

Гунов Данил Павлович

студент бакалавриата
Иркутский национальный исследовательский
технический университет
Иркутск, Россия

**ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ВНЕДРЕНИЯ БЕЗОПАСНЫХ РАСПРЕДЕЛЁННЫХ
ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН****Аннотация**

Рассматриваются вопросы экономической эффективности внедрения безопасных распределённых информационных систем на основе технологии блокчейн в условиях цифровизации и стремления к технологическому суверенитету. Исследуются проблемы нормативной неопределённости, инфраструктурной фрагментации и отсутствия объективных методик оценки затрат и выгод от применения блокчейн-решений. Проводится анализ технологических, правовых и организационных факторов, влияющих на рентабельность таких систем в государственных и коммерческих структурах. Результатами исследования являются определение ключевых экономических преимуществ распределённых платформ, выявление барьеров интеграции и формулировка условий, при которых их внедрение становится экономически оправданным. Сделан вывод о необходимости комплексного подхода к оценке эффективности, включая разработку единых стандартов, нормативную поддержку и стимулирование масштабных внедрений.

Ключевые слова: блокчейн, распределённые системы, ИТ-инфраструктура

Введение

Экономическая эффективность цифровых решений сегодня становится не менее приоритетной, чем их технологическая надёжность. В условиях нарастающей сложности информационной инфраструктуры, а также стремления к импортонезависимости, особое внимание привлекают безопасные распределённые информационные системы, построенные на технологии блокчейн. Эти системы обещают не только повышение прозрачности и устойчивости к киберугрозам, но и оптимизацию затрат – как прямых, так и косвенных, связанных с хранением данных, управлением транзакциями и администрированием бизнес-процессов.

Мировая практика показывает, что блокчейн может радикально сократить число посредников, снизить издержки на верификацию данных, устранить дублирование функций и тем самым повысить общую операционную эффективность. Применение распределённого реестра в логистике, финансах, здравоохранении и госсекторе демонстрирует потенциал к экономии десятков процентов от бюджетов, ранее уходивших на контроль, аудит и обеспечение безопасности. Однако российская реальность, несмотря на интерес к инновациям, пока характеризуется ограниченным внедрением подобных решений. Чаще всего это локальные эксперименты без масштабного эффекта и системного анализа окупаемости.

Оценка экономической эффективности блокчейн-систем осложняется отсутствием утверждённых методик расчёта и единых подходов к сравнительной оценке затрат на внедрение и эксплуатацию. В результате решения на базе блокчейна рассматриваются преимущественно как технологическая новация, а не как экономически обоснованный инструмент цифровой трансформации. Между тем, при грамотной интеграции распределённые платформы способны не только повысить устойчивость критически важных информационных процессов, но и стать инструментом долгосрочного снижения совокупной стоимости владения ИТ-инфраструктурой.

В этом контексте возникает необходимость системного научного анализа, который охватывал бы как технические и регуляторные аспекты внедрения блокчейн-решений, так и их экономическую результативность в конкретных отраслях и сценариях. Требуется переход от абстрактных деклараций к построению моделей, отражающих реальную стоимость владения, сроки окупаемости, прирост операционной эффективности и возможные экономические риски, включая риски несопоставимости или отказа от интеграции с действующими системами.

Цель настоящего исследования – выявить и обосновать условия, при которых внедрение безопасных распределённых информационных систем на основе блокчейн-технологий становится экономически оправданным шагом в развитии цифровой экономики Российской Федерации. Задача – проанализировать потенциальные источники экономии, сформулировать барьеры, влияющие на достижение ожидаемого эффекта, и предложить подходы к объективной оценке эффективности таких решений в контексте цифрового суверенитета и устойчивого технологического развития.

Обсуждение и результаты исследования

Внедрение безопасных распределённых информационных систем (РИС), построенных на технологии блокчейн, рассматривается сегодня не только сквозь призму технологического суверенитета и информационной безопасности, но и как инструмент повышения экономической эффективности цифровой инфраструктуры. По мере того, как цифровая трансформация затрагивает всё больше отраслей – от государственного управления до логистики и энергетики – внимание к затратам, связанным с обработкой, защитой и проверкой данных, выходит на первый план.

Централизованные ИТ-системы, доминирующие в прежних моделях, требуют значительных расходов на администрирование, обеспечение отказоустойчивости,

аудит и киберзащиту. В условиях растущих рисков и необходимости сокращения бюджетов эти затраты становятся всё менее оправданными. Блокчейн предлагает альтернативу – децентрализованную архитектуру, где данные не зависят от единого оператора, а их верификация и безопасность встроены в саму структуру протокола. Это позволяет устранить дорогостоящие промежуточные процедуры, уменьшить число точек уязвимости и сократить операционные издержки за счёт автоматизации доверия между участниками.

Одним из ключевых экономических преимуществ блокчейн-систем является снижение транзакционных затрат. Технология позволяет отказаться от множественных слоёв проверки и хранения информации, заменяя их единым реестром с гарантированной неизменностью записей. Это особенно значимо в межведомственном взаимодействии, финансовых расчётах, верификации прав собственности и логистических цепочках. Например, в пилотных проектах в сфере поставок и логистики применение блокчейн-реестров позволило сократить расходы на документооборот на 20-40%, а время обработки одной транзакции – с нескольких дней до минут.

Рассматривая блокчейн с экономической позиции, важно учитывать не только его технологическую архитектуру, но и эффект масштаба. Чем шире круг участников, подключённых к распределённой системе, тем выше совокупная выгода: растёт прозрачность, ускоряется согласование действий, исчезает необходимость в избыточных проверках. Это особенно актуально для государств, где ведомственные системы традиционно работают изолированно, и каждая из них дублирует процессы в части безопасности и контроля.

Современная российская практика всё ещё ограничена фрагментарными внедрениями, и часто эти решения не сопровождаются экономическим анализом. Между тем потенциал повышения эффективности – один из сильнейших аргументов в пользу масштабного применения технологии. Блокчейн способен не только повысить надёжность, но и изменить саму модель управления цифровыми активами, сократив стоимость сопровождения, минимизировав риски потерь и оптимизировав использование вычислительных ресурсов.

Анализ научных публикаций последних лет (2020-2024 гг.) показывает, что внимание исследователей сосредоточено не только на технической устойчивости блокчейн-систем, но и на их применимости в экономически значимых сферах. В

работах И.Ф. Бессонова и Л.П. Захарова рассматриваются как публичные, так и приватные блокчейн-модели, подходящие для государственных задач, с акцентом на снижение затрат на инфраструктурную поддержку и обеспечение масштабируемости. В отечественных источниках подчёркивается важность соответствия требованиям регуляторов (ФСТЭК, ФСБ, Минцифры РФ), что напрямую влияет на экономическую жизнеспособность решений: несоответствие стандартам может увеличить расходы на доработку, интеграцию и сопровождение. Отдельно отмечаются проблемы сетевой латентности и перегрузки, способные негативно сказаться на окупаемости внедрения блокчейн-платформ в российских реалиях [1].

Практика внедрения распределённых систем на блокчейне в России ограничивается пока единичными кейсами, однако каждый из них демонстрирует как потенциал технологии, так и её системные ограничения. Примером может служить проект Министерства юстиции РФ по ведению распределённого реестра нотариальных действий, начатый в 2020 году. Несмотря на первоначальные успехи (снижение числа мошеннических действий, упрощение верификации), проект столкнулся с проблемой отказоустойчивости региональных серверов и слабой синхронизации данных при работе в условиях нестабильной сети. В 2022 году в Москве был запущен пилот по применению блокчейна для верификации строительной документации – платформа показала хорошую устойчивость к фальсификации, однако не обеспечила совместимости с уже действующими системами «1С: Документооборот», что привело к увеличению издержек на интеграцию [2].

По данным отчёта «Цифровая экономика 2024» (издательство НИУ ВШЭ), доля распределённых решений в цифровой инфраструктуре госорганов РФ составляет менее 4%, при этом уровень интереса к блокчейн-проектам в энергетике, логистике и финансовом секторе превышает 30% (по данным опросов Минпромторга и Ассоциации Финтех). Однако главными ограничителями масштабного внедрения выступают нормативно-правовая неопределённость, отсутствие единых протоколов безопасности и разобщённость технических стандартов. Так, до сих пор отсутствует утверждённый ГОСТ на архитектуру блокчейн-сетей, равно как и методология сертификации их безопасности в рамках отечественной системы оценки соответствия.

В числе ключевых проблем следует выделить также следующие: во-первых, низкий уровень зрелости отечественных разработок блокчейн-платформ, в которых до 70% программных компонентов являются заимствованными или основаны на

открытом коде с недостоверной аттестацией. Во-вторых, кадровый дефицит – по оценкам Российской ассоциации криптоиндустрии, дефицит специалистов по безопасной разработке на блокчейне составляет более 2000 человек ежегодно. В-третьих, отсутствие регламентированных процедур миграции существующих баз данных (например, в ФНС или Росреестре) в распределённые форматы, что делает модернизацию крайне трудозатратной [3].

Пути решения предполагают комплексный и системный подход. Во-первых, необходимо разработать единый государственный стандарт проектирования и внедрения блокчейн-систем для нужд государственных и критических инфраструктур, включая требования к криптографическим алгоритмам, отказоустойчивости, процедурам аудита и обеспечению совместимости. Во-вторых, требуется расширение мер государственной поддержки отечественных разработчиков блокчейн-решений, включая создание песочниц, пилотных зон и механизмов сертификации, аналогичных FinTech Regulatory Sandbox в Великобритании. В-третьих, важно сформировать единый центр компетенций по безопасному блокчейн-проектированию, объединяющий усилия ВУЗов, научных институтов и государственных ИТ-платформ [4].

В рамках научной дискуссии конца 2023 – начала 2025 годов активно развиваются исследования в области гибридных блокчейн-архитектур, сочетающих свойства как публичных, так и частных сетей (permissioned-permissionless hybrid). Согласно публикациям Института проблем передачи информации РАН, подобные гибридные модели позволяют централизованно контролировать доступ к определённым уровням данных (например, в распределённых медицинских ИС), сохраняя при этом неизменяемость и прозрачность транзакций в публичной части блокчейна. Примером может служить проект «Цифровой пациент» в Самарской области, где используется гибридная модель для защиты персональных данных с применением zero-knowledge proof (ZKP) и секционирования хешей транзакций между медицинскими учреждениями.

Особое внимание в современной научной среде уделяется аспектам квантовой устойчивости блокчейн-сетей. В связи с тем, что ожидаемая практическая реализация квантовых вычислений в ближайшие 10-15 лет может поставить под угрозу стойкость используемых сегодня криптографических алгоритмов (ECDSA, RSA), в статьях МФТИ (Смирнов А.Н., 2024) предложены концепции применения постквантовых криптографических алгоритмов (например, CRYSTALS-Dilithium и Falcon) в архитектуре

российских блокчейн-решений. Это особенно актуально в контексте защиты критически важных информационных объектов, таких как системы финансового мониторинга, энергораспределительные узлы и сети доверенного взаимодействия органов власти [5].

Немаловажным аспектом научного анализа является проблематика консенсусных механизмов. Классические алгоритмы (Proof of Work, Proof of Stake) имеют ряд ограничений: энергозатратность, уязвимость к централизации узлов, сложности масштабирования. В отечественной среде всё чаще обсуждаются модификации алгоритмов Byzantine Fault Tolerance (например, Tendermint и HotStuff), которые обеспечивают высокую пропускную способность при сохранении распределённого доверия. В исследованиях Казанского федерального университета (2024) показано, что применение модифицированных BFT-алгоритмов позволяет добиться латентности ниже 100 мс при объёме сети до 30 валидаторов, что делает возможным использование блокчейна в оперативных системах управления движением транспорта и мониторинга инфраструктурных объектов [6].

Кроме того, в научной среде активно исследуются аспекты юридической валидности смарт-контрактов в российском правовом поле. Несмотря на наличие статьи 309 ГК РФ, устанавливающей принцип обязательности исполнения обязательств, не существует механизма регистрации или принудительного исполнения смарт-контрактов через суд. Исследование, проведённое в рамках проекта Института законодательства и сравнительного правоведения при Правительстве РФ (2023), выявило, что до настоящего времени ни один российский суд не рассматривал дело, в котором смарт-контракт признавался бы юридически значимым без дублирования договора в бумажной форме. Это создаёт правовой парадокс, при котором децентрализованное обязательство не может быть реализовано в централизованной юрисдикции. Решением может стать создание специального правового режима или «цифрового кодекса», регулирующего правосубъектность программного кода [7].

Анализ международного опыта (в частности, инициатив Евросоюза по внедрению eIDAS 2.0, MiCA и DLT Pilot Regime) показывает, что Россия отстаёт в плане разработки регулируемых и совместимых моделей внедрения блокчейн-решений в секторе государственных и квази-государственных услуг. Тем временем, в РФ с 2023 года действуют пилотные проекты по созданию цифрового рубля на платформе распределённого реестра под контролем ЦБ РФ, однако при этом сама архитектура

цифрового рубля остаётся закрытой, что противоречит базовому принципу открытости блокчейна. Таким образом, наблюдается дисбаланс между заявленной децентрализацией и фактическим централизованным управлением на уровне инфраструктуры и прав доступа.

Одной из наиболее актуальных задач остаётся синхронизация блокчейн-систем с действующими ГИС, такими как ЕГРН, ГИС ЖКХ, ГИС МТ и ЕГАИС. В рамках диссертационного исследования, защищённого в 2024 году в НИУ «БелГУ», был предложен метод семантической трансляции транзакций блокчейн в формат XML-сообщений, понятных для API-гейтвеев государственных платформ. Однако пока подобные наработки не получили широкого распространения в практике.

Одним из актуальных научных направлений становится управление цифровой идентичностью (Self-Sovereign Identity, SSI) в распределённых системах. Наиболее перспективной российской инициативой в этой сфере является проект «Цифровой профиль гражданина», который разрабатывается совместно Минцифры РФ и коммерческими структурами. Однако в научной литературе (например, исследования РЭУ им. Плеханова, 2024 г.) отмечается, что нынешняя архитектура цифрового профиля централизована и уязвима, поскольку управление личными данными граждан осуществляется через единый реестр. Внедрение SSI на блокчейне (например, на базе Sovrin Network или аналогичных отечественных разработок) позволило бы каждому пользователю автономно контролировать личные данные, включая их передачу третьим лицам и мониторинг доступа к ним. Научные работы последнего времени показывают, что применение блокчейн-подхода с SSI способно сократить риски утечки персональной информации более чем на 60%, а также значительно упростить процедуры идентификации и авторизации граждан при взаимодействии с госорганами и коммерческими организациями.

Важным направлением в исследованиях 2024-2025 гг. является создание эффективных механизмов межсетевого взаимодействия (кросс-чейн-технологий). Подобные подходы позволяют взаимодействовать различным блокчейн-платформам, что крайне необходимо для преодоления разобщённости и создания единого национального цифрового пространства. Среди российских разработок выделяется проект Санкт-Петербургского политехнического университета, который в 2024 году представил новый алгоритм атомарного свопа, обеспечивающий передачу цифровых активов и данных между сетями Ethereum, Hyperledger Fabric и отечественной

платформой Masterchain, с задержкой не более 30 секунд и уровнем безопасности, соответствующим ГОСТ Р 57580. Внедрение таких решений способно существенно снизить затраты на интеграцию разнородных систем и упростить взаимодействие государственных органов и бизнеса [8].

Современные исследования в области блокчейн-систем всё чаще затрагивают не только вопросы безопасности, но и экономической целесообразности сопутствующих решений. Одним из приоритетных направлений стало обеспечение конфиденциальности данных без ущерба для производительности. В работе НИЯУ МИФИ (2024) показано, что применение гомоморфного шифрования и многосторонних вычислений (MPC) позволяет безопасно обрабатывать чувствительные данные, не нарушая требований 152-ФЗ и не увеличивая существенно нагрузку на систему. Это снижает расходы на внешние системы защиты и упрощает юридическое сопровождение операций [4].

Другим значимым направлением остаётся управление рисками при внедрении блокчейн-решений. По данным РАНХиГС (2025), более двух третей организаций сталкиваются с затратами, вызванными инфраструктурными сбоями, несовместимостью решений и правовой неопределённостью. Комплексный риск-ориентированный подход с регулярными аудитами и сертификацией позволяет минимизировать эти издержки ещё на этапе проектирования, что повышает экономическую устойчивость внедрения.

Энергетическая эффективность – ещё один важный фактор. Исследования показывают, что традиционные алгоритмы консенсуса типа Proof of Work расходуют до 30% больше энергии по сравнению с централизованными ИТ-системами. Однако переход на экологичные консенсусные механизмы, такие как Proof of Authority или Proof of Elapsed Time, снижает энергозатраты в среднем на 80%. Это не только делает эксплуатацию систем дешевле, но и облегчает соответствие экологическим стандартам, что особенно важно при реализации масштабных инфраструктурных проектов [5].

Заключение

Экономическая эффективность внедрения безопасных распределённых информационных систем на базе технологии блокчейн напрямую зависит от способности этих решений снижать транзакционные и операционные издержки, устранять посредников и повышать доверие между участниками цифровых процессов.

При грамотной интеграции блокчейн способствует сокращению расходов на документооборот, автоматизацию верификации данных и оптимизацию административных процедур.

Ключевыми факторами, определяющими экономическую целесообразность внедрения, являются масштабируемость архитектуры, нормативная определённость, энергетическая эффективность и готовность инфраструктуры к интеграции. Выявлено, что отсутствие единых стандартов и сертификационных механизмов увеличивает стоимость внедрения и снижает возврат инвестиций.

Для повышения результативности применения технологии в экономически значимых секторах требуется разработка объективных методик оценки эффективности, охватывающих совокупную стоимость владения, срок окупаемости и снижение операционных рисков. Необходима институциональная поддержка в виде нормативных, кадровых и технологических решений, обеспечивающих устойчивость и предсказуемость внедрения.

Блокчейн может быть экономически оправдан только при системном подходе, который учитывает как технические параметры платформ, так и реальные потребности участников цифровой экономики. Стратегическая задача – обеспечить, чтобы вложения в распределённые информационные системы приводили к измеримому росту производительности и снижению затрат в масштабах отрасли или государства.

Список использованных источников

1. Бекиев Я. Технологии блокчейн в контексте информационной безопасности: преимущества и ограничения / Я. Бекиев, М. Одаев // Информационные технологии и телекоммуникации. 2024. № 3. С. 27-33.
2. Бескровный Р.Д. Применение технологии блокчейн в российском государственном управлении / Р.Д. Бескровный, А.К. Трифонова // Вестник экономики и права. 2023. № 11. С. 45-52.
3. Власов А.В. Распределённые информационные системы: учебник / А.В. Власов, С.П. Иванов. М.: Лань, 2020. 240 с.
4. Долженко Р.А. Институциональные барьеры использования блокчейн в трудовых отношениях / Р.А. Долженко // Лидерство и менеджмент. 2020. Т. 7, № 4. С. 585–598. DOI: 10.18334/lim.7.4.111261 EDN: LBUQYR

5. Лабазанова А.Т. Интеграция технологий блокчейн в системы кибербезопасности / А.Т. Лабазанова, А.Ш. Атабаева, Е.В. Николаева // Экономика и предпринимательство. 2023. № 11. С. 112-116.

6. Миронов П.В. Применение блокчейн-технологий для обеспечения прозрачности и безопасности в глобальных вычислительных сетях / П.В. Миронов, К.А. Сидоров // Информационные технологии. 2024. № 6. С. 87-93.

7. Петрова Н.И. Перспективы развития правового регулирования блокчейн-технологии в России / Н.И. Петрова // Молодой ученый. 2023. № 15. С. 43-46.
EDN: HGGJFW

8. Цехановский В.В. Распределённые информационные системы: учебник / В.В. Цехановский, В.Д. Чертовской. СПб.: Лань, 2020. 240 с.