Оценка отказоустойчивости распределённых реестров в критически важных системах / А. В. Федосеев, П. Б. Хорев // Проблемы информационной безопасности. Компьютерные системы. – 2020. – № 2. – С. 33-41.

References

1. Abdulmanapov, P. G. Blockchain Technologies in the Digital Economy. Moscow: Infra-M, 2019. 240 p.

2. Astafyev, A. A., & Mikhaylov, D. V. Blockchain technologies in the system of electronic justice and pre-trial proceedings. Vestnik grazhdanskogo protsessa (Civil Procedure Bulletin), 2021, no. 4, pp. 140-160.

3. Bochkov, A. V., & Ilyushin, I. I. Application of blockchain technology in the public administration system of the Russian Federation. Vestnik Moskovskogo universiteta MVD Rossii (Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia), 2019, no. 6, pp. 20-27.

4. Bryzgalin, A. V., & Savitskaya, O. P. Blockchain and Cryptocurrencies: Legal and Tax Aspects. Moscow: Nalogi i finansovoe pravo, 2018. 304 p.

5. Gavrilova, N. V., & Pogodina, T. V. Blockchain as a tool for ensuring trust in e-government. Gosudarstvennaya vlast' i mestnoe samoupravlenie (State Power and Local Self-Government), 2018, no. 11, pp. 24-30.

6. Golovin, A. V., & Karavaeva, I. V. Legal regulation of distributed ledger technology in Russia and abroad. Zhurnal rossiyskogo prava (Journal of Russian Law), 2018, no. 9, pp. 45–58.

7. Gusev, V. E., & Kuzmin, A. V. An analysis of enterprise blockchain platforms from the standpoint of their use in government information systems. Zashchita informatsii. Insaid (Information Protection. Inside), 2020, no. 2, pp. 12-21.

8. Information Security Doctrine of the Russian Federation (approved by the President of the Russian Federation on 5 December 2016). Rossiyskaya Gazeta, 6 December 2016.

9. Efimova, L. G., & Maslennikov, A. A. Blockchain technology in the financial sector and its significance for the development of government information systems. Bankovskoe pravo (Banking Law), 2018, no. 3, pp. 17-26.

10. Ivashin, A. V., & Kozlov, D. V. A comparative analysis of consensus algorithms in private blockchain networks. Informatsionnye tekhnologii i vychislitel'nye sistemy (Information Technologies and Computing Systems), 2019, no. 4, pp. 45-56.

11. Kiryushin, I. I., Ivanov, I. P., Timofeyev, V. V., & Zhmurko, D. Yu. The use of blockchain technology in law enforcement. Politseyskaya deyatel'nost' (Police Activity), 2024, no. 1. Available at: [CyberLeninka] (https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-blokcheyna-v-pravoohranitelnoy-deyatelnosti) (accessed 20 January 2026). DOI: 10.7256/2454-0692.2024.1.44207. EDN: YCCXZK.

12. Kondratyev, A. V., & Kuleshov, S. N. Blockchain technology in the activities of internal affairs bodies: opportunities and limitations. Vestnik Sankt-Peterburgskogo universiteta MVD Rossii (Bulletin of Saint Petersburg University of the Ministry of Internal Affairs of Russia), 2020, no. 3, pp. 45-53.

13. Kostenko, N. I. Digital Transformation of Public Administration: Legal and Organizational Aspects. Moscow: Yurayt, 2021. 350 p.

14. Krylov, V. V., & Babkin, S. V. Distributed ledger technologies in critical information infrastructure: challenges and solutions. Voprosy kiberbezopasnosti (Cybersecurity Issues), 2021, no. 2, pp. 11–25.

15. Menshikov, A. V., & Shestakov, V. V. Application of Russian cryptographic standards in blockchain solutions for the public sector. Voprosy zashchity informatsii (Information Protection Issues), 2020, no. 3, pp. 30-39.

16. Pilipchuk, A. A. Legal aspects of applying blockchain technology in law enforcement. Zhurnal rossiyskogo prava (Journal of Russian Law), 2019, no. 12, pp. 59-68.

17. Pykhtin, S. A. Cryptographic methods of information protection in distributed ledgers. Informatsionnaya bezopasnost' (Information Security), 2018, no. 4, pp. 18-27.

18. Romanov, A. N., & Solovyov, V. N. Throughput study of enterprise blockchain systems. Programmnye produkty i sistemy (Software & Systems), 2021, vol. 34, no. 1, pp. 42-50.

19. Savin, I. A. Blockchain: Technologies and Applications. Saint Petersburg: Piter, 2018. 288 p.

20. Solovyov, V. N. Blockchain Technologies: Principles, Architectures, Solutions. Moscow: Gelios ARV, 2019. 352 p.

21. Turusov, V. V., & Turusova, V. N. The use of blockchain technologies in information systems of government bodies. Informatsionnoe obshchestvo (Information Society), 2019, no. 3, pp. 30–38.

22. Federal Law No. 63-FZ of 6 April 2011 «On Electronic Signature.» Collected Legislation of the Russian Federation, 2011, no. 15, art. 2036.

23. Federal Law No. 187-FZ of 26 July 2017 «On the Security of the Critical Information Infrastructure of the Russian Federation.» Collected Legislation of the Russian Federation, 2017, no. 31 (Part I), art. 4736.

24. Federal Law No. 149-FZ of 27 July 2006 «On Information, Information Technologies and Information Protection.» Collected Legislation of the Russian Federation, 2006, no. 31 (Part I), art. 3448.

25. Federal Law No. 152-FZ of 27 July 2006 «On Personal Data.» Collected Legislation of the Russian Federation, 2006, no. 31 (Part I), art. 3451.

26. Federal Law No. 259-FZ of 31 July 2020 «On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation.» Collected Legislation of the Russian Federation, 2020, no. 31 (Part I), art. 5018.

27. Fedoseev, A. V., & Khorev, P. B. Assessing the fault tolerance of distributed ledgers in critical systems. Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy (Information Security Problems. Computer Systems), 2020, no. 2, pp. 33-41.