УДК 004.056:336.711

БЕЗОПАСНОСТЬ ЦИФРОВОГО РУБЛЯ: ОБЗОР РИСКОВ И МЕР ЗАЩИТЫ

В.А. Никольская[1], Г.В. Кошкина[1], К.Э. Никитина-Кошкина[2]
[1]Тверской государственный технический университет, г. Тверь
[2]Территориальный орган Федеральной службы государственной статистики по Тверской области, г. Тверь

DOI: 10.46573/2409-1391-2026-1-69-74

Аннотация. *Настоящая статья представляет собой комплексный анализ безопасности цифрового рубля (ЦР), охватывающий правовые, технологические, кибернетические, социальные и экономические аспекты. Рассмотрены правовые основы на базе Федеральных законов № 152-ФЗ и № 340-ФЗ, архитектура технической защиты с использованием отечественного программного обеспечения, криптографии и специализированных модулей, а также ключевые угрозы – от фишинга и мошенничества до системных рисков, связанных с централизацией и потенциальным вмешательством государства. Особое внимание уделено антифрод-механизмам, включая тройную аутентификацию и гарантии возмещения убытков, а также критически важному социальному компоненту – уровню доверия населения, который остается низким из-за дезинформации и опасений по поводу финансового контроля. Проанализированы экономические последствия внедрения ЦР для банковского сектора и его роль как инструмента финансового суверенитета в условиях международных санкций. Сделан вывод, что устойчивое и успешное внедрение ЦР возможно только при условии баланса между технологической надежностью, правовой прозрачностью, экономической устойчивостью и общественным доверием.*

Ключевые слова: *цифровой рубль, безопасность, правовая регуляция, финансовый суверенитет, кибербезопасность, антифрод-механизм, социальные уязвимости.*

За последние годы в России, как и в других странах, выросла доля безналичных расчетов, что потребовало развития и совершенствования цифровых платежных инструментов. Результатом разработок стало внедрение на платформе Центрального банка (ЦБ) цифровой валюты, по сути являющейся новой формой денег. Цифровой рубль (ЦР) представляет собой технологически сложную и социально значимую инновацию. Его внедрение ставит перед регулятором задачу обеспечения не только технической защищенности, но и правовой легитимности, экономической устойчивости и общественного доверия. В данной статье представлен комплексный обзор ключевых аспектов безопасности ЦР: правовой и технической инфраструктуры, киберугроз, антифрод-механизмов, социального восприятия и системных экономических рисков.

1. Правовая и техническая основа безопасности.

Безопасность ЦР строится на двух взаимосвязанных компонентах: национальной правовой базе и отечественной технологической инфраструктуре.

Правовую основу составляет в первую очередь Федеральный закон № 152-ФЗ «О персональных данных», дополненный Федеральным законом № 340-ФЗ «О цифровом рубле» (2023 год) [13]. Последний наделяет Банк России полномочиями по обработке персональных данных пользователей ЦР в целях надежного функционирования платформы [13]. Требования закона № 152-ФЗ включают обязательную локализацию данных граждан РФ на территории страны, необходимость получения информированного согласия на их обработку и право субъекта на отзыв этого согласия [10, 12]. Особые меры защиты применяются к биометрическим и иным («специальным») категориям данных [12].

На техническом уровне безопасность обеспечивается:

использованием отечественного оборудования и программного обеспечения, включенного в официальные реестры [6];

шифрованием всех каналов связи с применением сертифицированных ФСБ средств криптографической защиты информации [6, 7, 16];

двухсторонней аутентификацией банков через собственный центр сертификации Банка России [6, 7];

специализированным программным модулем (BR Software Module), интегрируемым в мобильные приложения банков для изолированного хранения криптографических ключей [6, 7];

применением логического, структурного, дублирующего и авторского контроля для обеспечения целостности данных и смарт-контрактов.

Данная архитектура создает многоуровневую защиту, ориентированную на соответствие национальным стандартам и минимизацию зависимости от зарубежных технологий.

2. Киберугрозы и специфические риски.

Несмотря на продвинутую защиту, ЦР подвержен ряду угроз, которые условно делятся на внешние и системные. Внешние угрозы в первую очередь касаются конечных пользователей. Уже на этапе подготовки к внедрению ЦР активизировались мошенники, использующие фишинг, фейковые инвестиционные программы, спам и телефонные скамы, эксплуатирующие дезинформацию и страх граждан перед «обязательным переходом» на ЦР. Опрос Mar Consult в октябре 2025 года показал, что 31 % респондентов почти ничего не знают о ЦР, и это создает благоприятную среду для мошенничества.

Риски для коммерческих банков также значительны. Поскольку доля безналичных расчетов перейдет к ЦР, у банков будет оставаться меньше средств для свободного использования. Нововведение приведет к оттоку средств и, соответственно, снижению доходов, не исключены и репутационные потери в случае компрометации кошельков, даже при отсутствии прямой вины банков.

Системные риски, связанные с архитектурой ЦР:

централизация внедрения: компрометация или сбой платформы Банка России может парализовать систему электронных платежей;

гипотетическое вмешательство государства: распространены опасения, что ЦБ может «аннулировать» неиспользуемые ЦР или заблокировать кошельки, а это подрывает доверие к ЦР как форме собственности. Главной целью ЦР 47 % россиян считают государственный контроль над финансами;

офлайн-транзакции: отсутствие реального времени мониторинга усложняет борьбу с мошенничеством, а утрата устройства может привести к безвозвратной потере доступа к средствам;

низкая технологическая зрелость части банков: до 30 % кредитных организаций имеют устаревшие IT-системы, что затрудняет интеграцию и создает риски для всей экосистемы [3, 11].

3. Антифрод-системы и механизмы защиты.

В ответ на угрозы Банк России внедряет комплекс мер:

многоуровневую защиту («тройной барьер»): доступ к средствам требует прохождения трех уровней аутентификации – в банке, на платформе ЦБ и при дополнительной проверке со стороны регулятора [1, 2, 4, 9, 14];

гарантию сохранности средств: Банк России официально заявляет, что возместит убытки пользователям в случае хищения средств; это создает большой стимул для обеспечения максимальной безопасности [2, 4, 9, 14];

период охлаждения: с февраля 2025 года банки могут замораживать подозрительные транзакции на 48 ч для подтверждения пользователем, что снижает риски социальной инженерии [5];

процедуры реагирования: в случае утечки данных Банк России обязан уведомить Роскомнадзор в течение 24 ч и направить отчет в течение 72 ч.

Указанные меры эффективны против внешних атак, но не устраняют системных рисков, связанных с централизацией и доверием к государству.

4. Социальный компонент безопасности: доверие и недоверие.

Техническая безопасность ЦР не гарантирует его социального принятия. Опрос Mar Consult (2025 год) выявил следующее:

только 36 % россиян доверяют системе безопасности ЦР;

46 % имеют серьезные опасения, главными причинами которых являются хакерские атаки (39 %), технические сбои (43 %) и вмешательство государства (38 %);

47 % считают, что ЦР создан для контроля над финансами, а не для удобства граждан.

Дезинформация (например, об обязательном переходе на ЦР или возможном их «сгорании» при неполном использовании) активно распространяется в Сети, и Банк России вынужден регулярно ее опровергать [8, 15]. Это свидетельствует о глубоком разрыве между официальной риторикой и общественным восприятием.

Успех внедрения и использования ЦР зависит не столько от криптографии, сколько от способности регулятора завоевать доверие через прозрачность своих действий, просвещение граждан и уважение их финансовой автономии.

5. Экономические и системные вызовы.

Внедрение ЦР создает ряд дополнительных проблем в банковской системе, а именно:

1. Конкуренцию с коммерческими банками: ЦР может привлечь депозиты населения, снижая ликвидность и кредитоспособность банков. Руководство «Сбербанка» и других крупных игроков выражает скептицизм относительно выгод от ЦР.

2. Сопротивление банков: банки могут медлить с внедрением или предлагать менее качественные услуги, что замедлит распространение ЦР [3, 11, 16].

3. Технологический разрыв: интеграция с устаревшими банковскими системами требует времени и ресурсов, что создает риски неравенства в доступе к услугам.

4. Необеспеченность населения ресурсами: отсутствие у населения (или пользователей) стабильного интернета, возможности доступа к платформе ЦБ, алгоритма использования в розничной торговле.

Одновременно ЦР рассматривается как инструмент финансового суверенитета. Он может стать альтернативой SWIFT, позволив России проводить международные расчеты вне западных финансовых систем, особенно в условиях санкций. Эта геополитическая функция может перевесить экономические риски, ускоряя внедрение ЦР даже ценой давления на банковский сектор.

Стоит отметить, что указанные риски не позволяют ЦБ официально признать ЦР дополнительной валютой, как планировалось изначально, а потому в начале 2026 года апробация продолжится только в рамках пилотного проекта.

Цифровой рубль – это проект с высоким уровнем технической и правовой защищенности, но с глубокими системными и социальными уязвимостями. Его безопасность не сводится к киберрезистентности: она определяется балансом между контролем и доверием, суверенитетом и свободой, инновацией и стабильностью.

Ключевые проблемы, требующие решения:

1. Выбор архитектуры: определиться с тем, сохранить ли двухуровневую модель (ЦБ + банки) или перейти к прямому взаимодействию с пользователями.

2. Управление доверием: преодолеть дезинформацию и страх через прозрачность и образование.

3. Гармонизация интересов: сбалансировать геополитические цели с поддержкой здоровой банковской конкуренции.

Цифровой рубль способен стать мощным инструментом модернизации финансовой системы, но его успех зависит не от технологий, а от способности государства создать экосистему, в которой граждане, бизнес и банки увидят не угрозу от его использования, а выгоду. Без этого даже самая безопасная цифровая валюта рискует остаться никем не востребованной.

Библиографический список

1. В ЦБ не ожидают массового перехода россиян на цифровой рубль. URL: https://www.kommersant.ru/doc/8212466 (дата обращения: 20.11.2025).
2. В Центробанке ответили на главные вопросы россиян о цифровом рубле. URL: https://rg.ru/2025/12/21/na-lichnyj-raschet.html (дата обращения: 17.12.2025).
3. Герман Греф: Цифровой рубль мне не нужен ни как физлицу, ни как главе банка. URL: https://www.cnews.ru/news/top/2025-07-03_glava_sberbanka_ne_verit (дата обращения: 25.10.2025).
4. Зачем нужен цифровой рубль, станет ли он обязательным и что нам даст единый куар-код. Интервью заместителя председателя ЦБ Зульфии Кахрумановой KP.RU. URL: https://www.kp.ru/daily/27699/5087872/ (дата обращения: 25.10.2025).
5. Информация Банка России о введении «периода охлаждения». URL: https://www.consultant.ru/document/cons_doc_LAW_498420/ (дата обращения: 20.11.2025).
6. Информация Банка России о технической архитектуре цифрового рубля. URL: https://cbr.ru/fintech/dr/ (дата обращения: 25.10.2025).
7. Материалы по архитектуре и безопасности платформы ЦР (Банк России, 2023–2025). URL: https://cbr.ru/information_security/ (дата обращения: 25.10.2025).
8. Платежом опасен: в РФ появились первые мошенничества с цифровым рублем. URL: https://iz.ru/1839276/anton-belyi-natala-ilina/platezom-opasen-v-rf-poavilis-pervye-mosennicestva-s-cifrovym-rublem (дата обращения: 20.11.2025).
9. Пресс-конференция председателя Комитета по финансовому рынку Госдумы РФ Анатолия Аксакова 16.10.23. URL: https://pressria.ru/20231016/955585743.html (дата обращения: 25.10.2025).

10. Об обработке персональных данных в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 15.12.2022 № 201. URL: https://www.garant.ru/products/ipo/prime/doc/406813536/ (дата обращения: 25.10.2025).
11. Только бумажный. Россиянам оказался не нужен цифровой рубль. URL: https://banks.cnews.ru/news/top/2025-07-17_tolko_bumazhnyj_ili_virtualnyj (дата обращения: 20.11.2025).
12. О персональных данных: Федер. закон от 27.07.2006 № 152-ФЗ. URL: https://www.consultant.ru /document/cons_doc_LAW_61801/ (дата обращения: 25.10.2025).
13. О цифровом рубле: Федер. закон от 24.07.2023 № 340-ФЗ. URL: https://www.garant.ru/hotlaw/federal/1637250/ (дата обращения: 25.10.2025).
14. ЦБ рассказал о возмещении клиентам банков украденных средств. URL: https://pravo.ru/news/251258/ (дата обращения: 20.11.2025).
15. Центробанк обнаружил кампанию по распространению мифов о цифровом рубле. URL: https://www.anti-malware.ru/news/2025-02-04-121598/45180 (дата обращения: 25.10.2025).
16. Цифровой рубль: что он изменит в экономике и зачем это инвестору. URL: https://bcs-express.ru/novosti-i-analitika/tsifrovoi-rubl-chto-on-izmenit-v-ekonomike-i-zachem-eto-investoru (дата обращения: 20.11.2025).

THE SECURITY OF THE DIGITAL RUBLE: OVERVIEW OF RISKS AND PROTECTION MEASURES

V.A. Nikolskaya[1], G.V. Koshkina[1], K.E. Nikitina-Koshkina[2]
[1]Tver State Technical University, Tver
[2] Territorial Office of the Federal State Statistics Service for the Tver Region, Tver

Abstract. *This article presents a comprehensive analysis of the security of the digital ruble (DR), covering its legal, technological, cyber, social, and economic dimensions. It examines the legal framework based on Federal Laws No. 152-FZ and No. 340-FZ, the technical security architecture employing domestically developed software, cryptographic solutions, and specialized modules, as well as key threats ranging from phishing and fraud to systemic risks associated with centralization and potential state intervention. Particular attention is given to anti-fraud mechanisms – including triple-factor authentication and guarantees for loss compensation – as well as to the critically important social component: public trust, which remains low due to misinformation and concerns about financial surveillance. The paper also analyzes the economic implications of the DR for the banking sector and its potential role as an instrument of financial sovereignty under international sanctions. The study concludes that the sustainable and successful adoption of the digital ruble is feasible only if a balance is achieved among technological reliability, legal transparency, economic stability, and public trust.*

Keywords: *digital ruble, security, legal regulation, financial sovereignty, cybersecurity, anti-fraud mechanisms, social vulnerabilities.*

Об авторах:

НИКОЛЬСКАЯ Вера Александровна – кандидат технических наук, доцент кафедры экономики и управления производством, Тверской государственный технический университет, г. Тверь, Россия; e-mail: nbvas@mail.ru

КОШКИНА Галина Вячеславовна – старший преподаватель кафедры информатики и прикладной математики, Тверской государственный технический университет, г. Тверь, Россия; e-mail: gkoshkina@rambler.ru

НИКИТИНА-КОШКИНА Кристина Эдуардовна – ведущий специалист-эксперт отдела информационных ресурсов и технологий, Территориальный орган Федеральной службы государственной статистики по Тверской области, г. Тверь, Россия; e-mail: kris22t@rambler.ru

About the authors:

NIKOLSKAYA Vera Aleksandrovna – Candidate of Technical Sciences, Associate Professor of the Department of Economics and Production Management, Tver State Technical University, Tver, Russia; e-mail: nbvas@mail.ru

KOSHKINA Galina Vyacheslavovna – Senior Lecturer at the Department of Informatics and Applied Mathematics, Tver State Technical University, Tver, Russia; e-mail: gkoshkina@rambler.ru

NIKITINA-KOSHKINA Kristina Eduardovna – Leading Specialist-Expert of the Department of Information Resources and Technologies, Territorial Office of the Federal State Statistics Service for the Tver Region, Tver, Russia; e-mail: kris22t@rambler.ru