

УДК 336.71:004

101. ТРАНСФОРМАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ БАНКОМ В УСЛОВИЯХ ПОЯВЛЕНИЯ КРИПТОБАНКОВ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Фомин А.В., Ременчик Е.П. студенты группы 377901

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Нагулевич Р.С. – магистр эк. наук, старший преподаватель

Аннотация. В статье рассмотрено потенциальное влияние института криптобанков на информационные системы управления в финансово-банковской деятельности Республики Беларусь. Систематизированы нормативные предпосылки появления криптобанков, выделены новые требования к данным, процессам и внутреннему контролю. Предложена целевая модель трансформации информационной системы управления банка, основанная на интеграции токеновых операций в контуры учета, риск-менеджмента и комплаенса. Показано, что модернизация системы управления становится условием финансовой устойчивости, надзорной прозрачности и качества управленческой отчетности.

Ключевые слова. Информационные системы управления, криптобанк, цифровые знаки (токены), Парк высоких технологий, банковский надзор, AML/CFT, управленческая отчетность, риск-данные.

Введение

Грядущее появление криптобанков формирует для банковского сектора новую управленческую реальность: наряду с денежными средствами и традиционными платежными инструментами объектом управления становятся токены, криптоаккаунты, адреса, хэши транзакций и связанные с ними риски. В этих условиях информационная система управления банка перестает быть только средством подготовки отчетности и превращается в ядро управления рисками, комплаенсом и операционной устойчивостью.

В Республике Беларусь правовой режим цифровой трансформации был сформирован нормами Декрета № 8 «О развитии цифровой экономики», который в последующем был дополнен специальным режимом криптобанков, регламентированным Указом Президента Республики Беларусь № 19 [1]. С учетом этого задача исследования заключается не только в анализе новых услуг, но и в определении того, каким образом должна измениться архитектура информационной системы управления (далее – ИСУ) банка, чтобы обеспечить управляемость операций с токенами, соответствие требованиям регуляторов и качество управленческих решений [1], [2], [4].

Нормативно-институциональные предпосылки криптобанков в Беларуси

Базой для формирования криптофинансовой инфраструктуры в Беларуси стал специальный режим Парка высоких технологий (далее – ПВТ), легализовавший отдельные операции с токенами и деятельность операторов криптоплатформ и обмена. На следующем этапе происходит внедрение института криптобанка как организации, сочетающей банковские и платежные операции с операциями в сфере цифровых знаков. Такая конструкция означает переход от изолированной криптодеятельности к гибридной модели финансового посредничества.

С управленческой точки зрения ключевое значение имеет двойной контур регулирования. Банковские и платежные операции криптобанка контролируются Национальным банком Республики Беларусь, тогда как перечень допустимых токенов и часть операций с ними согласовываются также в рамках режима ПВТ. Из этого следует, что ИСУ криптобанка должна одновременно поддерживать требования банковского надзора, правила внутреннего контроля, процедуры удаленной идентификации клиентов, раскрытие рисков для потребителей и отдельные механизмы надзорной «проверяемости» по операциям с токенами.

Отдельное значение имеет и то обстоятельство, что средства физических лиц, размещенные в криптобанке, подчиняются специальному режиму гарантий и раскрытия рисков. Поэтому ИСУ криптобанка должна обеспечивать не только учет активов и обязательств, но и своевременную риск-коммуникацию: фиксировать содержание уведомлений клиенту, контролировать полноту раскрытий и связывать данные фронт-офиса с контуром внутреннего контроля банка [1], [2], [3].

Изменение требований к информационной системе управления банка

Во-первых, расширяется состав управленческих данных. Если в традиционной модели доминируют счета, кредиты, платежи и валютные операции, то в криптобанке в контур данных включаются криптоаккаунты, токеновые портфели, признаки происхождения активов, история on-chain-транзакций, риск-метки адресов и данные о цифровых кошельках. Это требует единого словаря данных и сопоставимости информации между банковским ядром, токеновой платформой и внешними сервисами внешними сервисами блокчейн-аналитики (как собственными инструментами банка, так и данными специализированных провайдеров).

Во-вторых, возрастают требования к скорости и качеству риск-отчетности. Высокая волатильность цифровых активов делает недостаточной редкую переоценку позиций: ИСУ должна поддерживать более частую оценку портфелей, сценарный анализ и стресс-тестирование. В этом контексте методологически важны принципы BCBS 239, ориентирующие банк на быстрое агрегирование риск-данных, минимизацию ручных корректировок и повышение качества управленческой отчетности.

В-третьих, усложняется комплаенс, связанных с легализацией доходов, полученных преступным путем, и финансированием терроризма. В системе должны быть встроены механизмы KYC/AML, контроль источников происхождения токенов, анализ связей адресов, учет требований Travel Rule и противодействие мошенничеству. Иначе контроль будет выполняться постфактум, а это снижает как скорость обслуживания, так и качество надзорной функции.

В-четвертых, на первый план выходят технологические и операционные риски цифровых активов. Управление криптографическими ключами, резервирование, ведение журнала действий операторов, отдельный учет активов банка и клиентов, предотвращение мультиаккаунтинга и обеспечение проведения проверок операций становятся элементами самой архитектуры ИСУ, а не вспомогательными мерами информационной безопасности [4], [5], [6], [8].

Целевая модель трансформации ИСУ криптобанка

Рациональной, с точки зрения обеспечения вышеизложенных требований, будет многоуровневая архитектура, в которой традиционное банковское ядро дополняется отдельной платформой цифровых активов (Digital Asset Platform), а также комплаенс-контуром, объединяющим AML/CFT, antifraud, chain analytics и контроль передачи данных по операциям. На рисунке 1 представлена обобщенная схема такой архитектуры.

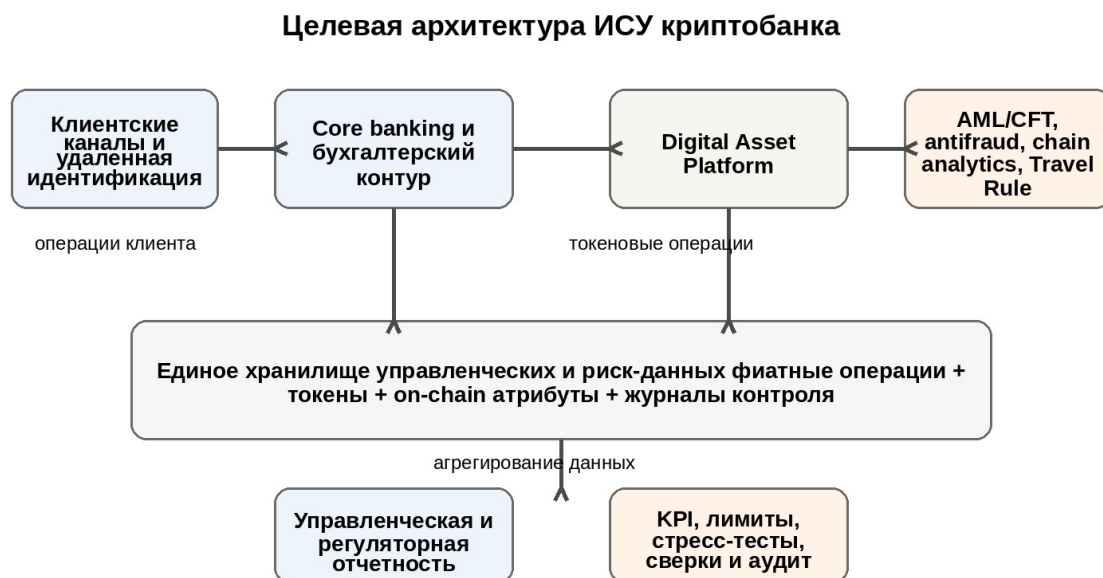


Рисунок 1 – Целевая архитектура ИСУ криптобанка

Центральным элементом модели выступает единое хранилище управленческих и риск-данных, куда поступает информация из core banking, токеновой платформы, клиентских каналов и контрольных сервисов. Это позволяет формировать единую управленческую отчетность по фиатным и токеновым операциям, рассчитывать лимиты, проводить сверки транзакционных данных и остатков между

контурами учета и быстро формировать наборы данных для службы внутреннего контроля и регулятора.

Для интегральной оценки риска токеновой операции может использоваться формула (1), учитывающая уровень комплаенс-риска, волатильность актива, технологическую уязвимость и качество ключевого управления:

$$R = w_1C + w_2V + w_3T + w_4K \quad (1)$$

где R – интегральная оценка риска токеновой операции, выраженная в национальной валюте (белорусских рублях, BYN); C – комплаенс-риск (оценивается в баллах от 0 до 1); V – волатильность актива (процентное отклонение рыночной стоимости токена за расчетный период); T – технологическая уязвимость (от 0 до 1, где 1 – максимально уязвимый); K – уровень надежности ключевого управления (от 0 до 1, где 1 – самый надежный); $w_1 \dots w_4$ – весовые коэффициенты факторов.

Практически это означает переход от фрагментарной автоматизации к сквозному управлению жизненным циклом операции: прием клиента на обслуживание (onboarding), выполнение операции, мониторинг, формирование сигналов о подозрительной активности (алертинг), управленческая и регуляторная отчетность. Чем меньше ручных разрывов (неавтоматизированных этапов передачи и обработки данных) между этими этапами, тем выше достоверность данных, устойчивость процессов и готовность банка к надзорной проверке.

Для систематизации подходов к проектированию систем в таблице 1 обобщены основные отличия требований к ИСУ традиционного банка и криптобанка.

Таблица 1 – Сравнение требований к ИСУ традиционного банка и криптобанка

Компонент	Традиционный банк	Криптобанк
Объекты учета	Счета, кредиты, платежи, FX.	Счета и платежи дополняются криптоаккаунтами, токенами и on-chain-атрибутами.
Риск-отчетность	Периодическая финансовая и риск-отчетность.	Более частая переоценка, стресстесты и лимиты по токеновым портфелям.
Комплаенс	KYC/AML по традиционным операциям.	KYC/AML, проверка происхождения токенов, Travel Rule, chain analytics и antifraud.
ИТ-контроли	Стандартные банковские журналы и разграничение доступа.	Усиленное журналирование, сверки между контурами, резервирование, контроль ключей.
Защита клиента	Типовые раскрытия и стандартный режим гарантий.	Специальный режим раскрытия рисков и учет особенностей гарантий по средствам клиентов.

Заключение

По результатам проведенного исследования можно сделать следующие выводы.

1. Перспектива появления криптобанков в Республике Беларусь изменяет сам предмет управления в банковской сфере: наряду с традиционными денежными потоками объектом системного контроля становятся токеновые операции, on-chain-атрибуты и новые виды клиентских и технологических рисков. Поэтому трансформация ИСУ является не вспомогательным ИТ-проектом, а необходимым условием финансовой устойчивости, надзорной прозрачности и легитимности деятельности криптобанка.

2. Предложенная модель показывает, что ключевыми направлениями модернизации ИСУ выступают интеграция данных, усиление риск-отчетности, встраивание комплаенс-проверок в процессинг и развитие ИТ-контролей по цифровым активам. Именно такое сочетание позволяет

обеспечить управляемость операций с токенами, повысить качество управленческих решений и адаптировать банк к новой институциональной среде [1], [4], [6].

3. Эффективность функционирования ИСУ после проведенной трансформации целесообразно оценивать по набору KPI: времени формирования риск-отчетов, доле операций, проходящих контроль в режиме near real time, уровню ручных корректировок, точности сверок между контурами учета, доступности критичных сервисов и числу инцидентов комплаенса. Такой подход связывает качество данных с качеством управленческих решений и позволяет оценивать зрелость архитектуры на практике. [1], [6]

Список использованных источников:

1. О криптобанках и отдельных вопросах контроля в сфере цифровых знаков (токенов): Указ Президента Республики Беларусь от 16 янв. 2026 г., № 19.
2. О развитии цифровой экономики: Декрет Президента Республики Беларусь от 21 дек. 2017 г., № 8.
3. Правила осуществления деятельности резидентами ПВТ, осуществляющими сделки с цифровыми знаками (токенами) в интересах других лиц [Электронный ресурс]: утв. решением Наблюдательного совета Парка высоких технологий. – Режим доступа: <https://park.by/analytics/documents/>. – Дата доступа: 20.03.2026.
4. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers [Electronic resource] / FATF. – 2021. – Mode of access: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf>. – Date of access: 20.03.2026.
5. Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs [Electronic resource] / FATF. – 2024. – Mode of access: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-VA-VASP-2024.pdf>. – Date of access: 20.03.2026.
6. Principles for effective risk data aggregation and risk reporting (BCBS 239) [Electronic resource] / Basel Committee on Banking Supervision. – 2013. – Mode of access: <https://www.bis.org/publ/bcbs239.pdf>. – Date of access: 26.03.2026.
7. Prudential treatment of cryptoasset exposures [Electronic resource] / Basel Committee on Banking Supervision. – 2022. – Mode of access: <https://www.bis.org/bcbs/publ/d545.htm>. – Date of access: 21.03.2026.
8. Recommendation for Key Management: Part 1 – General (NIST SP 800-57) [Electronic resource] / National Institute of Standards and Technology. – 2020. – Mode of access: <https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/upd1/final>. – Date of access: 26.03.2026.
9. Market Structure of Core Banking Services Providers [Electronic resource] / Federal Reserve Bank of Kansas City. – 2024. – Mode of access: <https://www.kansascityfed.org/research/payments-system-research-briefings/market-structure-of-core-banking-services-providers/>. – Date of access: 21.03.2026.
10. Blockchain technology in the banking sector: a content analysis / R. Sheikh [et al.] // *Frontiers in Blockchain*. – 2025. – Vol. 8. – P. 1667848.

UDC 336.71:004

TRANSFORMATION OF BANK MANAGEMENT INFORMATION SYSTEMS IN THE CONTEXT OF THE EMERGENCE OF CRYPTO BANKS IN THE REPUBLIC OF BELARUS

Fomin A.V., Remenchik E.P.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Nagulevich R.S. – Master of Economic Sciences, Senior Lecturer

Annotation. The article considers the potential impact of the institution of crypto banks on management information systems in the financial and banking activities of the Republic of Belarus. The regulatory prerequisites for the emergence of crypto banks are systematized, and new requirements for data, processes, and internal control are highlighted. A target model for the transformation of a bank's MIS is proposed, based on the integration of token operations into the accounting, risk management, and compliance contours. It is shown that the modernization of MIS becomes a condition for financial stability, supervisory transparency, and the quality of management reporting.

Keywords. Management information systems, crypto bank, digital signs (tokens), HTP, banking supervision, AML/CFT, management reporting, risk data.