Целых Александр Николаевич – Южный федеральный университет; e-mail: ant@sfedu.ru; г. Таганрог, Россия; тел.: +79185562047; кафедра ИАСБ; д.т.н.; зав. кафедрой.

Васильев Владислав Сергеевич – Южный федеральный университет; e-mail: vsvasilev@sfedu.ru; г. Таганрог, Россия; тел.: +79185983647; кафедра ИАСБ; к.ф.-м.н.; доцент.

Целых Лариса Анатольевна – Южный федеральный университет; e-mail: l.tselykh58@gmail.com; г. Таганрог, Россия; тел.: +79185562047; кафедра ИАСБ; к.э.н.; доцент.

Подоплелова Елизавета Сергеевна – Южный федеральный университет; e-mail: chuzhinova@sfedu.ru; г. Таганрог, Россия; тел.: +79525844188; кафедра ИАСБ; старший преподаватель.

Tselykh Alexander Nikolayevich – Southern Federal University; e-mail: ant@sfedu.ru; Taganrog, Russia; phone: +79185562047; the department IASB; dr. of eng. sc.; head of department.

Vasilev Vladislav Sergeevich – Southern Federal University; e-mail: vsvasilev@sfedu.ru; Taganrog, Russia; phone: +79185983647; the department IASB; cand. of phys. and math. sc.; associate professor.

Tselykh Larisa Anatolievna – Southern Federal University; e-mail: l.tselykh58@gmail.com; Taganrog, Russia; phone: +79185562047; the department IASB; cand. of ec. sc.; associate professor.

Podoplelova Elizaveta Sergeevna – Southern Federal University»; e-mail: chuzhinova@sfedu.ru; Taganrog, Russia; phone: +79525844188; the department IASB; senior lecturer.

УДК 004.056 DOI 10.18522/2311-3103-2025-3-233-245

А.В. Иванов, А.В. Царегородцев, М.В. Валеев

ТЕХНОЛОГИЧЕСКОЕ РЕШЕНИЕ ПО ФОРМИРОВАНИЮ ИНФРАСТРУКТУРЫ ДОВЕРИЯ В СИСТЕМЕ ЗАЩИЩЕННОСТИ ЦИФРОВОГО РУБЛЯ

Актуальность статьи обусловлена цифровой трансформацией российской экономики, важнейшим направлением которой является разработка и внедрение инструментов цифрового рубля в кредитно-финансовой сфере. В этой связи национальная система должна базироваться на информационно-технологической инфраструктуре доверия в системе защищенности цифрового рубля. Основными функциональными свойствами подобной инфраструктуры доверия относятся механизмы идентификация и аутентификация, безопасных финансовых транзакций на основе защиты целостности и конфиденциальности данных участников и пользователей платформы цифрового рубля. Кроме технологической готовности инфраструктуры доверия необходимо формирование доверия населения к цифровому рублю. Вышеназванные обстоятельства обусловили важность и необходимость разработки технологического решения по формированию инфраструктуры доверия в системе защищенности цифрового рубля. В процессе исследования решены следующие задачи: проведена теоретическая интерпретация и эмпирическая операционализация базовых понятий инфраструктуры доверия цифрового рубля; исследованы ее организационно-технологические предпосылки; уточнены структурные элементы базовой и ролевой модели инфраструктуры цифрового рубля; проведён анализ методов шифрования и токенизации API, а также сформулировано технологическое решение по обеспечению защищенности инфраструктуры доверия цифрового рубля. По результатам исследования предложен комплекс мер направленных на безопасность допуска к платформе цифрового рубля участников и пользователей по защищённым каналам; безопасность допуска кредитных организаций на основе двухфакторной аутентификации, а также безопасность конфиденциальности физических и юридических лиц на инфраструктуре доверия в системе защищенности цифрового рубля. Практическое значение имеет перечень работ, связанных с развёртыванием Удостоверяющих центров, средств защиты информации и СКЗИ, интеграцией с единой системой идентификации и аутентификации информационного и системой быстрых платежей и их внедрением в общей системе цифрового рубля.

Цифровой рубль; инфраструктура доверия; защищенность системы цифрового рубля; инфраструктура доверия в системе цифрового рубля; удостоверяющие центры; шифрование; кредитные организации; сертификаты; платформа цифрового рубля.

A.V. Ivanov, A.V. Tsaregorodtsev, M.V. Valeev

TECHNOLOGICAL SOLUTION FOR FORMING A TRUST INFRASTRUCTURE IN THE DIGITAL RUBLE SECURITY SYSTEM

The relevance of the article is due to the digital transformation of the Russian economy, the most important direction of which is the development and implementation of digital ruble instruments in the credit and financial sector. In this regard, the national system should be based on the information technology infrastructure of trust in the digital ruble security system. The main functional properties of such a trust infrastructure include identification and authentication mechanisms, secure financial transactions based on protecting the integrity and confidentiality of data of participants and users of the digital ruble platform. In addition to the technological readiness of the trust infrastructure, it is necessary to build public trust in the digital ruble. The above circumstances determined the importance and necessity of developing a technological solution for the formation of a trust infrastructure in the digital ruble security system. In the course of the study, the following tasks were solved: a theoretical interpretation and empirical operationalization of the basic concepts of the digital ruble trust infrastructure were carried out; its organizational and technological prerequisites were investigated; the structural elements of the basic and role models of the digital ruble infrastructure were clarified; the analysis of encryption and tokenization methods of API was carried out, and a technological solution was formulated to ensure the security of the digital ruble trust infrastructure. Based on the results of the study, a set of measures aimed at the security of access to the digital ruble platform for participants and users via secure channels is proposed; the security of access for credit institutions based on two-factor authentication, as well as the security of the privacy of individuals and legal entities on the trust infrastructure in the digital ruble security system. Of practical importance is the list of works related to the deployment of Certification Authorities, information security tools and cryptographic information protection tools, integration with a unified information identification and authentication system and a fast payment system and their implementation in the general digital ruble system.

Digital ruble; trust infrastructure; security of the digital ruble system; trust infrastructure in the digital ruble system; certification authorities; encryption; credit institutions; certificates; digital ruble platform.

Введение. Актуальность исследования процессов формирования инфраструктуры доверия в системе защищенности цифрового рубля обусловлена необходимостью научного (теоретическая интерпретация) и технологического (технологическая операционализация) определения таких понятий как: «цифровой рубль», «инфраструктура доверия», «защищенность цифрового рубля», а также формирования инфраструктуры доверия в системе цифрового рубля. Цифровой рубль (ЦР) – форма денег наряду с наличными и безналичными рублями, которую выпускает Банк России в виде цифрового кода (токена), который хранится в цифровых кошельках на его платформе. С помощью цифрового рубля можно платить за товары и услуги, а также осуществлять его перевод другим лицам. Особенности цифрового рубля «нельзя открыть вклад или получить кредит, можно создавать один цифровой кошелёк в любом удобном банке, пополнять его и снимать средства, отсутствие комиссий для граждан **(**для компаний она составит 0,3%) [1, 2]. Понятие «инфраструктура доверия» включает как технологические (методы, средства, технологии), так и регуляторные (законы, стандарты, нормы, правила, стандарты) меры по формированию инфраструктурной среды в которой его участники могут взаимодействовать на основе доверительных отношений. В общем плане можно утверждать, что инфраструктура доверия подразумевается нами как многоуровневая система, обеспечивающая доверие на основе сочетания технологических (технических) решений, правовых норм и механизмов функционирования технических систем. Понятие «защищенность цифрового рубля» понимается как комплекс мероприятий, связанных с конфиденциальностью и целостностью информации, а также организацией доступа, защитой персональных данных (платежей, транзакций), идентификацией пользователей по защите от несанкционированных действий в системе цифрового рубля. Поэтому построение многоуровневой системы защищенности, надёжности и безопасности будет способствовать формированию доверия к системе цифрового рубля.

Основная часть. Для анализа формирования инфраструктуры доверия в системе защищенности цифрового рубля важен научный подход по изучению предмета исследования. Например, ряд ученных акцентируют внимание на проблемах и перспективах

обеспечения безопасности цифрового рубля, основанной на «применении криптографических методов шифрования данных, подписей электронных транзакций и мультифакторной аутентификации, а также анализе преимуществ использования гражданами и бизнесом цифрового рубля» [3, 4]. В отдельных работах рассматривает связь между моделями доверия и архитектурой инфраструктуры открытых ключей, которая для криптографических преобразований использует ключевую пару: секретный ключ и открытый ключ. В этой связи рассматриваются две модели использования ключевых пар и сертификатов: децентрализованная модель сетей доверия, создаваемых на основе соглашений доверия удостоверяющих центров (УЦ), не прошедших аккредитацию; модель квалифицированного единого пространства доверия, в основу которой положена система аккредитованных УЦ и развёрнутая на их базе инфраструктуры открытых ключей (ИОК). В системе удостоверяющих центров традиционно принято классифицировать УЦ по доверительным признакам, например, удостоверяющие центры, которым по умолчанию доверяет все пользователи системы (корневые центры сертификации) и удостоверяющие центры, которым доверяют сами владельцы сертификатов, в связи с чем они формирую свои домены доверия (доверенные центры сертификации). Если бы утеряно доверие к исходному значению корневого центра сертификации, то и автоматически теряется доверие ко всем последующим звеньям цепочки сертификации.

Выделяются различные модели доверия, такие как: иерархическая, браузерная, сетевая и кросс-сертификационные модели доверия [5].

Мельников Д. А. на основе математического аппарата субъективной логики криптографических средств защиты информации в инфраструктуре открытых ключей предлагает «объединить все существующие удостоверяющие центры инфраструктуры открытых ключей в единую инфраструктуру открытых ключей Российской Федерации, а также сформировать технологическую основу доверия для различных прикладных автоматизированных информационно-технологических систем» [6]. Отдельные работы посвящены исследованию доверия при безопасной разработке программного обеспечения. «Безопасная разработка программного обеспечения является основой доверия к информационно-коммуникационным технологиям в условиях современных киберугроз на объектах критической информационной инфраструктуры [7].

Важное значение имеют практические рекомендации по формированию инфраструктуры доверия в системе цифрового рубля. Основными элементами такой модели являются: «репозитарий «движения» (активных) цифровых рублей (ЦР), которые выпущены Центральным Банком Российской Федерации (ЦБ); корневой удостоверяющий центр ЦБ; территориальные удостоверяющие центры (УЦ) ЦБ РФ; головной центр подтверждения подлинности ЦР и платёжных операций, принадлежащий ЦБ РФ; территориальные центры подтверждения подлинности ЦР и платёжных операций, принадлежащие ЦБ РФ, принадлежащие банкам; центры подтверждения подлинности ЦР и платёжных операций, принадлежащие банкам, обслуживающим организации (например, Интернет-магазины), которые принимают ЦР в качестве оплаты товаров и услуг; удостоверяющие центры банков, образующие второй уровень иерархии УЦ в ИОК ЦБ РФ; аккредитованные ЦБ РФ организации-продавцы (Интернет-магазины), которые принимают ЦР в качестве оплаты товаров и услуг, и которые подключены к территориальным центрам проверки подлинности ЦР соответствующих КФО (банков); физические и юридические лица, которые являются владельцами ЦР на основании соответствующих договоров с КФО (банками), аккредитованными ЦБ РФ и функционально-процедурная модель оплаты приобретённых товаров с помощью ЦР [8]» (рис. 1).

Для оценки состояния защищенности СЦР прикладное значение имеет исследование организационно – технологических предпосылок, включающие две группы: организационные (нормативные) и технологические (инфраструктурные), которые в целом способствовали формированию инфраструктуры доверия СЦР. Например, в ходе апробации пилотного проекта цифрового рубля (2022 г.) вводится понятие «платформа цифрового рубля» (далее ПЦР), предусматривающее [9]:

- ♦ организацию доступа пользователей к ПЦР;
- ♦ организацию доступа кредитной организации к ПЦР;

- организацию защиты данных на ПЦР;
- организацию защиты информационной безопасности;
- организацию защиты прав потребителей.

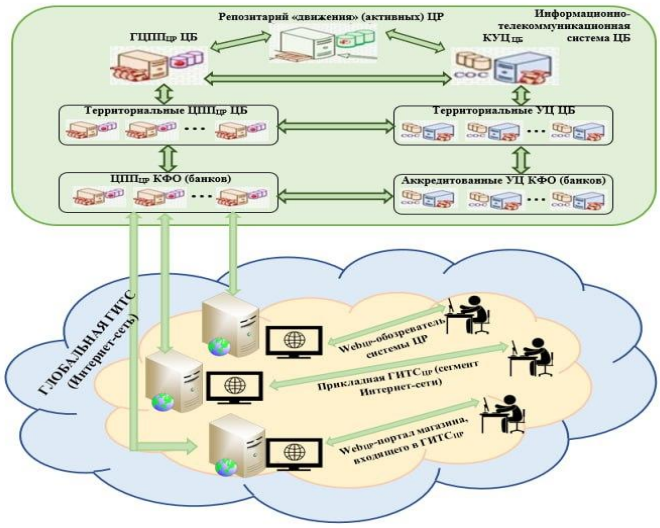

Рис. 1. Модель общей иерархической структуры инфраструктуры доверия Банка России [8]

Количественные характеристики соотношения наличных, безналичных и цифровых рублей представлено на рис. 2.

Рис. 2. Соотношение наличных, безналичных и цифровых рублей [Официальный сайт Банка России]

Организацию работ по противодействию финансовому мошенничеству среди различных категорий населения и формирования их доверия к системе цифрового рубля. Например, по результатам ежегодного опроса Банк России составил портрет пострадавшего от кибермошенников. В 2023 году 4 из 10 респондентов сталкивались с разными видами финансового мошенничества, при этом 10% лишились денег. Количество людей, которым звонили или писали злоумышленники, увеличилось. Например, чаще всего попадаются на уловки мошенников – это люди в возрасте от 25 лет до 64 лет, так как экономически более активны и часто пользуются банковскими онлайн-сервисами (рис. 3).

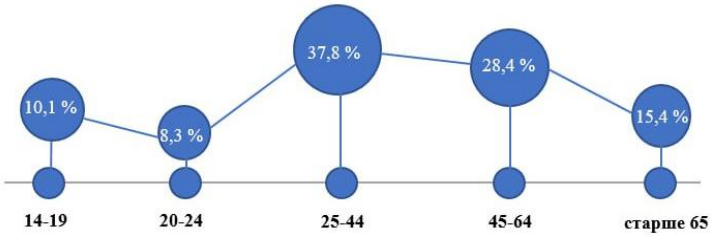

Рис. 3. Портрет пострадавших от кибермошенников по возрасту [https://cbr.ru/statistics/information_security/cyber_portrait/2024/]

С учётом сложившихся обстоятельств и в целях формирования инфраструктуры доверия в системе защищенности цифрового рубля Банком России сформулированы новые требования к участникам ПЦР [10] в соответствие с которыми разработана ролевая модель ее участников [11], включающей два уровня.

Первый уровень – **Банк России.** На первом уровне оператор платформы непосредственно создает и модифицирует саму «платформа цифрового рубля», а также подключает к ней Федеральное казначейство и иные финансовые организации (рис. 4).

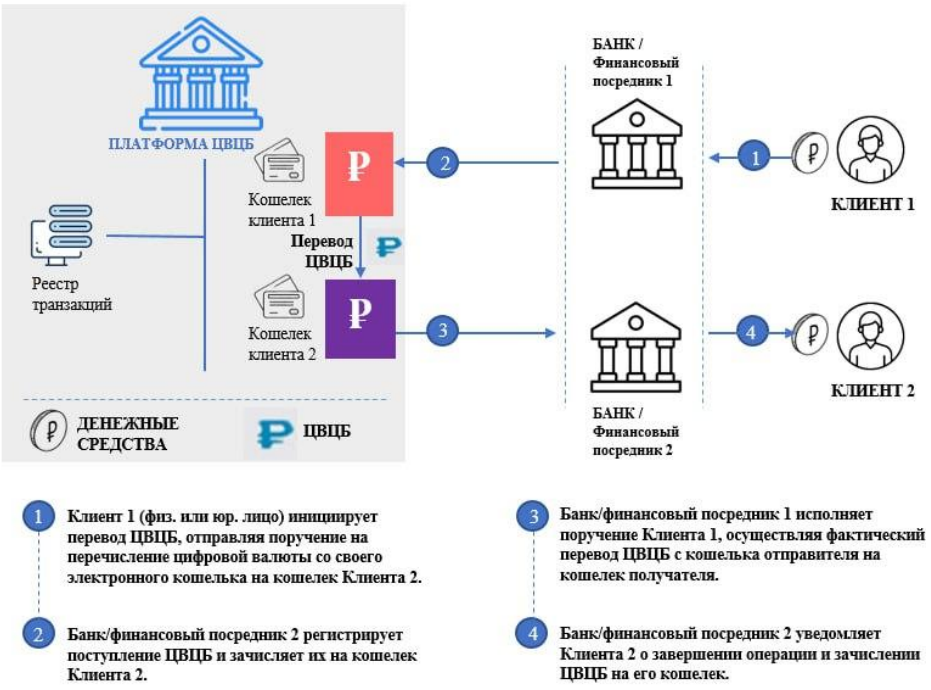

Рис. 4. Ролевая модель участников платформы цифрового рубля [Банк России. Концепция цифрового рубля. 2021]

Второй уровень – финансовые организации и Федеральное казначейство. На втором уровне уже финансовые организации взаимодействуют с клиентами по открытию и пополнению кошельков в рамках законодательства.

Архитектура прототипа ПЦР включает следующие ключевые компоненты: *Узлы Банка России, Удостоверяющий центр Банка России* и *Выделенный удостоверяющий центр Банка России*. *Удостоверяющие центры кредитных организаций* – компоненты, обеспечивающие регистрацию и сертификацию ключей клиентов; *API ПЦР* – программный интерфейс, через который кредитные организации будут подключаться к ПЦР; API *кредитных организаций (API КО)* – программный интерфейс для взаимодействия кредитных организаций и клиентов; *Устройства пользователей* – мобильные приложения, предоставляемые КО своим клиентам.

Функционально архитектурный анализ позволил разработать базовую модель инфраструктуры доверия цифрового рубля (рис. 5).

Предложенная базовая модель позволила разработать инфраструктуру доверия в системе цифрового рубля, структурными элементами которой являются:

1. *Платформа цифрового рубля Банка России* (ПЦРБР) на которую возложены функции оператора ПЦР [12, 13].

2. *Участники (кредитные организации) и пользователи (клиенты) ПЦР,* которым представляется доступ к платформе и обеспечивается возможности для совершения операций с цифровыми рублями. Участники ПЦР должны вести административное сопро-

вождение (вести документацию), а также применять технологические меры защиты информации, используемых для контроля целостности, подтверждения подлинности и обеспечения конфиденциальности электронных сообщений на этапах их подготовки, обработки, передачи и хранения, и правила их применения, в том числе порядок применения СКЗИ.

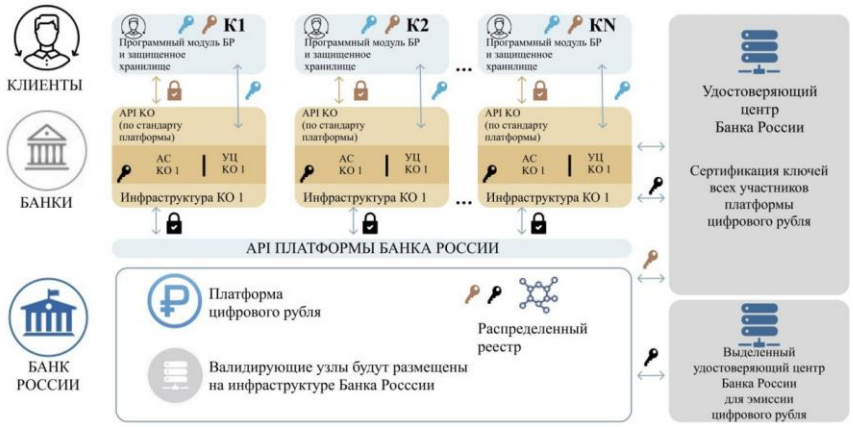

Рис. 5. Базовая модель инфраструктуры цифрового рубля [Банк России. Концепция цифрового рубля. С. 23]

3. *Инструменты,* обеспечивающие: открытие, ведение и закрытие счетов ЦР физических и юридических лиц; применение электронных денежных средств (ЭДС) и электронных средств платежа (ЭСП); перевод, пополнение счета и вывод средств со счета цифрового рубля.

4. *Механизмы контроля за соблюдением правил платформы*.

5. *Выполнение требований по инфраструктуре доверия к участникам ПЦР*, которые должны проводить оценку соответствия согласно следующим показателям: оценка соответствия должна проводиться в пределах выделенных сегментов (групп сегментов) вычислительных сетей в соответствии с требованиями Стандарта Российской Федерации ГОСТ Р 57580.2-2018, а также нормативных документов [14].

6. *Удостоверяющие центры кредитных организаций (УЦКО)* – обеспечивают регистрацию и сертификацию ключей клиентов. Например, в соответствие с Регламентом аккредитованного Удостоверяющего Центра АО «АЛЬФА-БАНК» определён порядок пользования такими ключами [15]. К их числу относятся: *ключ проверки электронной подписи* (предназначен для проверки подлинности электронной подписи); к*люч электронной подписи* (предназначен для создания электронной подписи); *сертификат ключа* проверки электронной подписи (Сертификат) – электронный документ, выданный УЦ для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа проверки электронной подписи; *список отозванных сертификатов* (СОС) – электронный документ с электронной подписью уполномоченного лица УЦ, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были аннулированы (отозваны); *средства УЦ* – сертифицированный ФСБ России программно-аппаратный комплекс «Удостоверяющий Центр «КриптоПро УЦ» версии 2.0 (ПАК «КриптоПро УЦ 2.0»), используемый для реализации функций удостоверяющего центра.

7. *API (прикладные программные приложения) Банка России и кредитных организаций.* Основу безопасности API составляет шифрование, под которым понимается преобразование исходных данных в зашифрованный вид, который должен быть расшифрован с помощью специального ключа. Выделяют два метода шифрования, а именно: симметричное и асимметричное. Например, симметричное шифрование предполагает использование одного ключа как для шифрования, так и для расшифрования. В этом случае, ис-

пользуется один ключ, этот метод отличается высокой скоростью работы и эффективностью, в то же время, это создает дополнительные риски при использовании в открытых сетях. Наиболее распространённые симметричные алгоритмы – AES (Advanced Encryption Standard), который является стандартом из-за своей устойчивости к криптоанализу, 3DES (Triple DES). Существует два основных типа такого вида шифрования: блочные и потоковые шифры. Упоминаемый выше AES является блочным шифром. Это означает, что он работает с блоками данных, и это обеспечивает более высокую криптографическую стойкость. В асимметричном шифровании используется два различных ключа: один из них – открытый, им информация шифруется, другой – закрытый, который используется для расшифрования сообщения. Российским аналогом является алгоритм Кузнечик (ГОСТ Р 34.12-2015), который применяется в национальных стандартах шифрования и обеспечивает высокий уровень защиты данных в финансовых учреждениях и государственных системах [16].

Криптографические методы применяются и в банковской сфере. Например, при совершении онлайн-платежей с использованием платежной система МИР, данные передаются через защищённые каналы с использованием протоколов TLS, которые позволяют обеспечить надежную и эффективную защиту информации. Решение процедур аутентификации и авторизации осуществляется на основе использования токенов доступа в целях управления сессиями и обеспечения безопасного доступа к ресурсам. Токены позволяют проверять подлинность пользователей без необходимости повторной авторизации при каждом запросе. Токены доступа делятся на несколько типов, наиболее распространённые из них – OAuth-токены и JWT (JSON Web Tokens). OAuth-токены используются для делегированной авторизации, при которой одно приложение может получать ограниченный доступ к ресурсам пользователя, находящимся на сервере другого приложения. Данная процедура применяется для интеграции сторонних сервисов, когда они могут выполнять операции от имени пользователя, но без доступа к его логину и паролю. Данная технология начинается с аутентификации пользователя на сервере авторизации, после чего выдается токен доступа, который клиент использует для взаимодействия с API. Российским аналогом в финансовой сфере является ГОСТ OAuth 2.0, который разрабатывается в рамках отечественных стандартов безопасности для защиты персональных данных при авторизации пользователей. JWT (JSON Web Tokens) – это компактные токены, в которых полезная нагрузка (payload) кодируется в формате JSON. Каждый такой токен содержит информацию о пользователе, его правах доступа, а также времени действия. Подпись токена выполняется с использованием как асимметричных, так и симметричных ключей, что позволяет убедиться в его подлинности и целостности.

Управление сессиями с использованием токенов доступа включает несколько ключевых аспектов. Во-первых, необходимо контролировать время жизни токенов. Если не ограничивать срок действия токенов, то существуют огромные риски компрометации. В то же время для выпуска нового токена необходимо повторное подтверждение пользователя, что повышает уровень безопасности. Во-вторых, важным аспектом является безопасное хранение токенов на клиентской стороне, так как злоумышленник не должен иметь возможности добраться до токенов, даже если получил доступ к устройству пользователя. Для этого необходимо использовать безопасные каналы связи (HTTPS, TLS 1.3) для передачи токенов, чтобы исключить возможность их перехвата злоумышленниками. В-третьих, если злоумышленник получил токен, необходимо иметь механизм его немедленного аннулирования. Для этого существуют чёрные списки (blacklists), при каждом запросе сервер проверяет, не входит ли полученный токен в список отозванных. Однако у этого метода есть серьезные недостатки: передача учетных данных в каждом запросе увеличивает риск их компрометации. Поэтому были разработаны более безопасные альтернативы, такие как аутентификация через API-ключи, которые представляют собой уникальные идентификаторы, выдаваемые клиентам для доступа к ресурсам API.

Дополнительную защиту API обеспечивает многофакторная аутентификация (MFA), при которой пользователь должен подтвердить свою личность несколькими способами (например, паролем и одноразовым кодом). Это значительно снижает вероят-

ность несанкционированного доступа, даже если злоумышленник получил учетные данные пользователя. OAuth 2.0 предоставляет возможность делегированной авторизации, разделяя процесс доступа на три компонента: Ресурсный сервер – хранит защищенные данные. Сервер авторизации – выдает токены доступа после успешной аутентификации. Клиент – запрашивает доступ к данным.

API активно используются в автоматизированных банковских системах (АБС) и системах дистанционного банковского обслуживания (ДБО). В АБС обеспечивается управление счетами, кредитами и платежами, а в ДБО пользователи взаимодействуют с банковскими сервисами через интернет и мобильные приложения. Надежность API-контроля в этих системах напрямую влияет на безопасность операций. Технология защиты и безопасности API включает четыре компонента: пользователь, клиент (запрашивает доступ), сервер авторизации (выдаёт токен), ресурсный сервер (предоставляет доступ при наличии токена). Эти элементы создают многослойную систему безопасности, в которой каждая роль строго определена, однако безопасность API зависит не только от их взаимодействия, но и от того, какие используются инструменты.

API Gateway играет важную роль в архитектуре API: он управляет потоком данных, организует маршруты запросов и защищает систему от угроз. Он принимает входящие запросы, проверяет их подлинность, маршрутизирует их к соответствующим ресурсам и возвращает ответы клиентам. В сущности, это интеллектуальный диспетчер, определяющий, куда направить каждый запрос, чтобы система работала эффективно.

Для безопасности API применяются различные инструменты: SAST (статический анализ); DAST (динамический анализ); IAST (интерактивное тестирование); Фаззинг.

По результатам сравнительного анализа можно сделать следующие выводы: SAST лучше всего подходит для ранних этапов разработки, когда важно обнаружить ошибки в коде до его развертывания. Он помогает находить логические уязвимости и проблемы в управлении памятью. DAST необходим для тестирования готовых API, он особенно полезен для анализа конфигурационных ошибок, утечек данных и проблем аутентификации. IAST нужен, когда важно понимать, как API ведёт себя в рабочей среде. Он даёт точную информацию о причинах уязвимостей и позволяет тестировать API во время его работы. Фаззинг применяется для поиска нестандартных уязвимостей, помогая выявлять неожиданные ошибки в обработке входных данных, отказоустойчивости API и механизмов защиты.

Лучший подход – это комбинация всех четырёх методов, например, на этапе разработки используется SAST для выявления ошибок ещё в коде. Перед релизом API проходит DAST, чтобы проверить безопасность в реальной среде. После развертывания применяется IAST, чтобы отслеживать динамическое поведение API и выявлять скрытые уязвимости. Фаззинг используется как дополнительный метод, позволяющий тестировать API на отказоустойчивость и выявление неожиданных уязвимостей, которые не обнаруживаются другими методами. Этот подход позволяет закрыть все возможные векторы атак, минимизировать риски и обеспечить надежную защиту API на всех этапах его жизненного цикла.

Процесс работы инструментов мониторинга API можно разделить на три этапа: *1 этап* – сбор данных. Инструменты анализируют входящий трафик, фиксируют все запросы и сравнивают их с нормальным поведением пользователей. *2 этап* – выявление аномалий. Любые отклонения от стандартных моделей поведения – резкое увеличение числа запросов, аномальные значения параметров, использование устаревших методов API – попадают в категорию подозрительных. *3 этап* – автоматическое реагирование. В зависимости от настроек система может отправлять уведомления администратору, блокировать подозрительный трафик, требовать дополнительной аутентификации или временно ограничивать доступ для конкретного IP-адреса.

Шифрование и механизмы токенизации остаются основой защиты API, но их эффективность зависит не только от используемых алгоритмов, но и от того, насколько грамотно они реализованы. Утечки данных происходят не из-за слабости криптографии, а из-за ошибок в её применении. Неправильное хранение ключей, устаревшие методы шифрования, утечки токенов или их повторное использование – всё это превращает даже самые защищённые API в уязвимые точки атаки.

В целях защиты и безопасности API в России действуют стандарты для финансовых API. Например, Приказ ФСТЭК № 17 определяет требования к защите информации в государственных и корпоративных системах [17], Приказ ФСТЭК № 21 регулирует вопросы безопасности государственных информационных систем, включая требования к API, используемым в электронном документообороте [18]. В финансовом секторе также применяются требования ФСБ РФ, в частности Приказ № 378, который касается использования средств криптографической защиты информации (СКЗИ) при передаче данных через API [19]. ГОСТ Р 57580.1-2017 обязывает компании в банковской сфере проводить сертификацию API перед запуском в эксплуатацию, используя сертифицированные средства криптографической защиты информации [20]. Организации должны внедрять системы обнаружения аномалий в API-трафике и анализировать аутентификацию пользователей на предмет аномального поведения.

Заключение и предложения. Формирование инфраструктуры доверия цифрового рубля осуществляется на основе соблюдения комплекса мер по обеспечению ее безопасности, включающей:

1. *Безопасность допуска участников и пользователей к инфраструктуре цифрового рубля:* Взаимодействие клиента с платформой цифрового рубля осуществляется по защищенным каналам через приложение банка, установленное на мобильное устройство пользователя. Доступ пользователя к кошельку, на котором хранятся его цифровые рубли, а также все операции пользователя с цифровым рублем осуществляются с использованием специализированного программного модуля Банка России, интегрированного с мобильными приложениями кредитных организаций. Программный модуль БР разрабатывается Банком России и будет предоставлять API для разработчиков приложений кредитных организаций и использоваться для: обеспечения безопасного взаимодействия пользователя с банком; генерации и хранения криптографического ключа доступа клиента кредитной организации к цифровому кошельку; подписания распоряжений по операциям с цифровыми рублями клиента. Криптографическая защита каналов взаимодействия пользователей с инфраструктурой кредитной организации (шифрование) при использовании мобильного приложения кредитной организации осуществляется с применением СКЗИ, сертифицированных ФСБ России.

2. *Безопасность доступа кредитной организации к платформе цифрового рубля:* при доступе к платформе цифрового рубля осуществляется «строгая» двухсторонняя аутентификация прямых участников с использованием ключей, сертифицированных УЦБР, по защищенным каналам взаимодействия, реализованным с применением сертифицированных ФСБ России СКЗИ.

3. *Безопасность по защите данных на платформе цифрового рубля:* Применение СКЗИ, сертифицированных ФСБ России, для обеспечения целостности и достоверности данных на платформе Банка России при подписании транзакций с цифровым рублем. Создание цифровых рублей исключительно с применением эмиссионного ключа Банка России. Эмиссионный ключ Банка России регистрируется в специально выделенном УЦ Банка России для эмиссии. Применение комплекса технологических мер защиты информации (логический контроль, структурный контроль, контроль дублирования, контроль авторства и так далее). На участках, где невозможно применение сертифицированных СКЗИ, предусмотрено применение специальных технологических мер, обеспечивающих целостность данных для операций с цифровым рублем. Организация контроля целостности «смарт-контрактов» и прав доступа к возможности их запуска.

4. *Безопасность конфиденциальности на платформе цифрового рубля* предусматривает меры по обеспечению безопасности, такие как: об операциях клиентов и защите их персональных данных, а также процедур, предусмотренных законодательством в сфере ПОД/ФТ/ФРОМУ. В этом смысле степень конфиденциальности операций на платформе цифрового рубля будет обеспечена на уровне не ниже, чем при существующем механизме безналичных платежей.

Банком России определён порядок подключения участника платформы к платформе цифрового рубля [21, 22], предусматривая следующую последовательность: процедуру проведения тестовых испытаний взаимодействия; регламент взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платфор-

мы Цифрового рубля; платформа цифрового рубля и правила заполнения полей сертификатов; стандарт платформы цифрового рубля «Требования и рекомендации к пользовательским интерфейсам при совершении операций с цифровым рублем».

Предложения по набору работ, связанных с внедрением инфраструктуры доверия системы цифрового рубля.

Минимальный и оптимальный набор работ:

1. *Удостоверяющие центры (УЦ), средства защиты информации (СЗИ), средства криптографической защиты информации (СКЗИ):*

- проектирование архитектуры решения и разработка проектной и эксплуатационной документации;
- монтаж серверов и автоматизированных рабочих мест (АРМ) обслуживающего персонала, настройка и конфигурация операционной системы (ОС);
- развёртывание и конфигурация Удостоверяющих Центров (включая HSM и сервер точного времени);
- установка и настройка средств защиты информации и средств критической защиты информации на серверах;
- установка и настройка межсетевых экранов, коммутаторов и TLS-шлюзов;
- разработка организационно-распорядительной документации;
- установка решения для автоматизации выпуска сертификатов;
- установка и настройка решения для мониторинга работоспособности Удостоверяющих Центров.

2. *Автоматизация банковской системы (АБС), дистанционное банковское обслуживание (ДБО), Мобильное приложение:*

- развёртывание решения для взаимодействия с платформой цифрового рубля (Контур контроля и контур обработки);
- доработка автоматизированной банковской системы (квитовка платежей (ED101), изменение статуса и баланса цифрового рубля клиента, изменение реквизитов клиента, проверки ПОД / ФТ и проверки АБС, бух. учет по новым счетам 30502-30504;
- API для дистанционного банковского обслуживания физических и юридических лиц;
- доработка дистанционного банковского обслуживания физических и юридических лиц (ПМ БР, экраны для веб-клиента, интеграция с АБС).

3. *Интеграция с единой системой идентификации и аутентификации информационного (ЕСИА) и системы быстрых платежей (СБП):*

- встраивание программного модуля Банка России (ПМБР) в мобильное приложение (при наличии мобильного приложения).

4. *Оценка и аудит:*

- оценка влияния для ПМ БР в мобильное приложение;
- оценка влияния для контура контроля и контура обработки;
- аудит на соответствие ГОСТ Р 57580.1-2017;
- аудит на соответствие для дистанционного банковского обслуживания и программного обеспечения в контуре контроля и контуре обработки;
- оценка влияния для решения автоматизации выпуска сертификатов[1].

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

[1] *График подключения к платформе*: Крупнейшие банки к 1 июля 2025 года должны будут обеспечить своим клиентам возможность проводить операции с цифровыми рублями. Остальным банкам с универсальной лицензией предоставляется больше времени на доработку своих систем – до 1 июля 2026 года, прочим кредитным организациям – до 1 июля 2027 года. Планируется установить сроки обязательного приема оплаты в цифровых рублях для торговых и сервисных предприятий (ТСП). Компании с годовой выручкой более 30 млн рублей должны будут это делать с 1 июля 2025 года, более 20 млн рублей – с 1 июля 2026 года, все другие – с 1 июля 2027 года [https://www.cbr.ru/fintech/dr/].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://blog.eldorado.ru/publications/chto-takoe-tsifrovoy-rubl-prostymi-slovami-komu-i-zachem-on-neobkhodim-36739.
2. https://media.halvacard.ru/financial-literacy/chto-takoe-cifrovoi-rubl-i-dlya-chego-on-nuzhen.
3. *Осипова В.С.* Безопасность цифрового рубля // Экономические науки. – 2024. – № 7 (236).
4. *Саадулаева Т.А., Шляхтина И.А.* Цифровой рубль как механизм обеспечения финансовой безопасности государства // Экономика и бизнес: теория и практика. – 2022. – № 13. – С. 111-116.
5. *Королёв В.И.* Архитектурное построение инфраструктуры открытых ключей интегрированного информационного пространства // Безопасность информационных технологий. – 2015. – Т. 22, № 3.
6. *Мельников Д.А.* Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем: автореф. дисс. … д-ра техн. наук. – М., 2022.
7. *Грачков И.А., Малюк А.А.* Проблемы разработки доверенного программного обеспечения, применяемого на объектах критической информационной инфраструктуры (организационные и методические аспекты) // Безопасность информационных технологий. – 2019. – Р. 56-63.
8. *Мельников Д.А. и др.* Рекомендации по созданию инфраструктуры доверия системы цифрового рубля // Безопасность информационных технологий. – 2024. – Т. 31, № 3. – С. 43-63.
9. Концепция цифрового рубля. Банк России. – 2021. – С. 9-10. – https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf.
10. *Шашурина Ирина*. – https://in4security.com/news/tpost/jpmmfiab51-chto-nuzhno-znat-o-novih-standartah-bezo?ysclid=m7c1y7gk5404288694.
11. Положение Центрального Банка Российской Федерации от 3 августа 2023 года № 820-П «О платформе цифрового рубля». (В ред. указания ЦБ РФ от 12.07.2024 N 6804-У).
12. Указание ЦБ РФ от 12.07.2024 N 6804-У.
13. Положение Банка России от 7 декабря 2023 г. № 833-п «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля».
14. Положение ПКЗ-2005, утвержденное приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года N 66 Зарегистрирован Минюстом России 3 марта 2005 года, регистрационный N 6382, с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 года N 173 (зарегистрирован Минюстом России 25 мая 2010 года, регистрационный N 17350); Приказ Федеральной службы безопасности Российской Федерации от 27 декабря 2011 года N 796; Положение Банка России от 7 декабря 2023 г. № 833-п «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля».
15. Регламент аккредитованного Удостоверяющего Центра АО «АЛЬФА-БАНК». Версия 3.0 от 27.04.2021 г. Приложение к Приказу № 519 от 27.04.2021.
16. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Блочные шифры. ГОСТ Р 34.12─2015.
17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК от 11 февраля 2013 г. N 17.
18. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК от 18 февраля 2013 г. N 21.
19. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности. Приказ ФСБ России от 10 июля 2014 г. N 378.
20. ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер". Утверждён Приказом Росстандарта от 08.08.2017 N 822-ст.
21. Концепция цифрового рубля. Банк России. 2021.
22. Стандарт платформы цифрового рубля «Порядок подключения участника платформы к платформе цифрового рубля» Версия 1.3.

REFERENCES

1. Available at: https://blog.eldorado.ru/publications/chto-takoe-tsifrovoy-rubl-prostymi-slovami-komu-i-zachem-on-neobkhodim-36739.
2. Available at: https://media.halvacard.ru/financial-literacy/chto-takoe-cifrovoi-rubl-i-dlya-chego-on-nuzhen.

3. *Osipova V.S.* Bezopasnost' tsifrovogo rublya [Security of the digital ruble], *Ekonomicheskie nauki* [Economic sciences], 2024, No. 7 (236).
4. *Saadulaeva T.A., Shlyakhtina I.A.* Tsifrovoy rubl' kak mekhanizm obespecheniya finansovoy bezopasnosti gosudarstva [Digital ruble as a mechanism for ensuring the financial security of the state], *Ekonomika i biznes: teoriya i praktika* [Economy and business: theory and practice], 2022, No. 13, pp. 111-116.
5. *Korolev V.I.* Arkhitekturnoe postroenie infrastruktury otkrytykh klyuchey integrirovannogo informatsionnogo prostranstva [Architectural construction of the public key infrastructure of the integrated information space], *Bezopasnost' informatsionnykh tekhnologiy* [Security of Information], 2015, Vol. 22, No. 3.
6. *Mel'nikov D.A.* Metody i sredstva postroeniya sistemy upravleniya kriptograficheskoy zashchitoy na osnove infrastruktury otkrytykh klyuchey dlya shirokomasshtabnykh informatsionno-telekommunikatsionnykh sistem: avtoref. diss. … d-ra tekhn. nauk [Methods and means of constructing a cryptographic protection management system based on the public key infrastructure for large-scale information and telecommunication systems: abstract of dr. of eng. sc. diss.]. Moscow, 2022.
7. *Grachkov I.A., Malyuk A.A.* Problemy razrabotki doverennogo programmnogo obespecheniya, primenyaemogo na ob"ektakh kriticheskoy informatsionnoy infrastruktury (organizatsionnye i metodicheskie aspekty) [Problems of developing trusted software used at critical information infrastructure facilities (organizational and methodological aspects)], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], 2019, pp. 56-63.
8. *Mel'nikov D.A. i dr.* Rekomendatsii po sozdaniyu infrastruktury doveriya sistemy tsifrovogo rublya [Recommendations for creating a trust infrastructure for the digital ruble system], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], 2024, Vol. 31, No. 3, pp. 43-63.
9. Kontseptsiya tsifrovogo rublya. Bank Rossii [The concept of the digital ruble. Bank of Russia], 2021, pp. 9-10. Available at: https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf.
10. *Shashurina Irina.* Available at: https://in4security.com/news/tpost/jpmmfiab51-chto-nuzhno-znat-o-novih-standartah-bezo?ysclid=m7c1y7gk5404288694.
11. Polozhenie TSentral'nogo Banka Rossiyskoy Federatsii ot 3 avgusta 2023 goda № 820-P «O platforme tsifrovogo rublya» [Regulation of the Central Bank of the Russian Federation dated August 3, 2023 No. 820-P "On the Digital Ruble Platform"]. (As amended by Bank of Russia Instruction dated July 12, 2024 No. 6804-U).
12. Ukazanie TsB RF ot 12.07.2024 N 6804-U [Instruction of the Central Bank of the Russian Federation dated July 12, 2024 No. 6804-U].
13. Polozhenie Banka Rossii ot 7 dekabrya 2023 g. № 833-p «O trebovaniyakh k obespecheniyu zashchity informatsii dlya uchastnikov platformy tsifrovogo rublya» [Regulation of the Bank of Russia dated December 7, 2023 No. 833-p "On the Requirements for Ensuring Information Security for Participants of the Digital Ruble Platform"].
14. Polozhenie PKZ-2005, utverzhdennoe prikazom Federal'noy sluzhby bezopasnosti Rossiyskoy Federatsii ot 9 fevralya 2005 goda N 66 Zaregistrirovan Minyustom Rossii 3 marta 2005 goda, registratsionnyy N 6382, s izmeneniyami, vnesennymi prikazom FSB Rossii ot 12 aprelya 2010 goda N 173 (zaregistrirovan Minyustom Rossii 25 maya 2010 goda, registratsionnyy N 17350); Prikaz Federal'noy sluzhby bezopasnosti Rossiyskoy Federatsii ot 27 dekabrya 2011 goda N 796; Polozhenie Banka Rossii ot 7 dekabrya 2023 g. № 833-p «O trebovaniyakh k obespecheniyu zashchity informatsii dlya uchastnikov platformy tsifrovogo rublya» [Regulation PKZ-2005, approved by the order of the Federal Security Service of the Russian Federation dated February 9, 2005 N 66 Registered by the Ministry of Justice of Russia on March 3, 2005, registration N 6382, with amendments introduced by the order of the FSB of Russia dated April 12, 2010 N 173 (registered by the Ministry of Justice of Russia on May 25, 2010, registration N 17350); Order of the Federal Security Service of the Russian Federation dated December 27, 2011 N 796; Regulation of the Bank of Russia dated December 7, 2023 N 833-p "On the requirements for ensuring the protection of information for participants in the digital ruble platform"].
15. Reglament akkreditovannogo Udostoveryayushchego TSentra AO «AL'FA-BANK». Versiya 3.0 ot 27.04.2021 g. Prilozhenie k Prikazu № 519 ot 27.04.2021 [Regulations of the accredited Certification Authority of ALFA-BANK JSC. Version 3.0 dated 04/27/2021. Appendix to Order No. 519 dated 04/27/2021].
16. Natsional'nyy standart Rossiyskoy Federatsii. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry. GOST R 34.12─2015 [National standard of the Russian Federation. Information technology. Cryptographic protection of information. Block ciphers. GOST R 34.12-2015].

17. Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh. Prikaz FSTEK ot 11 fevralya 2013 g. N 17 [On approval of requirements for the protection of information that does not constitute a state secret, contained in state information systems. Order of the FSTEC dated February 11, 2013 N 17].
18. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. Prikaz FSTEK ot 18 fevralya 2013 g. N 21 [On approval of the composition and content of organizational and technical measures to ensure the security of personal data when processing them in personal data information systems. Order of the FSTEC of February 18, 2013 N 21].
19. Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh s ispol'zovaniem sredstv kriptograficheskoy zashchity informatsii, neobkhodimykh dlya vypolneniya ustanovlennykh Pravitel'stvom Rossiyskoy Federatsii trebovaniy k zashchite personal'nykh dannykh dlya kazhdogo iz urovney zashchishchennosti. Prikaz FSB Rossii ot 10 iyulya 2014 g. N 378 [On approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data when Processing them in Personal Data Information Systems Using Cryptographic Information Protection Means Necessary to Meet the Requirements for the Protection of Personal Data for Each of the Security Levels Established by the Government of the Russian Federation. Order of the FSB of Russia of July 10, 2014 N 378].
20. GOST R 57580.1-2017. Natsional'nyy standart Rossiyskoy Federatsii. Bezopasnost' finansovykh (bankovskikh) operatsiy. Zashchita informatsii finansovykh organizatsiy. Bazovyy sostav organizatsionnykh i tekhnicheskikh mer". Utverzhden Prikazom Rosstandarta ot 08.08.2017 N 822-st. [GOST R 57580.1-2017. National standard of the Russian Federation. Security of financial (banking) transactions. Protection of information of financial organizations. Basic composition of organizational and technical measures". Approved by Order of Rosstandart dated 08.08.2017 N 822-st.].
21. Kontseptsiya tsifrovogo rublya. Bank Rossii. 2021 [Concept of the digital ruble. Bank of Russia. 2021].
22. Standart platformy tsifrovogo rublya «Poryadok podklyucheniya uchastnika platformy k platforme tsifrovogo rublya» Versiya 1.3 [Digital ruble platform standard "Procedure for connecting a platform participant to the digital ruble platform" Version 1.3].

Иванов Анатолий Викторович – Финансовый университет при Правительстве Российской Федерации; e-mail: aivanov@fa.ru; г. Москва, Россия; главный научный сотрудник Института цифровых технологий; д. социол. н.; профессор.

Царегородцев Анатолий Валерьевич – Финансовый университет при Правительстве Российской Федерации; e-mail: anvtsaregorodtsev@fa.ru; г. Москва, Россия; главный научный сотрудник Института цифровых технологий; д.т.н.; профессор.

Валеев Михаил Владимирович – Финансовый университет при Правительстве Российской Федерации; e-mail: waleew.miha@hotmail.com; г. Москва, Россия; младший научный сотрудник Института цифровых технологий.

Ivanov Anatoly Viktorovich – Financial University under the Government of the Russian Federation; e-mail: aivanov@fa.ru; Moscow, Russia; chief researcher at the Institute of Digital Technologies; dr. of social. sc.; professor.

Tsaregorodtsev Anatoly Valerievich – Financial University under the Government of the Russian Federation; e-mail: anvtsaregorodtsev@fa.ru; Moscow, Russia; chief researcher at the Institute of Digital Technologies; dr. of eng. sc.; professor.

Valeev Mikhail Vladimirovich – Financial University under the Government of the Russian Federation; e-mail: waleew.miha@hotmail.com; Moscow, Russia; junior research fellow at the Institute of Digital Technologies.