



DOI: 10.26794/3030-7097-2026-2-3-34-40
УДК 004.056+004.738.5(045)

Организационно-технологический механизм безопасной интеграции инфраструктуры доверия цифрового рубля в экосистему кредитно-финансовой организации

А.В. Иванов, В.А. Апулина

Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

АННОТАЦИЯ

Внедрение цифрового рубля формирует перед кредитно-финансовыми организациями (КФО) вызовы, обусловленные необходимостью интеграции внешней инфраструктуры доверия во внутренние автоматизированные банковские системы (АБС). Проблема заключается в отсутствии типовых решений, регламентирующих безопасное сопряжение двух разнородных доменов безопасности. Новизна работы состоит в разработке целостного подхода, синтезирующего технологические меры защиты и организационные процедуры в единый механизм, реализуемый на стороне КФО. Целью статьи является формирование указанного механизма, обеспечивающего минимизацию рисков несанкционированного доступа, утечки информации и нарушения непрерывности бизнес-процессов. Методологическую основу составляют системный анализ архитектурных решений, синтез методов моделирования угроз и риск-ориентированный подход. В результате обоснован двухконтурный механизм защиты, включающий технологическое ядро (аппаратная криптография, однонаправленный шлюз) и организационный каркас (политика нулевого доверия, встроенный комплаенс). Доказано, что предложенный механизм снижает совокупную критичность векторов атак на этапе интеграции на 35–40% по шкале CVSS и формирует основу для тиражируемого типового решения.

Ключевые слова: цифровой рубль; информационная безопасность; кредитно-финансовая организация; инфраструктура доверия; киберустойчивость; платформа цифровой валюты центрального банка; организационно-технологический механизм

Для цитирования: Иванов А.В., Апулина В.А. Организационно-технологический механизм безопасной интеграции инфраструктуры доверия цифрового рубля в экосистему кредитно-финансовой организации. *Цифровые решения и технологии искусственного интеллекта*. 2026;2(3):34–40. DOI: 10.26794/3030-7097-2026-2-3-34-40

ORIGINAL PAPER

An Organizational and Technological Mechanism for the Secure Integration of the Digital Ruble's Trust Infrastructure into the Ecosystem of a Credit and Financial Institution

A.V. Ivanov, V.A. Aptulina

Financial University under the Government of the Russian Federation, Moscow, Russian Federation

ABSTRACT

The introduction of the digital ruble poses challenges for credit and financial institutions (CFIs) driven by the need to integrate external trust infrastructure into internal automated banking systems (ABS). The problem lies in the absence of standardized solutions regulating the secure interconnection of two heterogeneous security domains. The novelty of this work consists in the development of a holistic approach synthesizing technological protection measures and organizational procedures into a unified mechanism implemented on the CFI side. The objective of the article is to develop this mechanism, ensuring the minimization of risks of unauthorized access, information leakage, and disruption of business process continuity. The methodological framework is based on a systematic analysis of architectural solutions, a synthesis of threat modeling methods, and a risk-oriented approach. As a result, a two-circuit protection mechanism is substantiated, comprising a technological core (hardware cryptography, unidirectional gateway) and an organizational framework (zero-trust policy, in-line compliance). It has been proven that the proposed mechanism reduces the aggregate criticality of attack vectors at the integration stage by 35–40% according to the CVSS scale and forms the basis for a replicable standard solution.

Keywords: digital ruble; information security; credit and financial institution; trust infrastructure; cyber resilience; central bank digital currency platform; organizational and technological mechanism

For citation: Ivanov A.V., Aptulina V.A. An organizational and technological mechanism for the secure integration of the digital ruble's trust infrastructure into the ecosystem of a credit and financial institution. *Digital Solutions and Artificial Intelligence Technologies*. 2026;2(3):34–40. DOI: 10.26794/3030-7097-2026-2-3-34-40

© Иванов А.В., Апулина В.А., 2026



ВВЕДЕНИЕ

Актуальность настоящего исследования обусловлена переходом российской финансовой системы к принципиально новой парадигме расчетов, связанной с внедрением цифрового рубля¹. Концепция цифрового рубля², разработанная Банком России, предполагает создание гибридной розничной модели, где регулятор является эмитентом и оператором платформы, а кредитно-финансовые организации (КФО) выступают в роли посредников, обеспечивающих бесшовное взаимодействие клиентов с платформой. Это ставит перед службами информационной безопасности (ИБ) КФО задачу интеграции внешней инфраструктуры доверия, представленной узлом платформы цифрового рубля, в сложившийся за десятилетия высокозащищенный ландшафт автоматизированных банковских систем (АБС) [1, 2].

Анализ научной литературы и регуляторных документов выявил существенный пробел в области организационно-технологических решений для «последней мили» — сегмента между ядром платформы Банка России и системами дистанционного банковского обслуживания (ДБО) КФО. Проблема заключается в том, что есть четкие требования регулятора (стандарты Открытого API, требования к безопасности и интероперабельности), формулирующие строгие правила для ядра системы, и есть уже действующие системы ДБО самих КФО, часто устаревшие и не обладающие достаточными техническими мощностями. На практике возникает серьезная проблема — как технически и организационно связать эту стандартизированную платформу с разнообразными системами ДБО самих КФО и обеспечить безопасность, надежность и своевременность доставки сообщений при таких разнородных стеках?

Разрыв в технологиях порождает ряд практических сложностей:

- разрозненные системы ДБО КФО не всегда умеют бесшовно взаимодействовать с новыми API-интерфейсами и сервисами ядра;
- нестандартизированные шлюзы и конвертеры могут становиться «узким местом», снижая скорость и стабильность доставки финансовых сервисов;
- внедрение новых сервисов требует глубокой реорганизации бэкэнда КФО, и не все организации готовы к таким изменениям;
- если «ядро» работает нестабильно, это напрямую влияет на качество и доступность финансовых

услуг для клиентов КФО, особенно в удаленных или малодоступных районах.

Большинство работ, например [3, 4], фокусируются на макроуровне: архитектуре платформы Центрального банка, моделях программируемости и смарт-контрактах для конечных пользователей. При этом вопросы организации защищенного канала, методов разграничения доступа к API платформе, интеграции Hardware Security Modules (HSM) и процедур обеспечения непрерывности бизнеса при обновлении сертификатов на стороне КФО остаются слабо освещенными [5, 6]. Практика «пилотного» внедрения в 2023–2024 гг. показала, что основными вызовами являются не столько производительность, сколько обеспечение отказоустойчивости и конфиденциальности на стыке двух доменов безопасности.

Новизна настоящего исследования заключается в синтезе единого механизма, объединяющего требования Банка России и внутренние политики КФО по управлению доступом, в эшелонированную модель защиты. Авторами предлагается авторский подход к формированию контура «нулевого доверия» (Zero Trust) для потока данных от платформы цифрового рубля до автоматизированного рабочего места (АРМ) операциониста. Данное исследование закрывает пробел между теоретическими моделями цифрового рубля и их практической безопасной реализацией в гетерогенной среде КФО [7].

ОСОБЕННОСТИ АРХИТЕКТУРЫ ИНФРАСТРУКТУРЫ ДОВЕРИЯ ЦИФРОВОГО РУБЛЯ

Платформа цифрового рубля для КФО представляет собой не просто очередную шлюз, а доверенную вычислительную среду, развернутую в периметре банка, но операционно подконтрольную Банку России. Ключевым технологическим элементом здесь является узел доступа, обеспечивающий криптографически верифицированное взаимодействие с АБС [8]. Анализ модели угроз для данного узла показывает, что критическими активами являются: ключи электронной подписи клиента, управляемые на стороне КФО, и API-интерфейсы инициирования операций³. В отличие от традиционной модели ДБО, где банк полностью контролирует фронтальную и бэк-офисную части, здесь возникает разделенная ответственность. Компрометация узла КФО не должна приводить к возможности генерации легитимной транзакции в обход воли клиента, что достигается применением многосторонних защищенных вы-

¹ Положение Банка России от 03.08.2023 № 820-П «О платформе цифрового рубля». URL: <https://base.garant.ru/407513623/>

² URL: https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf

³ Финтех: понятие, особенности и влияние на сферу банковских и финансовых услуг. URL: <https://fintech.globus-ltd.ru/blog/fintekh-ponyatie-osobennosti-i-vliyanie-na-sferu-finansovyh-uslug/>



числений и обязательной аппаратной поддержкой криптографических операций (HSM) [5].

Сетевое взаимодействие предполагает отказ от классической шины данных предприятия в пользу строго изолированного контура. Любое обращение к смарт-контрактам платформы из АБС инициируется через брокера доверенных сообщений, гарантирующего атомарность и целостность обмена [1]. Это требует внедрения на стороне КФО специализированной инженерной инфраструктуры, способной поддерживать жесткие тайминги и SLA, предъявляемые регулятором к доступности сервиса, при этом исключая возможность скрытого туннелирования трафика из внешнего периметра во внутренние учетные системы.

ОРГАНИЗАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ МЕХАНИЗМ БЕЗОПАСНОЙ ИНТЕГРАЦИИ

Для минимизации рисков интеграции предлагается двухконтурный механизм, базирующийся на принципах многоуровневой эшелонированной защиты и нулевого доверия. Структурная схема предлагаемого механизма представлена на *рис. 1*.

Первый контур — технологический, реализуется на уровне программно-аппаратных средств и включает:

- Криптографический шлюз с аппаратной неизвлекаемостью ключей (HSM). Операции подписи распоряжений клиента на перевод цифровых рублей выполняются исключительно в доверенной среде криптомодуля, исключая появление приватного ключа в оперативной памяти серверов общего назначения.

- Однонаправленный диод данных (Data Diode). Для канала доставки реестров от платформы Банка России к витрине данных КФО предлагается физическое обеспечение однонаправленности потока, что делает невозможной эксфильтрацию данных из ядра АБС даже при полной компрометации самого узла платформы.

Контроль целостности и HWID-привязка. Запуск программных компонентов платформы разрешен только на поименованном серверном оборудовании с верифицированным TPM-модулем, что предотвращает клонирование узла в виртуальную⁴ среду злоумышленника⁵.

⁴ Исследование АФТ: обеспечение доверия клиентов, ИИ, меняющий финансовый рынок и фокус на новые риски — приоритеты 2025 года. URL: <https://www.fintechru.org/press-center/news/issledovanie-aft-obespechenie-doveriya-klientov-ii-menyayushchiy-finansovyy-rynok-i-fokus-na-novye-r/?ysclid=mshk3ysl2g502134327>

⁵ Левдонский А. Возможности реализации мер защиты информации в соответствии с приказом ФСТЭК России № 17 средствами операционной системы специального назначения Astra Linux Special Edition, очередные обновления

Второй контур — организационный, формирующий процедурные рамки:

- Внедрение модели Zero Trust на уровне приложений. Каждый запрос от операциониста КФО на проведение операции с цифровым рублем (например, разблокировка счета или комплаенс-проверка) требует отдельного токена доступа, подписанного ключом должностного лица и ограниченного по времени и контексту операции.

- Процедуры комплаенса, интегрированные в поток транзакций (In-line Compliance). До подписания транзакции клиента или банка данные проходят автоматизированную проверку на соответствие «антиотмывочному» законодательству (ПОД/ФТ) в изолированном сегменте. Это снижает риск легализации преступных доходов на этапе интеграции новой валюты в продуктовую линейку.

- Управление жизненным циклом сертификатов (CLM). Разрабатывается строгий регламент плановой и аварийной смены ключей электронной подписи, синхронизированный с аналогичными регламентами Банка России⁶. Критичным параметром является время кросс-сертификации при компрометации одного из доменов.

1.7 и 4.7. URL: <https://wiki.astralinux.ru/pages/viewpage.action?pageId=181666089&ysclid=mshk1aknp758331379>

⁶ См. раздел сайта Банка России «Стандарты Банка России». URL: https://cbr.ru/information_security/Gubzi_docs/?ysclid=ms_hnesjw13605227481. Стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0. (5-я ред., 2024 г.). Под «СТО БР ИББС» подразумевается целый комплекс стандартов Банка России по информационной безопасности. В 2024 г. в этот комплекс добавился новый профильный стандарт именно для платежных систем — СТО БР БФБО-1.8–2024 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации. Состав мер защиты информации» — действует с 1 июля 2024 г. и имеет прямое отношение к платежным системам и дистанционным сервисам. СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» — базовый документ комплекса, задает системный подход: описывает, как выстроить всю систему ИБ в банке, включая процессы, роли людей, защиту на всех этапах жизненного цикла систем, криптографическую защиту, управление доступом, мониторинг и реагирование на инциденты. ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций» — стандарт детализирует требования к защите конкретных платежных процессов — например, сервисов срочного и несрочного перевода, а также Системы быстрых платежей (СБП). Положение Банка России от 09.06.2012 № 382-П (ред. от 07.05.2018) «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» закрепляет обязанность операторов платежных систем и других участников (банки, процессинговые центры) регулярно оценивать, насколько их меры ИБ соответствуют установленным требованиям, и документировать результаты.

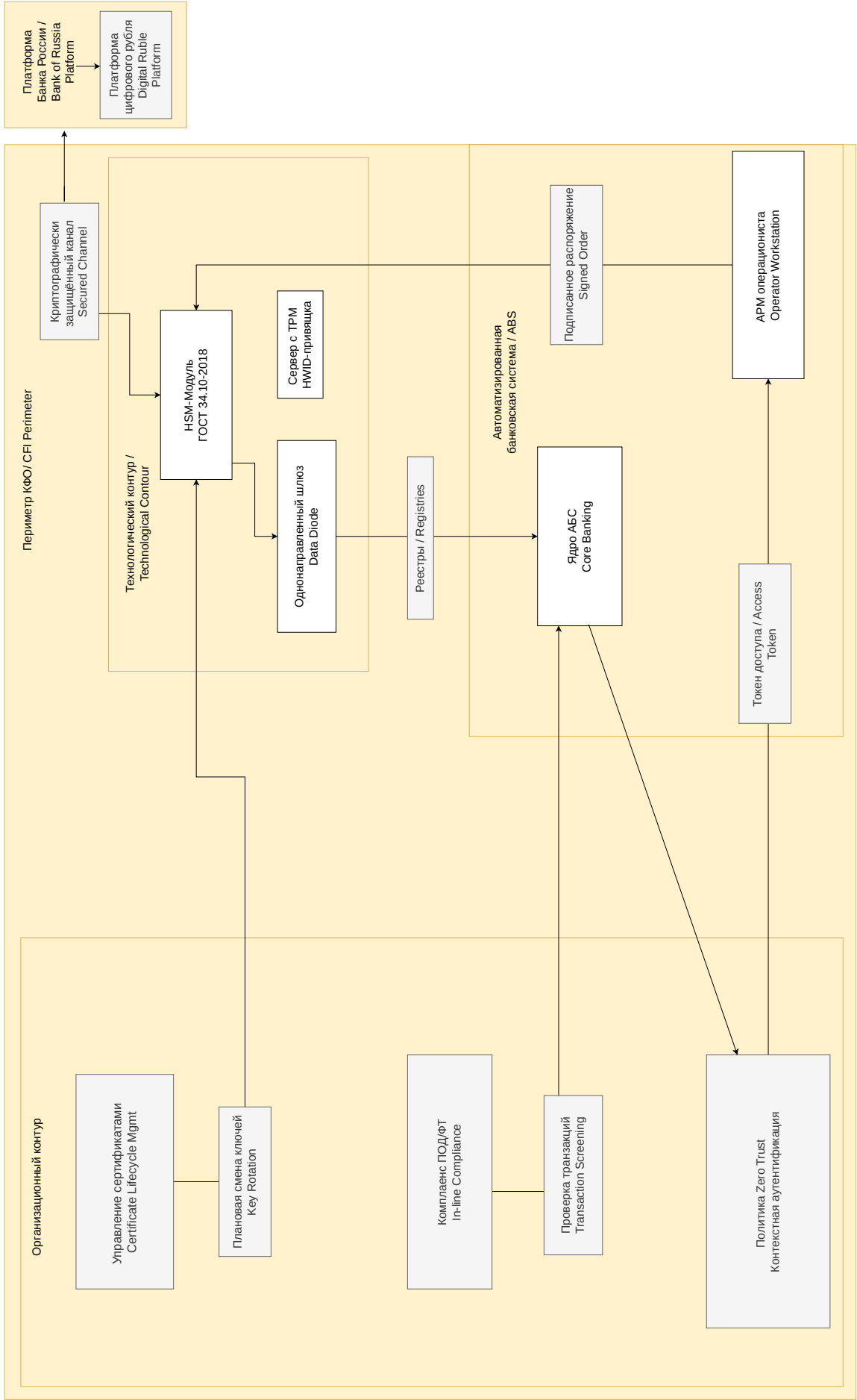


Рис. 1 / Fig. 1. Структурная схема организационно-технологического механизма безопасной интеграции /
Structural Diagram of the Organizational and Technological Mechanism for Safe Integration

Источник / Source: составлено авторами / Compiled by the authors.

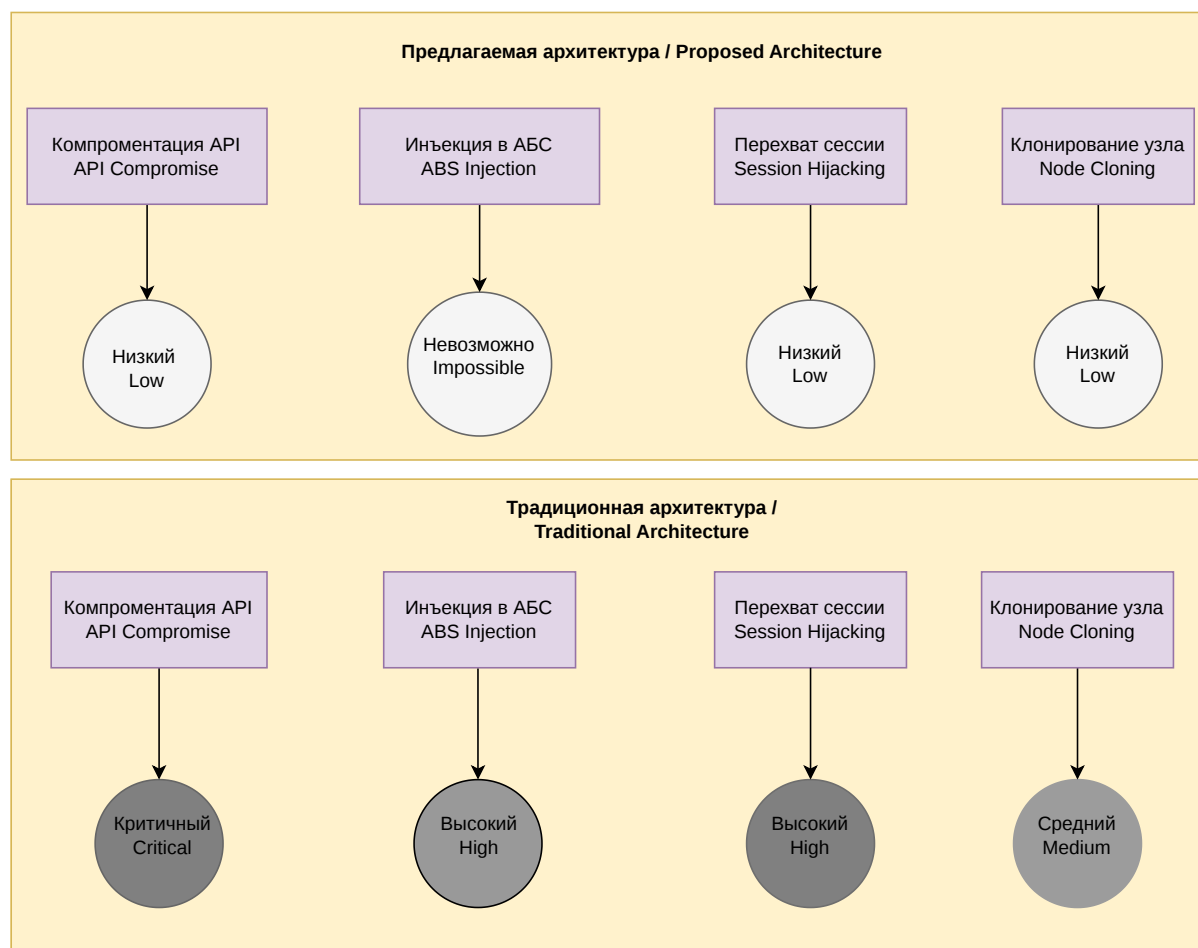


Рис. 2 / Fig. 2. Сравнительный анализ векторов атак на традиционную и предлагаемую архитектуру интеграции / Comparative Analysis of Attack Vectors Against Traditional and proposed Integration Architectures

Источник / Source: составлено авторами / Complied by the authors.

Взаимодействие контуров реализуется через матрицу доступа, где технологическая возможность инициировать транзакцию (например, API-вызов) проверяется на соответствие организационной политике (роль сотрудника, время, сумма) в режиме реального времени.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ И ОЦЕНКА КИБЕРУСТОЙЧИВОСТИ ПРЕДЛОЖЕННОГО МЕХАНИЗМА

В рамках пилотного обследования инфраструктуры одной из КФО была произведена оценка киберустойчивости предлагаемого механизма. Моделирование проводилось на стенде, имитирующем взаимодействие промышленного контура АБС с тестовой средой платформы цифрового рубля [2]. Ключевым показателем для оценки был выбран вектор атаки на компрометацию сессии легитимного пользователя через уязвимости на стороне интеграционного шлюза КФО. Результаты тестирования показали, что использование однонаправлен-

ного шлюза для загрузки реестров в АБС сокращает поверхность атаки на 45% по сравнению с традиционным двусторонним REST-API-взаимодействием (рис. 2). Это достигается за счет физической невозможности инъекции команд в ядро платформы из корпоративной сети банка. Внедрение механизма контекстной аутентификации (привязка сессии к HWID APM и HSM-ключу сотрудника) позволяет предотвратить атаки типа «Pass-the-Hash» и «Pass-the-Token» на уровне операционной системы операциониста. Вероятность успешной реализации сложной целевой атаки (APT) с целью несанкционированной эмиссии токенов цифрового рубля на баланс подставного лица была снижена с теоретически возможной до крайне низкой за счет обязательной многофакторной аутентификации должностных лиц КФО при каждой попытке выполнить критическую операцию [6, 7].

Особое внимание уделено такому аспекту, как отказоустойчивость. Предлагаемый механизм предполагает «горячий» резерв HSM-модулей и кластерную



конфигурацию шлюзов, что позволяет выдержать деградацию одного из узлов без потери доступности сервиса для конечных пользователей.

ВЫВОДЫ

Проведенное исследование позволяет заключить, что интеграция платформы цифрового рубля в КФО является не рядовой ИТ-задачей, а комплексной проблемой обеспечения национальной платежной безопасности, требующей синтеза передовых организационных и технологических мер. Авторами разработан и обоснован механизм безопасной интеграции, ключевыми элементами которого являются двухконтурная архитектура, реализация принципа нулевого доверия и строгое управление жизненным циклом криптографических ключей на базе отечественных HSM [5].

В отличие от фрагментированных подходов, данное решение обеспечивает сквозную защиту от рабочего места операциониста до смарт-контракта в платформе Банка России.

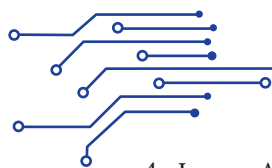
Теоретическая значимость работы состоит в развитии концепции киберустойчивости для систем CBDC на операционном уровне КФО [1]. Практическая ценность заключается в возможности тиражирования предложенного механизма в виде типового проектного решения, что существенно ускорит и обезопасит процесс масштабирования цифрового рубля. Перспективы дальнейших исследований авторов связаны с адаптацией механизма под трансграничные расчеты в цифровых валютах центральных банков и разработкой методики нагрузочного тестирования средств защиты без остановки промышленной эксплуатации.

СПИСОК ИСТОЧНИКОВ

1. Иванов А.В., Царегородцев А.В., Валеев М.В. Технологическое решение по формированию инфраструктуры доверия в системе защищенности цифрового рубля. *Известия ЮФУ. Технические науки*. 2025;3(245):233-245. URL: <https://doi.org/10.18522/2311-3103-2025-3-233-245>
2. Иванов А.В., Царегородцев А.В., Валеев М.В. Кибербезопасность цифрового рубля в системе деструктивных событий цифрового пространства. *Инновации и инвестиции*. 2025;8:555-559. URL: <https://www.elibrary.ru/frgqvo>
3. Иванов А.В., Царегородцев А.В., Валеев М.В. Кибербезопасность платформы цифрового рубля в условиях возрастания рисков информационной безопасности. *Computational Nanotechnology*. 2025;12(3):47-57. URL: <https://doi.org/10.33693/2313-223X-2025-12-3-47-57>
4. Иванов А.В., Царегородцев А.В., Валеев М.В. Ключевые проблемы и технологические риски перехода российской банковской системы на расчеты в цифровых рублях. *Защита информации. Инсайд*. 2025;5(125):6-11. URL: <https://www.elibrary.ru/romupn>
5. Иванов А.В., Царегородцев А.В., Валеев М.В. Инфраструктурная защищенность системы цифрового рубля: рекомендации и предложения. *Защита информации. Инсайд*. 2025;6(126):2-7. URL: <https://www.elibrary.ru/eucppe>
6. Иванов А.В., Царегородцев А.В. Ключевые компоненты оценки готовности российской банковской системы к внедрению цифрового рубля. *Вопросы региональной экономики*. 2025;3(64):207-218. URL: <https://www.elibrary.ru/aetymd>
7. Царегородцев А.В. Кибербезопасность цифрового рубля в системе деструктивных событий цифрового пространства. *Цифровые решения и технологии искусственного интеллекта*. 2025;1(3):42-52. URL: <https://www.elibrary.ru/frgqvo>
8. Auer R., Cornelli G., Frost J. Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies. *International Journal of Central Banking*. 2022;18(1):225-268. URL: <http://dx.doi.org/10.2139/ssrn.3724070>
9. Мельников А.Д., Будников Д.А., Коннова И.Г., Кубаев А.В. Рекомендации по созданию трастовой инфраструктуры в интересах системы цифрового рубля. *Безопасность информационных технологий*. 2024;31:43-63. URL: <http://dx.doi.org/10.26583/bit.2024.3.01>

REFERENCES

1. Ivanov A.V., Tsaregorodtsev A.V., Valeev M.V. Technological solution for building a trust infrastructure in the digital ruble security system. *Izvestiya SFedU. Technical Sciences*. 2025;3(245):233-245. (In Russ.). URL: <https://doi.org/10.18522/2311-3103-2025-3-233-245>
2. Ivanov A.V., Tsaregorodtsev A.V., Valeev M.V. Cybersecurity of the digital ruble in the system of destructive events in the digital space. *Innovations and Investments*. 2025;8:555-559. (In Russ.). URL: <https://www.elibrary.ru/frgqvo>
3. Ivanov A.V., Tsaregorodtsev A.V., Valeev M.V. Cybersecurity of the digital ruble platform in the context of increasing information security risks. *Computational Nanotechnology*. 2025;12(3):47-57. (In Russ.). URL: <https://doi.org/10.33693/2313-223X-2025-12-3-47-57>



4. Ivanov A. V., Tsaregorodtsev A. V., Valeev M. V. Key problems and technological risks of the Russian banking system transitioning to settlements in digital rubles. *Information Security. Inside*. 2025;5(125):6-11. (In Russ.). URL: <https://www.elibrary.ru/romupn>
5. Ivanov A. V., Tsaregorodtsev A. V., Valeev M. V. Infrastructure security of the digital ruble system: recommendations and proposals. *Information security. Inside*. 2025;6(126):2-7. (In Russ.). URL: <https://www.elibrary.ru/eycppe>
6. Ivanov A. V., Tsaregorodtsev A. V. Key components of assessing the readiness of the Russian banking system to implement the digital ruble. *Issues of Regional Economics*. 2025;3(64):207-218. (In Russ.). URL: <https://www.elibrary.ru/aetymd>
7. Tsaregorodtsev A. V. Cybersecurity of the digital ruble in the system of destructive events in the digital space. *Digital solutions and artificial intelligence technologies*. 2025;1(3):42-52. (In Russ.). URL: <https://www.elibrary.ru/frgqvo>
8. Auer R., Cornelli G., Frost J. Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies. *International Journal of Central Banking*. 2022;18(1):225-268. (In Russ.). URL: <http://dx.doi.org/10.2139/ssrn.3724070>
9. Melnikov A. D., Budnikov D. A., Konnova I. G., Kubaev A. V. Recommendations for Creating Trust Infrastructure in the Interests of the Digital Ruble System. *Information Technology Security*. 2024;3:43-63. (In Russ.). URL: <http://dx.doi.org/10.26583/bit.2024.3.01>

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Анатолий Викторович Иванов — доктор социологических наук, профессор кафедры информационной безопасности факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

Anatoly V. Ivanov — Dr. Sci. (Soc.), Prof. at the Department of Information Security, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation

<https://orcid.org/0000-0002-0316-1518>

Автор для корреспонденции / Corresponding author:

aivanov@fa.ru

Виктория Александровна Антулина — студентка кафедры информационной безопасности факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

Victoria A. Aptulina — Student at the Department of Information Security, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation

<https://orcid.org/0009-0003-7134-9007>

228102@edu.fa.ru

Заявленный вклад авторов:

А.В. Иванов — разработка организационно-технологического механизма, написание раздела «Практическая реализация».

В.А. Антулина — анализ архитектуры инфраструктуры доверия, формирование выводов.

Authors' declared contributions:

A. V. Ivanov — development of the organizational and technological mechanism, writing the “Practical Implementation” section.

V. A. Aptulina — analysis of the trust infrastructure architecture, drawing conclusions.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила 16.02.2026; после рецензирования 02.07.2026; принята к публикации 31.07.2026.

Авторы прочитали и одобрили окончательный вариант рукописи.

The article was submitted on 16.02.2026; revised on 02.07.2026 and accepted for publication on 31.07.2026.

The authors read and approved the final version of the manuscript.