аУДК 336.741:004.738.5
DOI: 10.34020/1993-4386-2025-4-76-84

ВЛИЯНИЕ ВНЕДРЕНИЯ ЦИФРОВОГО РУБЛЯ НА ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Е. Н. Димитриева
Сибирский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Новосибирск, Россия
А. Я. Верятина, А. Е. Петровская
ООО «Сорцум», Новосибирск, Россия

Аннотация. В статье проанализировано влияние внедрения цифрового рубля на обеспечение экономической безопасности государства. В работе рассматривается сущность цифрового рубля, нормативно-правовая база, регулирующая его обращение, и текущее состояние пилотного проекта. Особое внимание уделяется выявлению ключевых угроз при внедрении цифровой валюты, которые приводят к экономическим потерям, и предложению решений по защите данных государственных учреждений. Сделан вывод о необходимости достижения баланса между технологическими инновациями и обеспечением экономической безопасности для успешной интеграции цифрового рубля в финансовую систему страны.

Ключевые слова: цифровой рубль, экономическая безопасность, цифровизация, угрозы экономической безопасности государства, финансовая система, пилотный проект.

Для цитирования: Димитриева Е. Н., Верятина А. Я., Петровская А. Е. Влияние внедрения цифрового рубля на обеспечение экономической безопасности Российской Федерации в условиях цифровизации // Сибирская финансовая школа. 2025. № 4 (160). С. 76-84. DOI: 10.34020/1993-4386-2025-4-76-84.

За последние 50 лет социум испытал на себе последствия цифровой эволюции, знакомился с нововведениями в IT-сфере, учился пользоваться компьютерной техникой, создавал информационные новшества, благодаря чему появились новые специальности, повысилось качество товаров, работ и услуг. На фоне вышеназванных изменений внедрение цифровых валют, как одного из элементов процесса цифровизации, представляет собой значительный шаг вперед в развитии финансовых технологий. Однако, несмотря на потенциальные преимущества, цифровые валюты повышают уязвимость финансовой системы Российской Федерации к кибератакам, что может привести к масштабным экономическим потерям. Актуальность темы обусловлена растущей зависимостью национальной экономики от цифровых технологий на фоне санкционного давления и дефицита кадров в IT-сфере, поэтому идет активное развитие цифровой валюты Российской Федерации (цифрового рубля), что является следствием цифровизации денежной системы.

По словам Д. Мельмонта, «под цифровизацией понимается процесс перехода на цифровые технологии, распространяющийся на все сферы жизни общества» [1, с. 1217]. На основе цифровизации происходит формирование большинства общественных процессов, что является залогом высокого уровня успеха в жизнедеятельности социума; также осуществляется полномасштабное внедрение информационных новшеств в деятельность государственных структуры и различного рода организаций [2, с. 111]. С 2025 года в России этот процесс реализуется через национальный проект «Экономика данных и цифровая трансформация государства», бюджет которого превышает одного триллиона рублей. Национальный проект нацелен на формирование в России современной и безопасной цифровой среды, охватывающей как государственный сектор, так экономику и социальную жизнь граждан. Для этого создается комплексная инфраструктура, гарантирующая кибербезопасность, обеспечивается стабильный интернет и приток профессиональных кадров в ИТ-отрасль. Фунда-

ментом этой масштабной перестройки становится повсеместное внедрение культуры принятия решений, опирающихся на анализ данных. Именно этот подход позволит вывести на принципиально новый уровень организацию логистических маршрутов, возможности удаленного здравоохранения, эффективность онлайн-обучения и удобство получения государственных услуг. Важнейшим элементом стратегии является развитие национальных цифровых продуктов – от платформ и специального программного обеспечения (ПО) до передовых разработок в области искусственного интеллекта[1].

Процесс цифровизации оказывает многогранное влияние на экономику и общество, потому что благодаря широкому внедрению цифровых (искусственный интеллект, криптовалюта и др.) и финансовых технологий (цифровая валюта, цифровые финансовые активы), формируется новая среда экономического взаимодействия, где традиционные границы стираются, и возникает необходимость разработки новых моделей регулирования и контроля. По словам Леонида Сергеева, «цифровая валюта представляет собой денежные средства, не имеющие материального воплощения, которые могут использоваться как полноценный денежный знак» [3, с. 76]. В России цифровая валюта регламентируется Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», в котором закреплены понятия, связанные с цифровой валютой, и правила её оборота[2].

Одной из наиболее значимых инициатив является создание Банком России в 2021 году цифровой валюты под названием «цифровой рубль», проекта, направленного на повышение удобства расчетов и прозрачности операций. Внедрение цифрового рубля открывает новую страницу в истории денежной системы Российской Федерации. Вначале основное внимание было сосредоточено на анализе правовых аспектов и обсуждении необходимости создания новой формы денег. Особое значение придавалось оценке потенциального воздействия цифровой валюты на финансовую систему страны, а также на распределение ликвидных активов между цифровым рублем и традиционными формами денежных средств [4, с. 158].

Для нашей страны цифровой рубль будет являться третьей формой национальной валюты, он будет существовать только в электронном виде, в виде цифрового кода. Переводы средств между пользователями осуществляются путем передачи этого цифрового кода с одного кошелька на другой. Это нововведение обеспечивает прямой доступ экономических агентов к обязательствам Центрального банка, что является важным шагом в развитии финансовой системы [5, с. 549]. Цифровой рубль, как цифровая валюта Банка России, призван обеспечить безопасность, эффективность и доступность платежей, а также снизить зависимость от внешних платежных систем, что регламентируется Положением Банка России «О платформе цифрового рубля» от 3 августа 2023 г. № 820-П[3].

Как указано в Основных направлениях развития национальной платежной системы на период 2025-2027 годов, в целях обеспечения информационной безопасности, операционной надежности и киберустойчивости платформы цифрового рубля «Банком России совместно с ФСБ России и Роскомнадзором разработаны необходимые технологические решения для обеспечения безопасного доступа пользователей к платформе. Пользователям платформы цифрового рубля с сентября 2024 г. стали доступны не только открытие, закрытие и пополнение счетов, переводы между гражданами, оплата товаров и услуг, совершение автоплатежей с использованием смарт-контрактов, но и оплата по динамическому QR-коду, а также переводы цифровых рублей между юридическими лицами»[4].

С 1 сентября 2026 года ожидается начало массового внедрения в финансовую систему Российской Федерации цифрового рубля в качестве третьей формы денег в соответствии с Федеральным Законом от 23 июля 2025 г. № 248-ФЗ[5]. Ключевым фактором, который препятствует внедрению цифрового рубля, является неготовность как Банка России, так и кредитных организаций к реализации этой инициативы с технической и организационной точек зрения. Еще одним фактором, влияющим на процесс, является медленное развитие пилотного проекта цифрового рубля: Банк России с 1 сентября 2024 года, как уже было отмечено, расширил масштаб тестирования технологии, включив в него реальных клиентов. На начальном этапе в эксперименте участвовали 12 банков, 600 физических лиц и 22 юридические лица. Регулятор ожидал, что число физических лиц после расширения пилота вырастет до 9 тыс. человек, а число компаний – до 1,2 тыс. Однако спустя полгода участниками пилота являются лишь 1,7 тыс. граждан и около 30 компаний, а также 15 банков [6, с. 12].

[1] Экономика данных и цифровая трансформация государств: Национальный проект / Правительство Российской Федерации: [официальный сайт]. – 25 с. – URL: http://government.ru/rugovclassifier/923/about/ (дата обращения: 08.12.2025).

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 г. № 259-ФЗ (в ред. от 15.12.2025 № 466-ФЗ).

[3] О платформе цифрового рубля: Положение Банка России от 03 августа 2023 г. № 820-П (действует с изм. и доп., вступ. в силу с 01.01.2025 г.).

[4] Основные направления развития национальной платежной системы на период 2025-2027 годов. URL: https://cbr.ru/Content/Document/File/170680/onrnps_2025-27.pdf, с. 12.

[5] О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 23 июля 2025 г. № 248-ФЗ.

Что касается конкретного прироста, то за отчетный период число банков-участников увеличилось на три единицы (с 12 до 15), что составляет рост на 25 %. Эта положительная динамика указывает на устойчивый институциональный интерес и планомерное наращивание технологических мощностей (см. рис. 1).

Количество граждан, вовлеченных в тестирование, возросло на 1 100 человек – с 600 до 1 700, что в относительном выражении представляет собой значительный рост на 183 %. Однако, несмотря на эту высокую относительную величину, абсолютное число остается крайне низким на фоне запланированных 9 000, рисунок 2.

Наименьший прирост наблюдается в сегменте юридических лиц: их число увеличилось лишь на восемь организаций (с 22 до 30), что соответствует росту на 36 %, но в абсолютном выражении – это крайне малая величина для формирования репрезентативной выборки (см. рис 3).

Среди положительных нюансов рассматриваемой ситуации можно выделить поступательный, хотя и медленный, рост по всем категориям, что подтверждает продолжение операционной деятельности в рамках пилота. Увеличение числа банков создает задел для будущего масштабирования системы. Кроме того, текущие, меньшие по объему, но более вовлеченные группы тестирования могут предоставить более качественные и детальные данные о пользовательском опыте и технических аспектах взаимодействия.

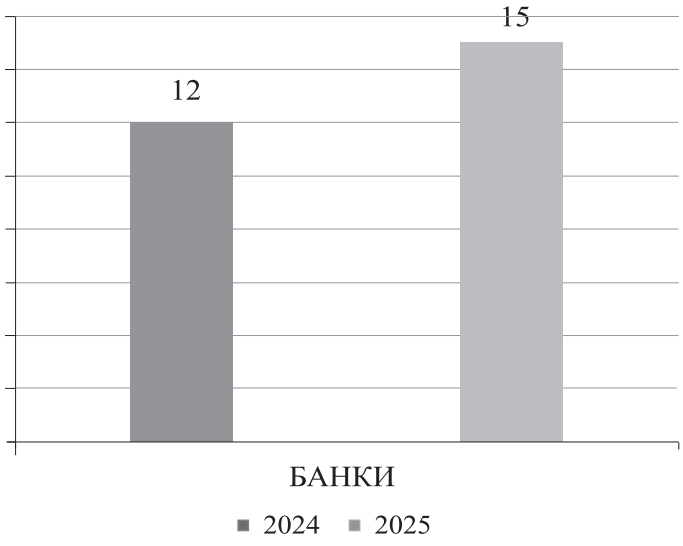

Рис. 1. Количество участников-банков в пилоте

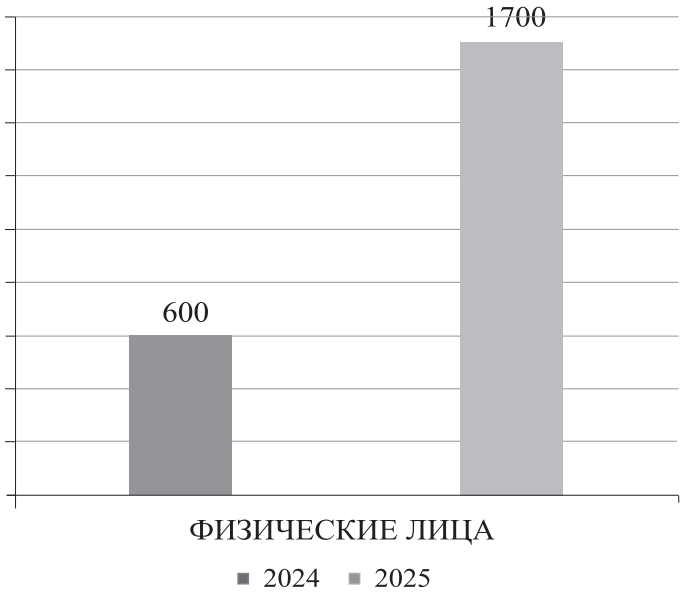

Рис. 2. Количество физических лиц в пилоте

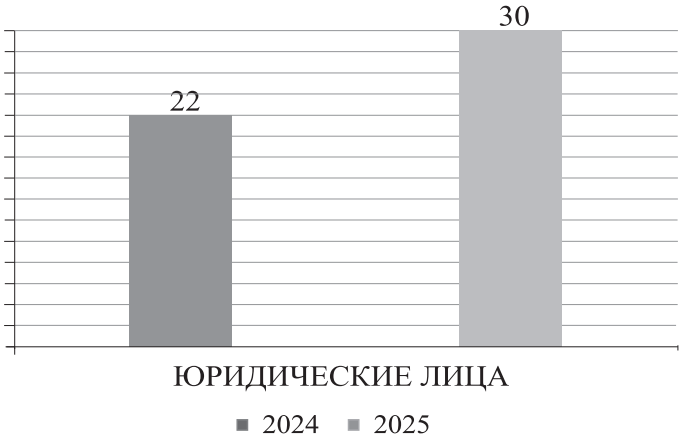

Рис. 3. Количество юридических лиц в пилоте

Ключевым негативным нюансом является критическое отставание от целевых показателей, особенно в части привлечения бизнеса. Низкая вовлеченность юридических лиц (всего восемь новых компаний за полгода) ставит под сомнение возможность полноценной апробации одной из основных функций цифрового рубля – проведения расчетов между организациями (B2B[6]). Этот недостаток становится особенно заметным на фоне формально позитивной статистики, изображенной на рис. 4: около 2500 открытых кошельков, доступность в 15 банках из более чем 150 населенных пунктов, свыше 63 тысяч C2C-переводов[7] и 13 тысяч C2B-платежей. Однако, при объективном анализе темпы развития выглядят замедленными – 2500 кошельков за примерно 1,5 года пилота несоизмеримо мало в масштабах российской финансовой системы, а транзакционная активность остается на уровне ограниченного эксперимента.

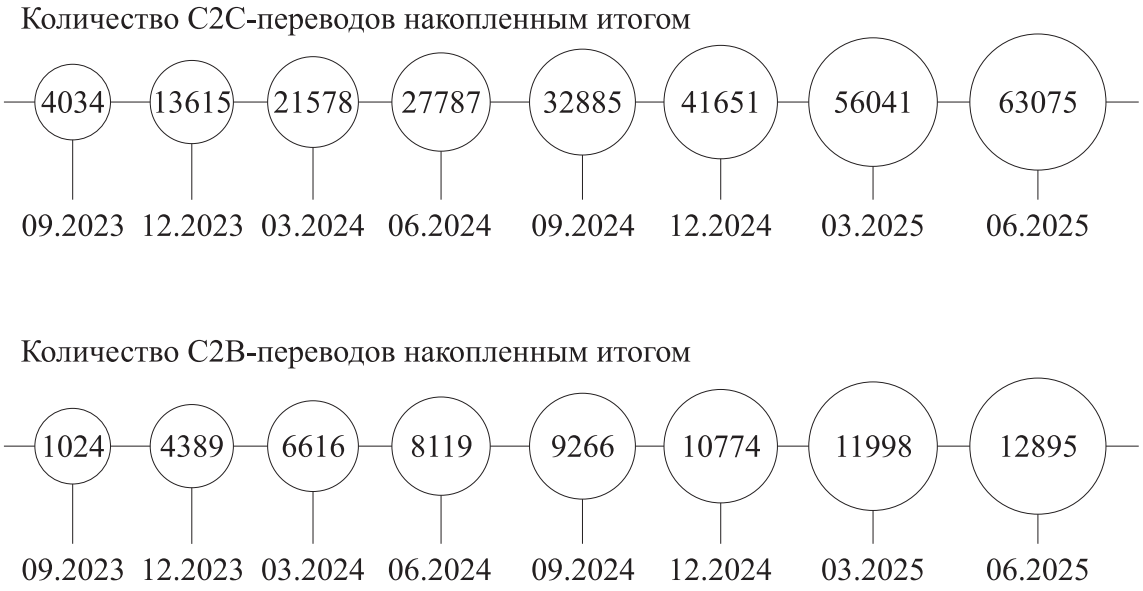

Рис. 4. Динамика операций перевода средств между физическими лицами (C2C) и между физическими лицами и бизнесом (C2B) на платформе цифрового рубля (штуки)

[6] B2B (business-to-business) – это бизнес-модель, при которой одна компания продаёт продукцию другим компаниям. Продажи в B2B масштабные, сложные, с длительным циклом сделки. Часто продажи в B2B длятся несколько недель и сопровождаются различными обсуждениями. Подробнее о применении данной модели см. публикацию «Что такое B2B: примеры компаний и особенности модели» URL: https://skillbox.ru/ media/ marketing/slovar-marketologa-chto-takoe-b2b-b2c-i-b2g/#stk-1 (дата обращения: 25.12.2025).

[7] C2C-переводы – это денежные переводы для физических лиц через систему быстрых платежей «СБП (C2C)», то есть переводы по номеру телефона между счетами клиентов в разных банках. Другими словами, C2C – это такая модель продаж, в которой сторонами сделки выступают частные лица, например, при реализации б/у вещей через объявления; также сюда входит оказание различных услуг или продажа хендмейд-товаров. Модель C2C востребована на специальных платформах в интернете: на маркетплейсах, в сервисах объявлений (Авито, Юла), мессенджерах или на интернет-аукционах. Подробнее см. публикацию «C2C: как устроены продажи между частными лицами». URL: https://sales-generator.ru/blog/c2c/ (дата обращения: 25.12.2025).

Для Банка России складывается тревожная ситуация: при наличии стратегических преимуществ в области экономической безопасности (укрепление финансового суверенитета, снижение зависимости от иностранных систем, повышение прозрачности финансовых потоков) и значительных потенциальных выгод для государственных (муниципальных) учреждений (оптимизация платежей, борьба с коррупцией, точечная денежно-кредитная политика), практическая реализация сталкивается с системными трудностями.

Особую озабоченность вызывает невозможность полноценного тестирования B2B-функционала, который является критически важным для интеграции цифрового рубля в реальную экономику. Низкий интерес бизнеса может быть связан как с технологическими барьерами, так и с недостаточной стимулирующей политикой.

При этом сохраняются фундаментальные риски: угрозы кибербезопасности централизованной платформы, потенциальная дестабилизация банковского сектора из-за миграции средств, дилемма между финансовым контролем и конфиденциальностью.

В контексте экономической безопасности наблюдающиеся темпы реализации пилота создают значительные риски. Замедленное расширение пилота сигнализирует о потенциальной неспособности инфраструктуры выдержать нагрузку в масштабах всей страны к установленному сроку, что может привести к операционным сбоям и подорвать доверие к национальной платежной системе. Успешное же развертывание, напротив, позволит усилить суверенитет финансовой системы, минимизировать зависимость от трансграничных платежных механизмов и повысить прозрачность денежных потоков, что является стратегическим приоритетом в условиях внешнего давления [7, с. 85]. Для государственных учреждений текущая динамика процесса означает необходимость ускоренной адаптации. Бюджетной системе, налоговым и таможенным органам предстоит обеспечить технологическую интеграцию с платформой цифрового рубля для проведения расчетов и контроля фискальных операций. Низкие показатели пилотного проекта демонстрируют, что как государственный, так и частный сектор не полностью готовы к этому переходу, что требует интенсификации организационно-технической подготовки для своевременного выполнения требований законодательства.

Внедрение цифрового рубля (ЦР), как третьей формы национальной валюты, формирует комплекс взаимосвязанных рисков для государственных учреждений, требующих системного анализа и адресного управления. Проведенная кластеризация угроз позволяет выделить три ключевых категории рисков: технологические риски и риски кибербезопасности, операционно-регуляторные риски, а также риски макроэкономические и системные (информации о проявлении указанных рисков проиллюстрирована в нижеприведенной таблице).

В рамках технологических рисков особую значимость приобретает угроза целевых атак на узлы (ноды) ключевых финансовых ведомств, таких как Министерство финансов и Федеральное казначейство. Реализация данной угрозы через методы Advanced Persistent Threat (APT)[8] может привести к прямому хищению бюджетных средств и подрыву финансовой стабильности государства [9, с. 50]. Не менее существенной является проблема компрометации алгоритмов смарт-контрактов, регулирующих критически важные бюджетные процессы, включая межбюджетные трансферты, исполнение государственных контрактов и социальные выплаты. Уязвимости в программном коде создают риски несанкционированного изменения финансовых потоков, что способно парализовать ключевые функции бюджетной системы. Дополнительным вызовом становится концентрация конфиденциальных данных о финансовых операциях государства в едином цифровом реестре, что создает предпосылки для масштабных утечек информации, составляющей государственную тайну. Завершает данный кластер угроза координационных DDoS-атак в периоды повышенной операционной нагрузки на платформу, способных вызвать коллапс системы расчетов в критически важные для бюджетного процесса моменты [8].

Операционно-регуляторные риски характеризуются наличием внутренних угроз, связанных с человеческим фактором. Недостаточная квалификация государственных служащих при работе с новыми цифровыми процедурами может привести к ошибкам в осуществлении трансакций на многомиллиардные суммы. Правовые коллизии и пробелы в нормативном регулировании создают существенные препятствия для оспаривания мошеннических операций с цифровым рублем, формируя правовую неопределенность. Отсутствие унифицированных административных регламентов для бюджетных платежей в цифровом рубле способно вызвать несогласованность действий между различными уровнями власти и бюджетными учреждениями. Особую опасность представляет риск внутренних злоупотреблений при настройке и администрировании смарт-контрактов, когда уполномоченные сотрудники могут умышленно изменять параметры контрактов в корыстных целях.

Макроэкономические и системные риски имеют стратегический характер и затрагивают основы финансовой стабильности. Массовый переход бюджетных учреждений на расчеты в цифровом рубле может спровоцировать отток ликвидности с корреспондентских счетов кредитных организаций, что способно дестабилизировать банковскую систему и вызвать кризис ликвидности. Централизация информации о всех финансовых потоках государства создает уникальный объект для экономического шпионажа и санкционного давления, повышая уязвимость национальной финансовой системы перед внешними угрозами. Технологическая зависи-

[8] APT (Advanced Persistent Threat) – это понятие, применяемое в сфере кибербезопасности, описывает сложные и долгосрочные кибератаки. Злоумышленники проникают в систему, закрепляются там и на протяжении нескольких месяцев или даже лет осуществляют скрытую деятельность [9, с. 50].

Таблица

Кластеризация рисков и угроз внедрения цифрового рубля в деятельность государственных учреждений

Кластер угроз	Конкретные проявления для государства и государственных учреждений	Потенциальные последствия
Технологические и кибербезопасности	1. Целевые атаки на ноды Казначейства и Минфина, ведущие к хищению бюджетных средств. 2. Компрометация смарт-контрактов, управляющих социальными выплатами, государственными контрактами и межбюджетными трансфертами. 3. Утечка конфиденциальных данных о финансовых потоках и закупках, составляющих государственнцю тайну. 4. Координированные DDoS-атаки[9] на платформу в ключевые моменты (например, перед выборами), парализующие работу бюджетной сферы.	1. Прямой ущерб федеральному и региональным бюджетам. 2. Срыв выполнения государственных программ и социальных обязательств. 3. Подрыв доверия к государству как к гаранту финансовой стабильности и защитнику данных. 4. Дестабилизация социально-экономической ситуации.
Операционные и регуляторные	1. Ошибки госслужащих из-за неосвоенности новых цифровых процедур, ведущие к ошибочным переводам на миллиарды рублей. 2. Правовые коллизии и пробелы в регулировании, затрудняющие оспаривание мошеннических операций с использованием ЦР. 3. Несовершенство регламентов: отсутствие четких процедур для бюджетных платежей в ЦР, что приводит к хаосу и задержкам. 4. Риск «человеческого фактора» – внутренние злоупотребления при настройке смарт-контрактов.	1. Некорректное исполнение бюджета, срывы в финансировании критически важных объектов (например, оборонных). 2. Правовая неопределенность и длительные судебные разбирательства. 3. Снижение эффективности государственного финансового управления и роста коррупционных рисков.
Макроэкономические и системные	1. Отток средств с корреспонденских счетов бюджетных учреждений в ЦР, ведущий к снижению ликвидности банковской системы и росту ее неустойчивости. 2. Концентрация всех финансовых операций государства в едином цифровом реестре, создающая уникальный объект для шпионажа и санкционного давления. 3. Риск технологической зависимости от ограниченного круга вендоров, создающих и обслуживающих платформу ЦР. 4. Снижение финансового суверенитета в случае успешной кибератаки на критическую финансовую инфраструктуру.	1. Дестабилизация национальной банковской системы, кризис ликвидности. 2. Утрата контроля над стратегической финансовой информацией. 3. Уязвимость государственных финансов перед внешними игроками. 4. Системный кризис экономической безопасности страны.

мость от ограниченного круга вендоров, разрабатывающих и обслуживающих платформу цифрового рубля, создает риски снижения технологического суверенитета и роста долгосрочных затрат на поддержание системы. Кумулятивный эффект от реализации перечисленных угроз создает предпосылки для системного кризиса экономической безопасности страны в случае успешной масштабной кибератаки на критическую финансовую инфраструктуру.

Проведенный анализ рисков позволяет утверждать, что переход на цифровой рубль коренным образом меняет структуру угроз для государственного аппарата. Формируется принципиально иная среда рисков, где традиционные финансовые опасности трансформируются в комплексные технологические и системные вызовы.

Если говорить конкретнее, государство сталкивается не с отдельными, изолированными проблемами, а с целой системой взаимосвязанных вызовов. Техническая уязвимость платформы может мгновенно спровоцировать операционный сбой в работе ключевых министерств, а ошибка в алгоритме способна вызвать цепную реакцию нарушений по всей бюджетной сети. Киберугроза перестает быть просто риском потери средств, превращаясь в угрозу срыва выполнения национальных проектов и социальных обязательств.

Это означает, что старые подходы к безопасности, основанные на защите периметра отдельных ведомств, больше не работают. Угрозы стали сложными, сетевыми и требуют таких же сложных, системных ответов. Недостаточно просто установить новые программы – необходима глубокая перестройка самих принципов управления финансами, подготовки кадров и взаимодействия между ведомствами в этой новой цифровой реальности.

[9] DDoS-атака – это разновидность атаки на отказ в обслуживании, при которой злоумышленники используют множество заражённых устройств, объединённых в так называемый ботнет [8].

Следовательно, внедрение цифрового рубля (ЦР) представляет собой стратегическую инициативу, направленную не только на модернизацию финансовой системы, но и на укрепление суверенитета и экономической безопасности Российской Федерации. Практическая реализация данного проекта сопряжена с комплексом вызовов и возможностей, требующих разработки уникальных решений и превентивных мер.

Традиционные риски, такие как кибератаки, отмывание денег и мошенничество, в условиях цифровой валюты Банка России трансформируются в более сложные схемы. Для их нейтрализации предлагается концепция «Адаптивной мультиагентной системы защиты цифрового рубля». Данная система основана на интеграции нескольких инновационных модулей, функционирующих в реальном времени и приведенных ниже.

1. *Модуль предиктивной аналитики на основе искусственного интеллекта*. В отличие от существующих систем, реагирующих на уже произошедшие инциденты, данный модуль будет анализировать паттерны транзакций в распределенном реестре ЦР, выявляя аномалии, нехарактерные для легальной экономической деятельности. Например, система сможет идентифицировать микроплатежи, используемые для тестирования уязвимостей, или сложные схемы обналичивания, маскирующиеся под легитимные операции.

2. *Модуль динамического смарт-контрактного регулирования*. Каждый цифровой кошелек будет оснащен смарт-контрактом, параметры которого (лимиты транзакций, разрешенные контрагенты, типы товаров и услуг) могут динамически изменяться Банком России в зависимости от оценки риска. Например, для транзакций свыше определенного порога или с юрисдикциями «повышенного риска» будет автоматически требоваться многофакторная аутентификация, включая биометрические данные, верифицированные через Единую систему идентификации и аутентификации (ЕСИА).

3. *Децентрализованная система аутентификации для государственных учреждений*. Для защиты критической инфраструктуры государственных учреждений, работающих с ЦР, предлагается внедрение квантово-устойчивой блокчейн-идентификации. Каждое учреждение будет иметь цифровой сертификат, записанный в защищенный блокчейн-реестр, не связанный напрямую с основным реестром ЦР. Доступ к проведению операций с ЦР будет предоставляться только после верификации через эту систему, что исключит возможность несанкционированного доступа даже в случае компрометации одного из элементов IT-инфраструктуры. Для наглядности представим на рисунке 5 структуру данной системы.

Практическая реализация предложений по защите данных физических и юридических лиц, государственных учреждений позволит трансформировать цифровой рубль из потенциального объекта уязвимости в ключевой актив национальной экономической безопасности, обеспечив суверенитет финансовой системы, технологическую независимость и устойчивость к современным киберугрозам в условиях цифровой трансформации.

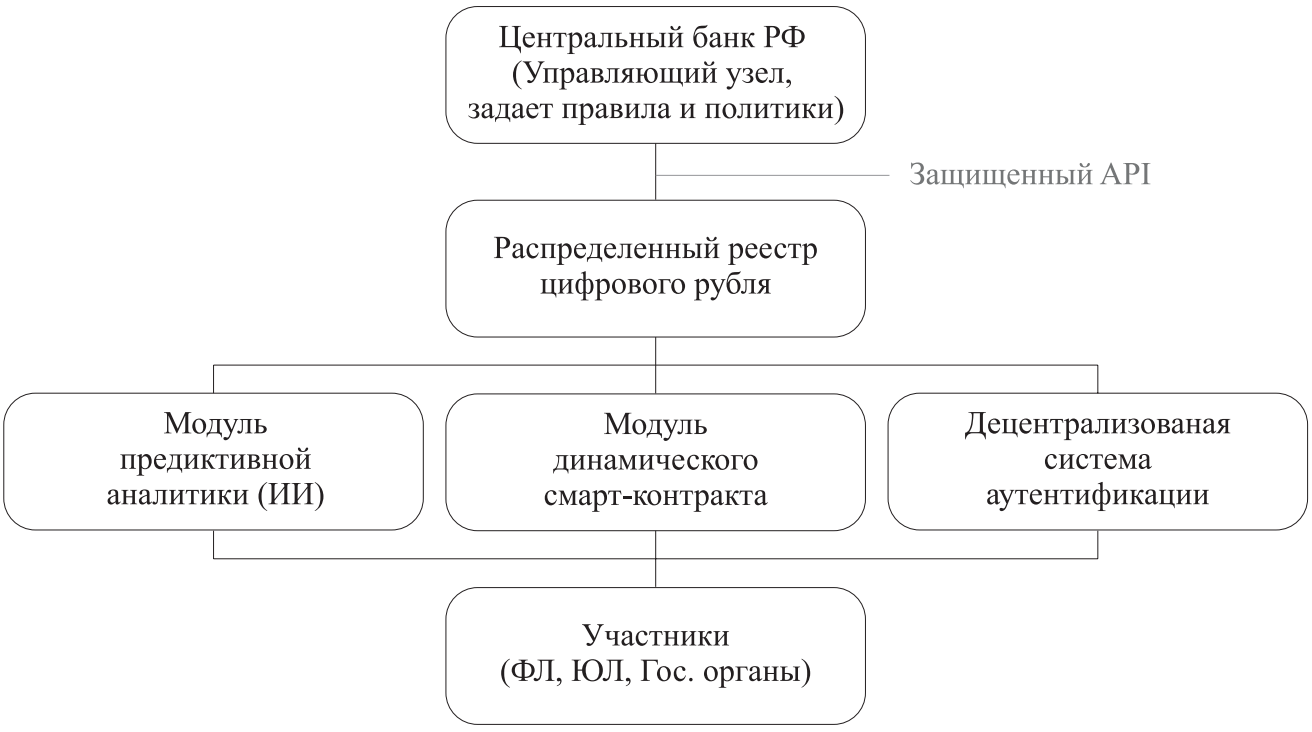

Рис. 5. Структура Адаптивной мультиагентной системы защиты цифрового рубля (АМСЗ ЦР)

Таким образом, проведенное исследование позволяет сделать вывод, что внедрение цифрового рубля представляет для Российской Федерации не только технологический вызов, но и стратегическую возможность системной трансформации государственного управления. Для государственных учреждений данный процесс означает фундаментальный пересмотр традиционных подходов к обеспечению экономической безопасности и выполнению бюджетных функций.

Особую значимость приобретает необходимость формирования принципиально новой архитектуры защищенного взаимодействия между ведомствами в условиях цифровой среды. Федеральное казначейство, Министерство финансов, налоговые и таможенные органы становятся не просто пользователями новой системы, а ключевыми элементами распределенной цифровой инфраструктуры, от устойчивости которой зависит национальная финансовая стабильность.

Практическая реализация проекта требует от государственного аппарата решения комплекса взаимосвязанных задач: от разработки межведомственных стандартов и протоколов до создания системы непрерывного профессионального развития сотрудников (работников государственных и муниципальных учреждений). Особое значение приобретает формирование единого нормативного поля, регулирующего использование смарт-контрактов для бюджетных расчетов и обеспечивающего правовую определенность совершаемых операций.

Центральным элементом стратегии должно стать опережающее развитие компетенций в области кибербезопасности и управления цифровыми рисками. Государственным (муниципальным) учреждениям предстоит не только освоить новые технологии, но и сформировать культуру проактивного управления угрозами, основанную на принципах непрерывного мониторинга и адаптации к изменяющимся условиям.

Успешная интеграция цифрового рубля в деятельность государственных институтов позволит не только повысить эффективность бюджетных процессов, но и создать основу для нового качества государственного управления – более прозрачного, технологически независимого и устойчивого к внешним вызовам. Это потребует скоординированных усилий по развитию национальной технологической базы, подготовке кадров нового поколения и формированию сбалансированной нормативно-правовой среды, способной обеспечить как инновационное развитие, так и надежную защиту национальных экономических интересов.

Литература

1. *Мельмонт Д. Д.* Влияние цифровизации на экономическое и социальное развитие регионов в России // Вопросы инновационной экономики. 2024. Т. 14, № 4. С. 1215–1228. DOI: 10.18334/vinec.14.4.122154

2. *Матюшкин Д. А.* Развитие цифровой экономики в Российской Федерации // Международный научный журнал «Вестник науки». 2022. № 5 (50). С. 111–126.

3. *Сергеев Л. И.*, *Сергеев Д. Л.*, *Юданова А. Л.* Цифровая экономика: учебник для вузов; под редакцией Л. И. Сергеева. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2023. – 437 с.

4. *Шумилова В. В.* Цифровой рубль Банка России как новая форма национальной валюты // Legal Concept. 2022. Т. 21, № 2. С. 156–162. DOI: 10/15688/1c.jvolsu.2022.2/20

5. *Порхачев С. К*. Цифровой рубль: проблемы и перспективы внедрения / В сборнике: Весенние дни науки // Международная конференция студентов и молодых ученых (Екатеринбург, 21-23 апреля 2022 г.) – Екатеринбург: Уральский федеральный университет им. первого Президента России Б. Н. Ельцина, 2022. С. 548–552.

6. Отчет Банка России от 30 июня 2025 года «Цифровой рубль: текущий статус проекта». – М.: Банк России, 2025. – 25 с. URL: https://cbr.ru/Content/Document/File/177415/ digital_ruble_30062025.pdf.

7. *Трофимов Д. В.* Преимущества и недостатки введения цифрового рубля // Финансовые рынки и банки. 2023. № 10. С. 84–87.

8. *Голубятников А.О.* DDOS-атаки и методы борьбы с ними // E-Scio. 2022. № 10 (73). URL: https://cyberleninka.ru/article/n/ddos-ataki-i-metody-borby-s-nimi/viewer (дата обращения: 14.10.2025).

9. *Будников С.А., Бутрик Е.Е., Соловьев С.В.* Моделирование APT-АТАК, эксплуатирующих уязвимость ZEROLOGON // Вопросы кибербезопасности. 2021. № 6 (46). С. 46–61. DOI: 10.21681/2311-3456-2021-6-47-61

Сведения об авторах

Димитриева Елена Николаевна – кандидат экономических наук, доцент, доцент кафедры финансов и кредита, Сибирский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Новосибирск, Россия.
E-mail: Ulagan-alena@mail.ru

Верятина Ася Яковлевна – бухгалтер ООО «Сорцум», Новосибирск, Россия.
E-mail: asyaveryatina09@gmail.com

Петровская Алина Евгеньевна – бухгалтер ООО «Сорцум», Новосибирск, Россия.
E-mail: petrovskaya_18_03@mail.ru

THE IMPACT OF THE INTRODUCTION OF THE DIGITAL RUBLE ON ENSURING THE ECONOMIC SECURITY OF THE RUSSIAN FEDERATION IN THE CONTEXT OF THE DIGITALIZATION

E. Dimitrieva
Siberian Institute of Management – branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Novosibirsk, Russia

A. Veryatina, A. Petrovskaya
Siberian Sortsum LLC, Novosibirsk, Russia

Abstract. This article analyzes the impact of the digital ruble's implementation on the country's economic security. It examines the nature of the digital ruble, the legal framework governing its circulation, and the current status of the pilot project. Particular attention is paid to identifying key threats to the implementation of digital currency that lead to economic losses and proposing solutions to protect government data. It concludes that a balance between technological innovation and economic security is essential for the successful integration of the digital ruble into the country's financial system.

Keywords: digital ruble, economic security, digitalization, threats to the state's economic security, financial system, and pilot project.

References

1. Mel'mont D.D. The impact of digitalization on the economic and social development of regions in Russia, *Voprosy innovatsionnoi ekonomiki*, 2024, Vol. 14, No. 4, pp. 1215–1228. (In Russ.). DOI: 10.18334/vinec.14.4.122154

2. Matyushkin D.A. Development of the digital economy in the Russian Federation, *Mezhdunarodnyi nauchnyi zhurnal "Vestnik nauki",* 2022, No. 5 (50), pp. 111–126. (In Russ.).

3. Sergeev L.I., Sergeev D.L., Yudanova A.L. *Tsifrovaya ekonomika: uchebnik dlya vuzov* [Digital economy: a textbook for universities], Moscow: Izdatel'stvo Yurait, 2023, 437 p. (In Russ.).

4. Shumilova V.V. The digital ruble of the Bank of Russia as a new form of national currency, *Legal Concept*, 2022, Vol. 21, No. 2, pp. 156–162. (In Russ.). DOI: 10/15688/1c.jvolsu.2022.2/20

5. Porkhachev S.K. Digital ruble: problems and prospects of implementation, *Vesennie dni nauki* [Spring Days of Science], International Conference of Students and Young Scientists (Yekaterinburg, April 21-23, 2022), Ekaterinburg: Ural'skii federal'nyi universitet im. pervogo Prezidenta Rossii B.N. El'tsina, 2022, pp. 548–552. (In Russ.).

6. *Otchet Banka Rossii ot 30 iyunya 2025 goda "Tsifrovoi rubl': tekushchii status proekta"* [The report of the Bank of Russia dated June 30, 2025 "Digital Ruble: current project status"], Moscow: Bank Rossii, 2025, 25 p., available at: https://cbr.ru/Content/Document/File/177415/ digital_ruble_30062025.pdf. (In Russ.).

7. Trofimov D.V. Advantages and disadvantages of introducing a digital ruble, *Finansovye rynki i banki*, 2023, No. 10, pp. 84–87. (In Russ.).

8. Golubyatnikov A.O. DDOS attacks and methods of combating them, *E-Scio*, 2022, No. 10 (73), available at: https://cyberleninka.ru/article/n/ddos-ataki-i-metody-borby-s-nimi/viewer (date of access: 14.10.2025). (In Russ.).

9. Budnikov S.A., Butrik E.E., Solov'ev S.V. Simulation of APT ATTACKS exploiting the ZEROLOGON vulnerability, *Voprosy kiberbezopasnosti*, 2021, No. 6 (46), pp. 46–61. (In Russ.). DOI: 10.21681/2311-3456-2021-6-47-61

About the authors

Elena N. Dimitrieva – Candidate of Economic Sciences, Associate Professor, Siberian Institute of Management – branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Novosibirsk, Russia.
E-mail: Ulagan-alena@mail.ru

Asya Ya. Veryatina – accountant of Sortsum LLC, Novosibirsk, Russia.
E-mail: asyaveryatina09@gmail.com

Alina E. Petrovskaya – accountant of Sortsum LLC, Novosibirsk, Russia.
E-mail: petrovskaya_18_03@mail.ru