Научная статья
https://doi.org/10.24412/2220-2404-2025-11-9
УДК 342.7

МНОГОКОМПОНЕНТНАЯ ЗАЩИТА ДАННЫХ ЦИФРОВЫХ ВАЛЮТ ЦЕНТРАЛЬНЫХ БАНКОВ: ИНТЕГРАЦИЯ ПРАВОВЫХ И ТЕХНОЛОГИЧЕСКИХ ПОДХОДОВ

Карпенко И.Н.
Финансовый университет при Правительстве РФ

Аннотация *Данное исследование направлено на преодоление правового дисбаланса между обеспечением конфиденциальности операций с цифровыми валютами центральных банков (далее – ЦВЦБ) и соблюдением режима противодействия отмыванию денег и финансирования терроризма (далее – ПОД/ФТ). В статье представлена многокомпонентная система защиты данных ЦВЦБ, разработанная на основе сравнительного анализа международных рекомендаций и правовых подходов ведущих юрисдикций к защите данных. Она реализуется посредством регулирования режимов доступа участников экосистемы: центральных банков, контролируемых финансовых организаций, органов по борьбе с отмыванием денег, других уполномоченных органов – к данным конечных пользователей. Разработанная система интегрирует три оригинальных компонента: иерархическую модель конфиденциальности, криптографический прокол разделенного доступа и механизм динамического согласия. Для практического внедрения предложенной Системы защиты данных ЦВЦБ требуется ее нормативное закрепление посредством подзаконных актов, в том числе в форме комплексной матрицы режимов доступа.*

Ключевые слова*: конфиденциальность, защита данных, цифровые валюты центральных банков, ЦВЦБ, режим доступа, ПОД/ФТ, пороговые значения транзакций, криптографический протокол, динамическое согласие, матрица доступа.*

Финансирование: *инициативная работа.*

Original article.

A MULTICOMPONENT DATA PROTECTION SYSTEM IN CENTRAL BANK FOR DIGITAL CURRENCIES: INTEGRATION OF LEGAL AND TECHNOLOGICAL APPROACHES

Irina N. Karpenko
Financial University under the Government of the Russian Federation

Abstract. *This study aims to address the legal imbalance between safeguarding the privacy of Central Bank Digital Currency (CBDC) transactions and complying with anti–money laundering and counter-terrorism financing (AML/CFT) requirements. The paper presents a multicomponent data protection system for CBDCs, developed through a comparative analysis of international recommendations and the legal approaches of leading jurisdictions to data protection. It is implemented by regulating the access regimes of ecosystem participant s— central banks, supervised financial institutions, anti-money laundering authorities, and other authorized bodies — to end-user data. The proposed system integrates three original components: the hierarchical privacy model, the cryptographic split-access protocol, and the dynamic consent mechanism. For practical deployment of the suggested data protection system in CBDCs, its codification through subordinate legislation is required, including the adoption of a comprehensive access matrix.*

Keywords: *Privacy, data protection, central bank digital currencies, CBDC, access regime, AML/CFT, transaction threshold values, cryptographic protocol, dynamic consent, access matrix.*

Funding: *Independent work.*

Введение.

Широкое внедрение цифровых валют центральных банков обостряет проблему защиты конфиденциальности. Сама их структура генерирует «цифровой след», включающий огромный объем персональных данных. Это создает фундаментальное противоречие между использованием этих данных неограниченным кругом субъектов для достижения неограниченного количества целей и обеспечением конфиденциальности [1, с. 1-2].

Согласно докладу Банка международных расчетов (далее – БМР), национальным юрисдикциям необходимо совершенствовать свои правовые базы, затрагивающие ЦВЦБ, для достижения оптимального баланса между конфиденциальностью и предотвращением финансовых преступлений [2, с. 2-3]. В число связанных с этим задач входит решение ключевого вопроса национальной политики о режиме доступа к данным, включенным в ЦВЦБ [3, с. 6], чему и посвящена данная статья.

В качестве источников для исследования были использованы:

- нормативные правовые документы ряда ведущих юрисдикций;

- отчеты авторитетных международных организаций;

- научные работы, опубликованные в ведущих юридических журналах.

Среди авторов статей по конфиденциальности ЦВЦБ можно выделить Auer R., Ballaschk D., Chen P.-K., Haene P., Holden H., Jiang J., Kaur G., Paulick J., Pocher N., Rennie E., Steele S., Tsang C.-Y., Veneris A. и др.

Методология исследования включает три метода. Первый – метод классификации, примененный для создания многомерной таксономии данных и иерархической модели конфиденциальности; второй – технико-юридический метод, использованный для разработки криптографического протокола разделенного доступа; третий – сравнительно-правовой анализ, проведенный для выявления различия парадигм конфиденциальности в разных юрисдикциях.

Вклад автора состоит в предложении многокомпонентной системы защиты данных, выходящей за рамки существующих подходов к обеспечению конфиденциальности национальных цифровых валют в мировых юрисдикциях.

Результаты.

Сравнительный анализ юрисдикционных подходов.

Сравнительно-правовой анализ методов обеспечения конфиденциальности данных ЦВЦБ, показывает, что в отсутствие специального законодательства ведущие юрисдикции демонстрируют правовое регулирование, ориентированное на принципы.

Так, Европейский союз реализует подход, основанный на принципах «конфиденциальности по умолчанию» и «проектируемой конфиденциальности», то есть конфиденциальности, изначально предусмотренной в архитектуре цифрового евро и реализуемой автоматически, без необходимости действий со стороны пользователя. Данные принципы установлены ст.25 GDPR [4].

Подход США можно назвать основанным на принципах «процедурной конфиденциальности» и «опосредованной конфиденциальности». Система США опирается на конституционную защиту от необоснованного доступа к личной жизни. Степень конфиденциальности при этом отражает развитие судебной практики, основанной на Поправке IV к Конституции США о неприкосновенности личности [5].

Правовой подход КНР в обеспечении конфиденциальности электронного юаня, основан на принципе «контролируемой»/«управляемой» конфиденциальности [6]. Многоуровневая структура электронного кошелька реализует разную приватность для разных типов кошельков. Использование смарт-контрактов обеспечивает программируемый характер, что означает прозрачность данных для регулирующих органов и конфиденциальность для коммерческих структур [7].

Многомерная таксономия данных ЦВЦБ.

Разработанная автором на основе академических источников таксономия устанавливает пять категорий данных ЦВЦБ, каждая из которых требует отдельного правового режима в соответствии с международными стандартами конфиденциальности и особенностями правового подхода юрисдикций.

1. Идентификационные данные включают персональные данные, включая биометрические идентификаторы, а также метки устройств, необходимые для аутентификации пользователей.

2. Данные о транзакциях включают операционную информацию, в том числе суммы, временные метки и идентификаторы контрагентов.

3. Поведенческие данные представляют собой алгоритмические производные от данных транзакций, включая анализ скорости расходования средств и историю транзакций.

4. Метаданные включают системные журналы, геолокацию, технические идентификаторы (IP-адреса устройств, MAC-адреса, данные об устройстве).

5. Производные данные включают оценки риска и агрегированные статистические показатели, полученные с помощью аналитических методов, которые обеспечивают сохранение конфиденциальности.

Иерархическая модель конфиденциальности.

Многомерная таксономия данных легла в основу разработки многокомпонентной системы защиты данных ЦВЦБ, включающей три оригинальных технико-правовых механизма, предназначенных для регулирования режимов доступа участников экосистемы к данным ЦВЦБ.

Первым компонентом созданной системы является иерархическая модель конфиденциальности, интегрирующая две подсистемы.

Первая подсистема – это структура уровней чувствительности данных, применяемая для определения важности содержащейся в них информации:

– уровень 0: Публичные данные – агрегированные статистические данные, обработанные с применением дифференцированная приватности, подходящие для исполнения обязательств центрального банка по обеспечению прозрачности;

– уровень 1: Псевдонимизированные данные, полученные заменой идентификаторов на криптографические хэши, что ведет к минимальному риску повторной идентификации. Данные используются для анализа и исследований;

– уровень 2: Зашифрованные данные, преобразованные в нашем случае с помощью пороговой схемы шифрования. Используются для защиты данных транзакций. Расшифровываются применением криптографического протокола.

– уровень 3: Данные специальной категории – персональные данные, подлежащие обработке только с явного согласия пользователя при соблюдении строгих условий, например, в соответствии со ст. 9 GDPR [4]. Для получения оперативного согласия предлагается Механизм динамического согласия.

– уровень 4: Особо защищенные данные – это данные, сбор и обработка которых запрещены, например, касающиеся государственной безопасности.

Вторая подсистема – структура уровней пороговых значений сумм транзакций, включает шкалу риска при операциях с ЦВЦБ. На ее основе определяется интенсивность контрольных мер. Диапазоны пороговых значений зависят прежде всего от особенностей правового подхода юрисдикций.

Пример уровней пороговых значений транзакций с ЦВЦБ:

– уровень 1 – микроплатежи (до 50 евро за транзакцию, до 150 евро в день): анонимность, отсутствие контроля;

– уровень 2 – розничные платежи: а) от 50 до 300; б) от 300 до 1000 евро).

Подуровни а) и б) отличаются строгостью процедур проверки «Знай своего клиента». Доступ правоохранительных органов к данным предоставляется в рамках расследования уголовного дела по судебному ордеру;

– уровень 3 – подозрительные платежи (от 1000 долларов/евро), полная прозрачность, для ЕС – обработка в соответствии с требованиями 6-й Директивы о борьбе с отмыванием денег.

Криптографический протокол разделенного доступа.

Протокол предоставляет доступ к данным транзакций с ЦВЦБ при подозрении на ОД/ФТ и отсутствии возбужденного уголовного дела. Для расшифровки необходимо выполнение криптографических условий всеми (тремя) сторонами, получившими независимые криптографические ключи:

– ключ ЦБ используется в рамках функций по контролю за выполнением другими уполномоченными органами предписанных мер защиты данных;

– ключ надзорного органа обеспечивает соблюдение требований регуляторов в области персональных данных;

– ключ судебного органа применяется для предусмотренного в исключительных случаях санкционирования судом дешифрования персональных данных.

Механизм динамического согласия.

Третий элемент многокомпонентной системы защиты данных – технико-юридический механизм динамического согласия. Он обеспечивает улучшенное управление субъектом данных своим согласием, реализуемое через использование смарт-контрактов. Это отвечает требованиям предметного, простого в интерфейсе, действующего в режиме реального времени согласия, в случае ЕС – требованиям, закрепленным в статье 7 GDPR [4]. Кроме того, механизм реализует автоматическое информирование пользователя об изменениях в условиях обработки персональных данных, а также об автоматической приостановке действия механизма согласия в случаях, предусмотренных действующим законодательством, в том числе для осуществления мер ПОД/ФТ при совершении подозрительных операций.

Принципы предлагаемого подхода для закрепления в законодательстве.

Предлагаются следующие принципы правового регулирования, обеспечивающие реализацию многокомпонентной системы защиты данных.

Первый – это принцип иерархической минимизации доступа, реализуемый через иерархическую модель конфиденциальности. Персональные данные получают прозрачность только при наличии обоснованного подозрения на финансовые правонарушения и при превышении пороговых значений сумм транзакций.

Второй принцип – это положение о разделении властей на криптографическом уровне. Каждый уполномоченный орган получает свой независимый криптографический ключ в рамках осуществления своих полномочий. Доступ к данным становится возможным только при коллективном согласии.

Третий принцип – положение о динамическом управлении согласием в режиме реального времени, которое в техническом плане предлагается реализовать посредством смарт-контрактов. Такой принцип включает как право субъекта на немедленный отзыв своего согласия, так и его приостановку в условиях совершения субъектом высокорисковых финансовых операций.

Предлагаемые принципы повышения конфиденциальности позволят усовершенствовать нормативно-правовую базу регулирования ЦВЦБ в различных юрисдикциях при соблюдении регуляторных требований.

Комплексная матрица режимов доступа.

Разработанная многокомпонентная система защиты данных ЦВЦБ получает свое практическое воплощение в комплексной матрице режимов доступа. В таблице 1 предлагается фрагмент возможного варианта матрицы на примере ЕС.

Таблица 1 – Комплексная матрица режимов доступа.

Заинтересованная сторона	**Тип данных**	**Цель использования**	**Уровень доступа**	**Срок хранения**	**Правовые основания**	**Технический механизм**	**Требования к аудиту**
ЕЦБ/Национальные ЦБ	Агрегированные данные	Денежно-кредитная политика	Только к агрегирован-ным данным	Постоянно	Договор о функционировании ЕС (*TFEU*), ст. 127	*API* с дифференци-альной конфиденциальностью	Ежеквартальный обзор
Коммер-ческие банки	Персональные данные своих клиентов	Предоставление услуг	К идентифици-рованным данным своих клиен-	5 лет, возможно до 7 лет	Регламент о регулировании рынка криптоактивов (*MiCA*), ст. 68	Процедура «Знай своего клиента» (*KYS*)	Ежегодная проверка
Финансовая разведка	Подозрительные транзакции	Расследование	К типу данных, обозначен-ному в мотивированном запросе	В ходе расследования	Шестая директива ЕС по борьбе с отмыванием денег (*6AMLD*), ст. 21	Криптографический протокол	По каждому доступу

Обсуждение и выводы

Теоретические аспекты

Данное исследование вносит вклад в теорию финансово-правового регулирования внедрения и оборота ЦВЦБ в мировых юрисдикциях посредством трех нововведений. Во-первых, исследование адаптирует теорию контекстной целостности Хелен Ниссенбаум к ЦВЦБ. Исследование показывает, что угрозы нарушения конфиденциальности заключаются не в самом сборе данных, а в ненадлежащей передаче информации между участниками экосистемы ЦВЦБ, связанной с отсутствием норм режима доступа к данным. В иерархической модели конфиденциальности теоретические принципы теории Хелен Ниссенбаум трансформируются в практические принципы иерархической минимизации доступа. Авторская разработка позволяет привести информационные потоки транзакционных данных ЦВЦБ в соответствие с правовыми нормами.

Во-вторых, исследование демонстрирует возможность преодоления ключевого парадокса ЦВЦБ: противоречия между соблюдением конфиденциальности и выполнением регуляторных требований. В трехключевой криптографической системе управления полномочиями для получения доступа к идентификационным данным необходимо согласие всех участников трипартитного контроля. Это позволяет обеспечить баланс между защитой прав субъектов, данных и исполнением регуляторных требований, включая рекомендации ФАТФ.

В-третьих, исследование предлагает новую правовую структуру – механизм динамического согласия, реализуемый через смарт-контракты. Его внедрение направлено на устранение несоответствия инерционности традиционных моделей получения согласия субъекта на обработку данных операционной скорости транзакций в ЦВЦБ, предотвращая риски нарушения прав субъектов данных.

Практические выводы

Практическое значение исследования проявляется в четырех направлениях:

– для регуляторов: исследование представляет предложения по внесению изменений в типовое законодательство, повышающие конфиденциальность ЦВЦБ при соответствии требованиям ПОД/ФТ ФАТФ;

– для центральных банков: исследование позволяет преодолеть «трилемму» ЦВЦБ, одновременно решая задачи соблюдения конфиденциальности (анонимность и полупрозрачность при небольших и средних суммах транзакций), соблюдения нормативных требований (проведение стандартных процедур KYS при средних суммах и полных при подозрительных транзакциях) и обеспечения финансовой стабильности через макроанализ данных ЦВЦБ и контроль денежных потоков;

– для финансовых организаций: предлагаемые автоматизированные механизмы обеспечения соответствия регуляторным требованиям снижают операционные расходы для низкорисковых транзакций, сохраняя при этом возможности выполнения требований ПОД/ФТ;

– для граждан: комплекс криптографических решений гарантирует полную анонимность транзакций для небольших сумм транзакций; ограничение доступа к данным для средних сумм. Исключениями являются раскрытие информации по судебному ордеру в рамках уголовного дела и по коллективному согласию

ЦБ и надзорного органа с санкцией суда – в случае подозрительных операций.

Будущие направления исследований

Полагаем, что три критически важных области требуют дальнейшего изучения:

Во-первых, необходимой является интеграция квантово-устойчивых криптографических протоколов, так как квантовые вычисления угрожают существующим стандартам шифрования, в том числе и в предлагаемом криптографическом протоколе разделенного доступа.

Во-вторых, проведение поведенческих исследований, изучающих реакцию пользователей на предлагаемые уровни сумм транзакций в иерархической модели конфиденциальности, позволит оптимизировать настройки пороговых значений и своевременную корректировку конфигурации.

В-третьих, необходима разработка международных автоматизированных механизмов динамического согласия при переносе данных ЦВЦБ в условиях трансграничного взаимодействия.

Заключение

Данное исследование направлено на устранение пробела в регулировании ЦВЦБ в мировых юрисдикциях – недостатка технико-правовых механизмов, эффективно обеспечивающих баланс между защитой конфиденциальности и регуляторными требованиями. В нашем исследовании для решения этой проблемы предлагается многокомпонентная система защиты данных.

Комплексная матрица режимов доступа позволяет перевести теоретические разработки в практическую плоскость, определяя точные типы данных, цели и уровни доступа, правовые основания, технический механизм и требования к аудиту для каждой категории заинтересованных лиц.

Рекомендации по внедрению многокомпонентной системы защиты данных.

Во-первых, предлагается закрепление в национальных законодательствах принципа технологической нейтральности и внедрения квантово-устойчивых протоколов сохранения конфиденциальности; в подзаконных актах – обновляемого реестра технологий и комплексной матрицы режимов доступа.

Во-вторых, рекомендуется осуществить пилотное тестирование составляющих многокомпонентной системы защиты данных в условиях «регуляторных песочниц» для проверки соответствия критериям защиты персональных данных и требованиям ПОД/ФТ.

В-третьих, провести исследование по адаптации многокомпонентной системы защиты данных ЦВЦБ к условиям трансграничного взаимодействия центральных банков в мультивалютной среде.

Предложенная многокомпонентная система защиты данных демонстрирует возможности преодоления дихотомии «конфиденциальность – доступность/прозрачность». Благодаря синергетическому эффекту от интеграции компонентов этой системы, связанной с управлением режимом доступа к данным можно добиться повышения конфиденциальности в ЦВЦБ в различных юрисдикциях.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. Murphy, K. P. Central Bank Digital Currency Data Use and Privacy Protection / K. P. Murphy, T. Sun, Y. S. Zhou [и др.]. - 2024. - 51 с. - Текст : электронный. - 10.5089/9798400286971.063 (дата обращения: 08.10.2025). DOI: 10.5089/9798400286971.063(

2. Central bank digital currencies: Legal aspects of retail CBDCs / Bank of Canada, Swiss National Bank, European Central Bank [и др.]. - 2024. - 29 с. - Текст: электронный. - URL: https://www.bis.org/publ/othp88_legal.pdf (дата обращения: 08.10.2025).

3. Central bank digital currencies: foundational principles and core features: report no 1 in a series of collaborations from a group of central banks / Bank of Canada, European Central Bank, Bank of Japan [и др.]. - 2020. - 21 с. - Текст: электронный. - URL: https://www.bis.org/publ/othp33.pdf (дата обращения: 08.10.2025).

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. - 2016. - L 119. - С. 1-88. - Текст: электронный. - URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (дата обращения: 08.10.2025).

5. The Digital Dollar Project. Exploring a US CBDC / Ch. H. Giancarlo [и др.]; Accenture and the Digital Dollar Foundation. - 2020. - 50 с. - Текст: электронный. - URL: https://digitaldollarproject.org/wp-content/uploads/2021/05/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf (дата обращения: 08.10.2025).

6. Progress of Research & Development of E-CNY in China / Working Group on E-CNY Research and Development of the People's Bank of China. - 2021. - 15 с. - Текст: электронный. - URL: http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf (дата обращения: 08.10.2025).

7. Taylor, M. The Digital Yuan: Purpose, Progress, and Politics / M. Taylor // Made in China Journal. - 2023. - Текст: электронный. - URL: https://madeinchinajournal.com/2023/11/27/the-digital-yuan-purpose-progress-and-politics/ (дата обращения: 08.10.2025).

References:

1. Murphy, K. P. Central Bank Digital Currency Data Use and Privacy Protection / K. P. Murphy, T. Sun, Y. S. Zhou [et al.]. – 2024. – 51 p. – Electronic text. – URL: https://doi.org/10.5089/9798400286971.063 (accessed: 08.10.2025). DOI: 10.5089/9798400286971.063(

2. Central bank digital currencies: Legal aspects of retail CBDCs / Bank of Canada, Swiss National Bank, European Central Bank [et al.]. – 2024. – 29 p. – Electronic text. – URL: https://www.bis.org/publ/othp88_legal.pdf (accessed: 08.10.2025).

3. Central bank digital currencies: foundational principles and core features : report no 1 in a series of collaborations from a group of central banks / Bank of Canada, European Central Bank, Bank of Japan [et al.]. – 2020. – 21 p. – Electronic text. – URL: https://www.bis.org/publ/othp33.pdf (accessed: 08.10.2025).

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. – 2016. – L 119. – P. 1–88. – Electronic text. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed: 08.10.2025).

5. The Digital Dollar Project. Exploring a US CBDC / Ch. H. Giancarlo [et al.] ; Accenture and the Digital Dollar Foundation. – 2020. – 50 p. – Electronic text. – URL: https://digitaldollarproject.org/wp-content/uploads/2021/05/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf (accessed: 08.10.2025).

6. Progress of Research & Development of E-CNY in China / Working Group on E-CNY Research and Development of the People's Bank of China. – 2021. – 15 p. – Electronic text. – URL: http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf (accessed: 08.10.2025).

7. Taylor, M. The Digital Yuan: Purpose, Progress, and Politics / M. Taylor // Made in China Journal. – 2023. – Electronic text. – URL: https://madeinchinajournal.com/2023/11/27/the-digital-yuan-purpose-progress-and-politics/ (accessed: 08.10.2025).

Информация об авторе:
Карпенко Ирина Николаевна, аспирантка кафедры международного и публичного права юридического факультета Финансового университета при Правительстве РФ, e-mail: 249356@edu.fa.ru
Irina N. Karpenko, postgraduate student of the department of international and public law of the faculty of law of the Financial University under the Government of the Russian Federation

Статья поступила в редакцию / The article was submitted 20.10.2025;
Одобрена после рецензирования / Approved after reviewing 06.11.2025;
Принята к публикации / Accepted for publication 20.11.2025.
Автором окончательный вариант рукописи одобрен.