

ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «AUSU»

БИН 260540022655

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРА ОБМЕНА НЕОБЕСПЕЧЕННЫХ ЦИФРОВЫХ АКТИВОВ ТОО «AUSU»

Версия: 1.0 · Дата утверждения: 2 июля 2026 года · Пересмотр: 2 июля 2027

Владелец: Единственный участник — Сахаров Никита Сергеевич

Утвердил: Единственный участник

Подготовлено в соответствии с пунктом 23 Правил осуществления деятельности операторов обмена необеспеченных цифровых активов, утверждённых постановлением Правления Национального Банка Республики Казахстан от 29 апреля 2026 года № 45 (далее — Правила НБ № 45); Законом Республики Казахстан «О цифровых активах в Республике Казахстан» и иными нормативными правовыми актами Национального Банка Республики Казахстан.



СОДЕРЖАНИЕ

№	Раздел	
Гл. 1	Общие положения, термины, нормативная база	
Гл. 2	Сфера деятельности и виды операций	
Гл. 2-1	Права и обязанности Оператора и клиентов	
Гл. 3	Перечень разрешённых необеспеченных ЦА	
Гл. 4	Категоризация клиентов и допуск	
Гл. 5	Лимиты по клиентам и операциям	
Гл. 6	Бизнес-процесс «Привлечение клиента» (сквозной)	
Гл. 7	Бизнес-процесс «Обменная операция» (сквозной)	
Гл. 8	Бизнес-процесс «Депозит / вывод средств»	
Гл. 9	Бизнес-процесс «Подача сообщения о подозрительных и пороговых операциях»	
Гл. 10	Регламент работы, нормативы обслуживания (SLA), каналы поддержки	
Гл. 11	Курсообразование, спред, оракулы цен	
Гл. 12	Тарифы и комиссии	
Гл. 13	Защита прав потребителей и жалобы	
Гл. 14	Конфиденциальность и обработка ПД	
Гл. 15	Хранение записей и архивирование	
Гл. 16	Внутренний контроль и мониторинг	
Гл. 17	Прекращение услуг и расторжение договора	
Гл. 18	Порядок и условия работы физических отделений и пунктов самообслуживания	
Гл. 19	Порядок и сроки завершения расчётов по сделкам	
Гл. 20	Источники пополнения ликвидности и реализация излишней ликвидности	
Гл. 21	Порядок и условия открытия и ведения кошельков цифровых активов	
Гл. 22	Адреса кошельков цифровых активов Оператора	
Гл. 23	Процедуры обеспечения кибербезопасности	
Гл. 24	Система анализа и контроля операций	
Гл. 25	Информация о рисках на интернет-ресурсе	
Гл. 26	Запрет на установление деловых отношений	
Гл. 27	Раздельные банковские счета	
Гл. 28	Утверждение и пересмотр Правил	
Прил. 1	Перечень 73 разрешённых необеспеченных ЦА	
Прил. 2	Реестр адресов кошельков цифровых активов Оператора	
Прил. 3	Тест квалификации клиента (12 вопросов)	
Прил. 4	Карта инцидента кибербезопасности (форма)	
Прил. 5	Журнал контроля встречного исполнения по сделкам (Т+2) (форма)	

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и область применения

Настоящие Правила осуществления деятельности (далее — «Правила») устанавливают порядок осуществления деятельности Товарищества с ограниченной ответственностью «Ausu» (далее — «Оператор», «ТОО «Ausu»») в качестве оператора обмена необеспеченных цифровых активов в Республике Казахстан и являются основным внутренним регламентным документом, регулирующим взаимоотношения Оператора с клиентами, иными участниками рынка цифровых активов и регулятором — Национальным Банком Республики Казахстан (далее — НБ РК).

Правила распространяются на:

- всех клиентов Оператора (физических и юридических лиц);
- всех работников Оператора, независимо от формы привлечения;
- подрядчиков и контрагентов Оператора в части, применимой к их деятельности;
- руководящий состав и единственного участника Оператора. Сервисные провайдеры, указанные в настоящих Правилах (провайдер идентификации клиента Sumsb, базы скрининга публичных должностных лиц (ПДЛ) WorldCheck / Dow Jones, сервисы анализа транзакций TRM Labs / Chainalysis, провайдер передачи данных о переводах Notabene (протоколы TRP/TRISA)), являются целевыми: договоры с ними заключаются после получения лицензии по результатам комплексной проверки. До подключения соответствующих сервисов проверки выполняются ответственными работниками по официальным открытым источникам (санкционные перечни ООН, OFAC, ЕС, UK HMT, перечень КФМ РК, публичные блокчейн-обозреватели). Источники рыночных данных для курсообразования (Binance Kazakhstan, CoinGecko, Coinbase, TradingView) являются публичными программными интерфейсами (API) и используются с момента запуска.

1.2. Нормативная база

№	Документ	Применимые нормы
1	Закон РК «О цифровых активах в Республике Казахстан»	В том числе статьи 1, 4, 12-1, 12-2 (определения, компетенция Национального Банка, деятельность и лицензирование операторов обмена НЦА)
2	Постановление Правления НБ РК от 29.04.2026 № 45 (зарегистрировано в МЮ РК 30.04.2026 № 38622)	Правила осуществления деятельности операторов обмена НЦА (Правила НБ № 45): лицензирование, квалификационные требования, порядок деятельности, кибербезопасность, лимиты
3	Постановление Правления НБ РК от 29.04.2026 № 47 (зарегистрировано в МЮ РК 30.04.2026 № 38614)	Правила формирования системы управления рисками и внутреннего контроля: требования к системе управления рисками, политикам и регламентам
4	Закон РК «О ПОД/ФТ/ФРОМУ»	Надлежащая проверка клиентов, финансовый мониторинг, внутренний контроль, предоставление сведений в АФМ РК
5	Закон РК «О персональных данных и их защите»	Сбор, обработка, согласие субъекта, меры по защите персональных данных
6	Закон РК «О защите прав потребителей»	Главы 2-3 (право на информацию, право на качество)
7	Гражданский кодекс РК	Глава 23 (договор), ст. 387–389 (присоединение, публичная оферта)
8	Закон РК «О валютном регулировании и валютном контроле»	Требования валютного законодательства при операциях с клиентами-нерезидентами в иностранной валюте

9	Кодекс РК «О налогах и других обязательных платежах в бюджет» (Налоговый кодекс)	Налоговые обязательства Оператора; информирование клиентов о необходимости соблюдения налогового законодательства
10	Постановление Правления НБ РК от 10.04.2026 № 33 (зарегистрировано в МЮ РК 13.04.2026 № 38408)	Требования к Правилам внутреннего контроля в целях ПОД/ФТ/ФРОМУ
11	Постановление Правления НБ РК от 10.04.2026 № 35 (зарегистрировано в МЮ РК 13.04.2026 № 38409)	Правила применения мер надзорного реагирования к оператору обмена НЦА
12	Постановление Правления НБ РК от 10.04.2026 № 36 (зарегистрировано в МЮ РК 13.04.2026 № 38404)	Правила представления отчётности операторами обмена НЦА
13	Трудовой кодекс РК	Подтверждение трудовой деятельности руководящего работника; трудовые отношения с работниками

Перечень нормативной базы приведён по состоянию на дату утверждения Правил и не является исчерпывающим: Оператор соблюдает все иные применимые нормативные правовые акты Республики Казахстан.

1.3. Определения и термины

Термин	Определение
Цифровой актив (ЦА)	Имущество, существующее в электронно-цифровой форме, созданное и учитываемое с применением средств криптографической защиты и (или) технологии распределённых данных (статья 1 Закона РК «О цифровых активах в Республике Казахстан»)
Необеспеченный цифровой актив (НЦА)	ЦА, не обеспеченный имуществом, иными активами или обязательствами эмитента
Стейблкоин	Необеспеченный цифровой актив, стоимость которого стабилизируется эмитентом или алгоритмом относительно фиатной валюты; обменивается в составе перечня 73 НЦА, установленного пунктом 57 Правил НБ № 45 (см. Гл. 3)
Обменная операция	Операция по покупке и (или) продаже необеспеченных цифровых активов, в результате которой клиент получает необеспеченные цифровые активы в обмен на деньги либо деньги в обмен на необеспеченные цифровые активы, по курсу, установленному Оператором (пункт 2 Правил НБ № 45); обмен НЦА на НЦА не осуществляется
Квалифицированный клиент (КИ)	Клиент, прошедший тест квалификации (пункты 53-54 Правил НБ № 45; Приложение № 3 к настоящим Правилам) с результатом не ниже 80 %
Неквалифицированный клиент (НКИ)	Клиент, не прошедший тест квалификации; применяются лимиты пункта 56: покупка до 7 000 000 Т/сутки и продажа до 7 000 000 Т/сутки (внутренний накопительный лимит Оператора — 70 000 000 Т/год)
правило передачи данных об отправителе и получателе перевода	Обязанность по передаче сведений об отправителе и получателе при переводе цифровых активов в случаях, установленных Законом Республики Казахстан «О ПОД/ФТ/ФРОМУ»
сообщение о подозрительной операции	Сообщение о подозрительной операции в АФМ РК
сообщение о пороговой операции	Сообщение о пороговой операции (порог установлен пунктом 1 статьи 4 Закона Республики Казахстан «О ПОД/ФТ/ФРОМУ»)
углублённая проверка клиента	Углублённая проверка клиента для высокорисковых категорий
стандартная проверка клиента	Стандартная проверка клиента
упрощённая проверка клиента	Упрощённая проверка для низкорисковых категорий (в рамках ограничений ФАТФ)

конечный бенефициарный собственник	Конечный бенефициарный собственник
Сегрегация активов	Раздельный учёт собственных активов Оператора и активов клиентов (Закон РК «О цифровых активах в Республике Казахстан»)
Горячий кошелек	Онлайн-кошелек для оперативных операций; не более 15% от объёма активов клиентов
Тёплый кошелек	Промежуточное хранилище с мультиподписью; 5–10% от объёма
Холодный кошелек	Офлайн-хранилище с физической изоляцией; не менее 85% от объёма активов клиентов
мультиподпись	Технология подписи транзакций несколькими ключами по схеме «m из n»; целевая схема Оператора — «3 из 5» (внедряется после перехода на кастодиальную инфраструктуру)
Перемещение средств	Регламентная процедура перевода поступивших активов из горячего в тёплый/холодный уровень

1.4. Принципы деятельности Оператора

Оператор осуществляет деятельность в соответствии со следующими принципами:

- (а) Законность — деятельность ведётся исключительно в рамках полученной лицензии и применимого законодательства РК;
- (б) Транспарентность — раскрытие тарифов, курсов, рисков и условий обслуживания в публичных каналах;
- (в) Защита клиента — сегрегация активов, многоуровневый контроль доступа, страхование операционных рисков (после перехода на кастодиальную инфраструктуру — в составе страхового покрытия кастодиального провайдера);
- (г) Риск-ориентированный подход — внутренние процессы построены на основе оценки рисков;
- (д) Чистая репутация — отказ от обслуживания клиентов из санкционных юрисдикций, лиц из перечня ФТФР, публичных должностных лиц (ПДЛ) без углублённой проверки клиента;
- (е) Непрерывность — наличие плана непрерывности деятельности и планов аварийного восстановления.

1.5. Организационная структура и ответственные работники

Руководство деятельностью осуществляет Директор — единственный участник. Функции ответственных работников распределены следующим образом (функция управления рисками выделена в самостоятельную и закреплена за ответственным работником по управлению рисками (риск-менеджером); допускается её совмещение с функцией комплаенс-контроля; совмещение функций управления рисками и комплаенс-контроля с функцией внутреннего аудита не допускается; функциональное разделение журналов и отчётности обеспечено):

Роль	Ответственный работник	Ключевые функции
Директор (исполнительный орган)	Сахаров Никита Сергеевич	Общее руководство, утверждение операционных решений, представление Оператора в НБ РК
Ответственный работник по комплаенс-контролю (ПОД/ФТ)	Ф.И.О. назначается приказом единственного участника	ПОД/ФТ/ФРОМУ, санкционный скрининг, сообщения о подозрительных и пороговых операциях, реестр рисков, взаимодействие с АФМ РК
Ответственный работник по управлению рисками (риск-менеджер)	Ф.И.О. назначается приказом единственного участника (допускается совмещение с функцией комплаенс-контроля)	Выявление, оценка, контроль и мониторинг рисков (включая риски ИТ и ИБ), лимиты остатков и Реестр рисков, контроль лимита 50 % по пункту 41 Правил НБ № 45, отчётность органу управления
Ответственный работник по правовому обеспечению	Ф.И.О. назначается приказом единственного участника	Правовая экспертиза, договорная работа, претензии и жалобы, взаимодействие с регулятором
Ответственный работник по внутреннему аудиту	Ф.И.О. назначается приказом единственного участника	Независимая оценка системы внутреннего контроля, аудиторские проверки, контроль исполнения рекомендаций
ИТ-администратор	Ф.И.О. назначается приказом единственного участника	Эксплуатация цифровой инфраструктуры, доступы, резервное копирование, поддержка платформы
Ответственный работник по информационной безопасности	Ф.И.О. назначается приказом единственного участника	Политика ИБ, контроль внедрения мер защиты, координация реагирования на критические инциденты; независимый аудит ИБ и тестирование на проникновение — внешний специализированный подрядчик, привлекаемый на договорной основе после получения лицензии

Контроль строится по модели трёх линий защиты (Глава 16): первая линия — операционные работники и ИТ; вторая — комплаенс и управление рисками; третья — внутренний аудит.

ГЛАВА 2. СФЕРА ДЕЯТЕЛЬНОСТИ И ВИДЫ ОПЕРАЦИЙ

2.1. Виды деятельности

В рамках лицензии оператора обмена необеспеченных цифровых активов Оператор оказывает следующие виды услуг:

№	Вид услуги	Описание	Каналы доступа
1	Обмен НЦА на национальную валюту (KZT)	Покупка/продажа НЦА за тенге безналичным расчётом	Веб-приложение, мобильное приложение
2	Обмен НЦА на иностранную валюту (USD/EUR/RUB/CNY)	Покупка/продажа НЦА за иностранную валюту в безналичной форме — только для клиентов-нерезидентов Республики Казахстан; с клиентами-резидентами операции совершаются в национальной валюте (тенге)	Веб-приложение, мобильное приложение
3	Кастодиальное хранение НЦА клиентов	Хранение активов клиентов на кошельках под управлением Оператора (сегрегированный учёт) — в рамках обслуживания обменных операций с необеспеченными цифровыми активами.	Личный кабинет в веб-приложении
4	Сопутствующие операции по кошелькам (зачисление и вывод НЦА)	Вывод необеспеченных цифровых активов на адреса кошельков клиентов и зачисление необеспеченных цифровых активов на кошельки, открытые Оператором клиенту, — исключительно в рамках исполнения обменных операций, с соблюдением правила передачи данных об отправителе и получателе перевода.	Веб-приложение, мобильное приложение
5	Информационные услуги по курсам и комиссиям	Публикация котировок 73 НЦА, исторических данных, сравнения курсов	Веб-приложение, мобильное приложение, программный интерфейс (API) (только для чтения)

2.2. Осуществление исключительно лицензируемого вида деятельности

В соответствии с Законом Республики Казахстан «О цифровых активах» Оператор осуществляет исключительно лицензируемый вид деятельности — обменные операции с необеспеченными цифровыми активами (дилерская деятельность на рынке цифровых активов). Осуществление любых иных видов деятельности, не предусмотренных лицензией, не допускается.

2.3. Сегрегация активов клиентов и собственных средств

В соответствии с Законом РК «О цифровых активах в Республике Казахстан» Оператор обеспечивает отдельный учёт собственных активов и активов клиентов:

(а) активы клиентов хранятся на сегрегированных омнибус-кошельках, не смешиваются с собственными активами Оператора;

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

(б) внутренний реестр клиентских активов (Сегрегированный реестр) ведётся в реальном времени и ежедневно реконсилируется с он-чейн балансами по 6 типам реконсиляции (внутренняя политика управления кошельками Оператора);

(в) собственный казначейский кошелёк используется для покрытия операционных издержек и не доступен для удовлетворения обязательств Оператора перед иными лицами;

(г) активы клиентов учитываются отдельно как не принадлежащие Оператору и подлежат возврату клиентам, в том числе при прекращении деятельности Оператора.

ГЛАВА 2-1. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА И КЛИЕНТОВ

2-1.1. Оператор вправе: запрашивать у клиента документы и сведения для идентификации, верификации, определения квалификации и надлежащей проверки в целях ПОД/ФТ/ФРОМУ; отказать в установлении деловых отношений или совершении операции, приостановить либо прекратить обслуживание в случаях, предусмотренных законодательством Республики Казахстан и настоящими Правилами; применять лимиты и ограничения по операциям в соответствии с квалификацией клиента; определять размер вознаграждения (комиссий) и спреда в раскрытом клиенту порядке; привлекать поставщиков услуг с сохранением ответственности перед клиентом.

2-1.2. Оператор обязан: осуществлять деятельность исключительно в пределах лицензии и требований законодательства Республики Казахстан; обеспечивать отдельный учёт (сегрегацию) собственных активов и активов клиентов; до совершения операции доводить до клиента информацию о рисках, тарифах, курсе и условиях обслуживания; обеспечивать встречное исполнение клиенту в срок не более 2 (двух) рабочих дней с момента получения денег или необеспеченных цифровых активов; идентифицировать клиентов-резидентов через ЦОИД, обеспечивать биометрическую аутентификацию резидентов и идентификацию нерезидентов; обеспечивать кибербезопасность и сохранность активов и сведений клиентов; рассматривать обращения и жалобы и возмещать причинённый по вине Оператора ущерб; представлять отчётность в Национальный Банк Республики Казахстан.

2-1.3. Клиент вправе: получать полную и достоверную информацию о тарифах, курсе, рисках и условиях обслуживания; совершать операции в пределах лимитов согласно своей квалификации; распоряжаться своими активами без необоснованных ограничений; подавать обращения и жалобы и получать ответ в установленные сроки; на

возмещение причинённого по вине Оператора ущерба и возврат денег и (или) необеспеченных цифровых активов; на защиту персональных данных и обращение в уполномоченный орган и суд.

2-1.4. Клиент обязан: предоставлять достоверные сведения и документы при идентификации, верификации и определении квалификации; своевременно уведомлять Оператора об изменении сведений; соблюдать настоящие Правила и условия договора присоединения; не использовать услуги для операций, запрещённых законодательством Республики Казахстан; самостоятельно нести принятые им риски, связанные с покупкой, продажей и владением необеспеченными цифровыми активами.

ГЛАВА 3. ПЕРЕЧЕНЬ РАЗРЕШЁННЫХ НЕОБЕСПЕЧЕННЫХ ЦА

Оператор осуществляет обмен исключительно по перечню из 73 необеспеченных цифровых активов, установленному пунктом 57 Правил НБ № 45 и приведённому в Приложении № 1 к настоящим Правилам. Оператор не устанавливает собственных дополнительных критериев допуска необеспеченных цифровых активов к обмену.

3.1. Порядок актуализации перечня разрешённых НЦА

Перечень разрешённых НЦА установлен пунктом 57 Правил НБ № 45 и изменяется исключительно вслед за изменением указанного пункта. Актуализация Приложения № 1 к настоящим Правилам оформляется решением единственного участника. Мониторинг оснований для актуализации осуществляется:

- (а) планоно — ежеквартально, в течение 10 рабочих дней после окончания квартала;
- (б) внепланоно — при внесении изменений в пункт 57 Правил НБ № 45, а также при возникновении обстоятельств, требующих временного приостановления операций с отдельным НЦА (санкционные ограничения, компрометация сети блокчейн, технические причины);
- (в) по требованию НБ РК.

Актуализация Приложения № 1 оформляется решением единственного участника. Временное приостановление обслуживания отдельного НЦА по операционным основаниям (без изменения перечня) оформляется приказом Директора по представлению риск-менеджера и ответственного работника по комплаенс-контролю, с заключением ИТ-администратора; информация публикуется в личном кабинете клиентов не позднее чем за 30 календарных дней, за исключением случаев, требующих немедленного приостановления в соответствии с законодательством Республики Казахстан.

3.2. Действия при исключении НЦА из перечня

При исключении НЦА из перечня Оператор:

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

(а) уведомляет клиентов через личный кабинет, e-mail и push-уведомления не позднее чем за 30 календарных дней;

(б) приостанавливает приём депозитов в исключаемом НЦА с даты публикации уведомления;

(в) сохраняет возможность вывода средств клиентами на внешние адреса в течение 60 календарных дней с даты уведомления;

(г) по истечении срока вывода активы клиента продолжают учитываться на кошельке клиента; возможность вывода на внешний адрес сохраняется по обращению клиента через службу поддержки; принудительная конвертация активов клиента не осуществляется.

ГЛАВА 4. КАТЕГОРИЗАЦИЯ КЛИЕНТОВ И ДОПУСК

4.1. Категории клиентов

Категория	Критерии	Лимиты
Неквалифицированный клиент-резидент РК (НКИ-Р)	Физ. лицо, резидент РК, не прошедший тест квалификации	Покупка — до 7 000 000 Т/сутки и продажа — до 7 000 000 Т/сутки (раздельно, пункт 56 Правил НБ № 45); внутренний накопительный лимит Оператора — 70 000 000 Т/год
Неквалифицированный клиент-нерезидент (НКИ-Н)	Физ. лицо, нерезидент РК, не прошедший тест	Обмен: до 7 000 000 тенге в сутки и до 70 000 000 тенге в год (раздельно по покупке и продаже; в тенговом эквиваленте операций в иностранной валюте по официальному курсу на дату операции)
Квалифицированный клиент — физ. лицо (КИ-Ф)	Клиент, прошедший тест квалификации (пункты 53-54 Правил НБ № 45; Приложение № 3 к настоящим Правилам) с результатом не ниже 80 %	Лимиты не применяются (кроме внутренних лимитов по ПОД/ФТ и политике казначейства)
Квалифицированный клиент — юр. лицо (КИ-Ю)	Прохождение теста квалификации (Приложение № 3) уполномоченным представителем с результатом не ниже 80 %	Лимиты не применяются (кроме внутренних)
Иностранное юридическое лицо (КИ-И)	Аналогично КИ-Ю, при условии прохождения углублённой проверки клиента	Лимиты не применяются (кроме внутренних). Резиденты санкционных юрисдикций не допускаются

4.2. Определение квалификации клиента

Квалификация клиента для совершения операций с цифровыми активами определяется исключительно посредством оценки знаний клиента с использованием вопросника (теста) в соответствии с пунктами 53-54 Правил НБ № 45 (Приложение № 3 к настоящим Правилам). Минимальный проходной балл — 80 (восемьдесят) процентов; повторное проведение оценки знаний доступно через 30 (тридцать) календарных дней. Иные критерии (имущественные, профессиональные, по опыту операций) для определения квалификации не применяются.

4.3. Подтверждение статуса квалифицированного клиента

Статус квалифицированного клиента подтверждается исключительно прохождением теста квалификации (Приложение № 3) с результатом не ниже 80 % и проставлением всех обязательных отметок о принятии рисков. Подтверждающие документы (о доходах, источнике средств) могут запрашиваться Оператором в рамках надлежащей проверки клиента независимо от его квалификации.

Статус КИ подтверждается на 12 месяцев и продлевается по аналогичной процедуре. При отзыве хотя бы одного из критериев — клиент переводится в категорию НКИ до повторного подтверждения.

ГЛАВА 5. ЛИМИТЫ ПО КЛИЕНТАМ И ОПЕРАЦИЯМ

5.1. Категориальные лимиты

Категория	Лимит на сутки	Лимит на год	Особые ограничения
НКИ-Р	7 000 000 ₸	70 000 000 ₸	Обязательное ознакомление с информацией о рисках и предупреждающие уведомления при первой операции
НКИ-Н	7 000 000 тенге	70 000 000 тенге	Допуск только из не-санкционных юрисдикций; обязательная видео-идентификация
КИ-Ф	Внутренние лимиты по ПОД/ФТ/Казначейство	—	Лимит на разовую операцию: 125 000 000 тенге без дополнительной проверки источника происхождения средств
КИ-Ю	Внутренние лимиты по ПОД/ФТ/Казначейство	—	Лимит на разовую операцию: 500 000 000 тенге без дополнительной проверки источника происхождения средств
КИ-И	Внутренние лимиты + углублённая проверка клиента	—	Только не-санкционные юрисдикции; обязательное предоставление сертификата налогового резидентства

В соответствии с пунктом 56 Правил НБ № 45 лимиты неквалифицированного клиента применяются отдельно: по покупке необеспеченных цифровых активов — до 7 000 000 (семи миллионов) тенге в сутки и по продаже необеспеченных цифровых активов — до 7 000 000 (семи миллионов) тенге в сутки; суточные лимиты покупки и продажи не суммируются. Годовой лимит 70 000 000 тенге является внутренним дополнительным ограничением Оператора.

Накопительные внутренние лимиты Оператора (сверх суточных лимитов пункта 56, применяемых отдельно по покупке и продаже):

Категория	Сутки	Месяц	Год
НКИ-Р	7 000 000 ₸ (покупка) / 7 000 000 ₸ (продажа)	30 000 000 ₸	70 000 000 ₸
НКИ-Н	эквивалент 7 000 000 тенге	30 000 000 тенге	70 000 000 тенге
КИ-Ф	внутренние ПОД/ФТ-лимиты	250 000 000 тенге (автопереход на углублённую проверку клиента)	—
КИ-Ю	внутренние ПОД/ФТ-лимиты	1 000 000 000 тенге (автопереход на углублённую проверку клиента)	—

5.2. ПОД/ФТ-пороги (триггеры контроля)

Примечание: суточный и годовой лимиты неквалифицированного клиента установлены в тенге в соответствии с пунктом 56 Правил НБ № 45. Внутренние мониторинговые пороги Оператора приведены в тенге по расчётному курсу 500 тенге за 1 доллар США; для целей контроля применяется официальный курс Национального Банка Республики Казахстан на дату операции. Порог пороговой

операции определяется в соответствии с пунктом 1 статьи 4 Закона Республики Казахстан «О ПОД/ФТ/ФРОМУ».

Триггер	Порог	Действие
Совокупная сумма операций за календарный месяц	25 000 000 тенге (НКИ) / 125 000 000 тенге (КИ-Ф)	Запрос актуального источника средств (обновление источника происхождения средств)
Разовая операция	7 500 000 тенге (НКИ) / 50 000 000 тенге (КИ-Ф) / 250 000 000 тенге (КИ-Ю)	Проверка по санкционным спискам, мониторинг транзакций, при превышении — сообщения о подозрительных и пороговых операциях
Серия операций (дробление операций)	>3 операций суммой между 4 000 000 и 7 499 999 тенге в течение 72 часов	Автоматическое формирование красного флага в системе мониторинга транзакций; ручная проверка
Перевод на некастодиальный кошелек	>500 000 тенге (Рекомендация ФАТФ 16)	Запрос подтверждения владения адресом (проверка владения адресом); обмен данными по правилу передачи данных об отправителе и получателе перевода
Высокорисковая страна	Любая операция	Обязательная углублённая проверка клиента; запрет для юрисдикций из чёрного списка ФАТФ

5.3. Операционные лимиты Оператора

Внутренние лимиты Оператора, не доводимые до клиента, но соблюдаемые в процессе обработки сделок:

- Лимит на разовую сделку без согласования с Казначейство: эквивалент 50 000 000 тенге;
- Лимит на сделку с согласованием Казначейство: эквивалент 500 000 000 тенге;
- Лимит на сделку с согласованием Директора: свыше 500 000 000 тенге;
- Лимит проскальзывания: не более 0,5 % по клиентским операциям (НЦА ↔ KZT; НЦА ↔ иностранная валюта для клиентов-нерезидентов); не более 0,3 % по казначейским операциям пополнения и реализации ликвидности.

Детальные внутренние лимиты утверждаются приказом Директора в составе казначейской политики Оператора.

ГЛАВА 6. БИЗНЕС-ПРОЦЕСС «ПРИВЛЕЧЕНИЕ КЛИЕНТА» (сквозной)

6.1. Назначение процесса

Цель: обеспечить идентификацию, верификацию и оценку риска нового клиента в соответствии с требованиями ст. 5 Закона РК «О ПОД/ФТ/ФРОМУ» и Рекомендации 10 ФАТФ, а также присвоить клиенту категорию и установить применимые лимиты.

6.2. Целевые показатели

Метрика	Целевое значение	Триггер эскалации
Норматив обслуживания (SLA) полной верификации (от регистрации до активации)	< 30 минут для 80% заявок; < 24 часа для 99%	Если > 48 часов — эскалация на руководителя комплаенс-контроля
доля одобрения (отношение успешных верификаций к попыткам)	> 70%	< 50% за неделю — пересмотр настроек провайдера идентификации нерезидентов (кандидат после комплексной проверки)
доля ложных срабатываний (отказы по причинам, не связанным с реальным риском)	< 5%	> 10% — пересмотр критериев
доля отказов на этапе идентификации клиента	< 35%	> 50% — анализ пользовательского интерфейса

6.3. Сквозной процесс (детально по шагам)

Процесс привлечения клиента состоит из 12 шагов:

****Шаг 1. Регистрация****

- Клиент вводит: e-mail, номер телефона (+7 для резидентов РК), пароль; принимает Пользовательское соглашение, Политику конфиденциальности, Согласие на обработку ПД (явное согласие в форме чекбокса);
- Система формирует идентификатор клиента; устанавливает статус = «ожидает проверки»;
- Триггерные события: создание клиентского профиля, отправка письма со ссылкой подтверждения e-mail, SMS-кода подтверждения номера телефона;
- Длительность шага: 1–3 минуты.

****Шаг 2. Подтверждение каналов (подтверждение каналов связи)****

- Клиент подтверждает e-mail (одноразовая ссылка) и SMS-код (6-значный код, срок действия 5 минут);

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

- Если e-mail не подтверждён в течение 24 часов — статус "незавершённый", требуется повторная регистрация;
- Длительность шага: 1–2 минуты.

****Шаг 3. Базовая идентификация (ЦОИД для резидентов)****

- Резиденты РК — обращение в Центр обмена идентификационными данными (ЦОИД) через единый программный интерфейс (API): запрос данных по ИИН (ФИО, дата рождения, пол, адрес регистрации, статус документа);
- При успешном ответе — данные подтягиваются автоматически без необходимости предоставления удостоверения личности (УДО);
- Длительность шага: 5–15 секунд (программный интерфейс (API) ЦОИД).

****Шаг 4. Идентификация и проверка документов (для клиентов-нерезидентов)****

- Загрузка паспорта (для клиентов-нерезидентов) — фото двух сторон;
- провайдер идентификации нерезидентов (кандидат после комплексной проверки) извлекает данные через OCR + MRZ; проверка подлинности документа;
- Длительность шага: 1–3 минуты.

****Шаг 5. Биометрия (проверка живости + сличение лица)****

- Запрос на видео-селфи с проверкой «живости» (моргание/поворот головы);
- сличение лица с фото на документе через провайдер идентификации нерезидентов (кандидат после комплексной проверки) (порог совпадения $\geq 85\%$);
- При несовпадении — отказ; при сомнениях (60–85%) — ручная проверка комплаенс;
- Длительность шага: 30 секунд.

****Шаг 6. Санкционная проверка и проверка ПДЛ****

- Проверка по 7 санкционным спискам: OFAC, EU, UN, UK HMT, СНГ КФМ, РФ Росфин, Switzerland SECO;
- Проверка статуса ПДЛ через WorldCheck/Dow Jones (целевые провайдеры — раздел 1.1; до подключения — по открытым официальным источникам) — категории: ПДЛ / связанные с ПДЛ лица;

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

- При попадании в санкционный список — автоматический отказ + сообщение о подозрительной операции в АФМ РК; при выявлении ПДЛ — углублённая проверка клиента (внутренние Правила внутреннего контроля по ПОД/ФТ/ФРОМУ);
- Длительность шага: 5–15 секунд (провайдер идентификации нерезидентов (кандидат после комплексной проверки) + WorldCheck программный интерфейс (API)).

****Шаг 7. Анкета идентификации клиента и категоризация****

- Сведения о профессии, источнике дохода, цели использования платформы, ожидаемых объёмах операций;
- Тест квалификации (опционально — для статуса КИ; см. Прил. 3);
- Декларация о согласии с лимитами для НКИ или о принятии повышенных рисков для КИ;
- Длительность шага: 5–10 минут.

****Шаг 8. Скоринг риска клиента****

- Применение внутренней модели скоринга риска клиента — 6 групп факторов с весами:
 - Географический риск: 25% (страна резидентства, страна источника средств)
 - Профильный риск: 20% (профессия, отрасль, политический статус)
 - Продуктовый риск: 20% (запрашиваемые НЦА)
 - Фактор ПДЛ: 15%
 - Канальный риск: 10% (новый клиент или переход по реферальной ссылке)
 - Поведенческий риск: 10% (на этапе привлечения клиента — базовое значение)
- Итоговая оценка риска (0–100) определяет категорию: низкий (0-39), средний (40-69), высокий (70-89), очень высокий (90-100);
- Для среднего уровня → облегчённая углублённая проверка клиента; для высокого → полная углублённая проверка клиента; для очень высокого → эскалация на руководителя комплаенс-контроля и возможный отказ.

****Шаг 9. Источник происхождения средств — для стандартной проверки клиента и углублённой проверки клиента****

- Для НКИ — декларация источника средств в форме (зарплата, бизнес-доход, наследство, продажа имущества, иное);

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

- Для клиентов, проходящих углублённую проверку, — подтверждающие документы (справка с места работы, налоговые декларации, договоры).

****Шаг 10. Активация счёта****

- При прохождении всех проверок — статус «активен»;
- Открытие сегрегированных кошельков для разрешённых НЦА (на момент привлечение клиента — основные 10–15 активов; остальные открываются при первом обращении клиента);
- Установка применимых категориальных лимитов в системе.

****Шаг 11. Приветственная коммуникация****

- E-mail с приветствием, инструкциями по началу работы;
- Пуш-уведомление в мобильном приложении;
- Опциональная приветственная сессия с обучающим материалом по рискам ЦА.

****Шаг 12. Запись в реестры и архивирование****

- Создание записи в реестр клиентов;
- Архивирование документов в защищённое S3-хранилище на инфраструктуре PS Cloud Services (шифрование AES-256-GCM);
- Срок хранения: 5 лет после прекращения отношений (Закон о ПОД/ФТ/ФРОМУ).

6.4. Текстовая диаграмма потока (текстовая схема)

[Регистрация] → [Подтверждение каналов] → [программный интерфейс (API) ЦОИД / документы идентификации] → [проверка живости + сличение лица] → [санкционный скрининг и проверка ПДЛ] → [Анкета идентификации клиента + Тест] → [скоринг риска клиента] → [декларация источника происхождения средств] → [Активация / Отказ] → [приветственная коммуникация] → [Архивирование]

6.5. Точки отказа и эскалации

Шаг	Триггер	Результат
3	программный интерфейс (API) ЦОИД недоступен > 5 минут	Идентификация клиентов-резидентов осуществляется исключительно через ЦОИД; при недоступности ЦОИД идентификация резидента откладывается до восстановления сервиса. Ручная идентификация клиентов-резидентов не применяется
5	сличение лица оценка < 60%	Автоматический отказ + сохранение для расследования
5	сличение лица оценка 60-85%	Эскалация на комплаенс — ручная проверка в течение 4 часов
6	Совпадение с OFAC/UN/EU	Автоматический отказ + сообщение о подозрительной

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

		операции в АФМ РК в течение 24 часов
6	статус ПДЛ	Эскалация на руководителя комплаенс-контроля; принятие решения об углублённой проверке клиента и допуске
8	оценка риска > 90	Эскалация на руководителя комплаенс-контроля; возможный отказ

ГЛАВА 7. БИЗНЕС-ПРОЦЕСС «ОБМЕННАЯ ОПЕРАЦИЯ» (сквозной)

7.1. Назначение и виды операций

Глава регулирует жизненный цикл обменной операции от инициации клиентом до зачисления актива на сегрегированный кошелек клиента или вывода на внешний адрес.

Виды обменных операций:

- (а) купля-продажа необеспеченных цифровых активов: обмен необеспеченных цифровых активов на деньги и денег на необеспеченные цифровые активы;
- (б) с клиентами-резидентами Республики Казахстан операции совершаются в национальной валюте (тенге); с клиентами-нерезидентами — в национальной и (или) иностранной валюте;
- (в) встречное исполнение предоставляется клиенту в виде денег или необеспеченных цифровых активов в зависимости от вида совершённой операции;
- (г) сопутствующие операции в рамках исполнения обменной операции: зачисление НЦА на кошелек, открытый Оператором клиенту, и вывод НЦА на внешний адрес кошелька клиента;
- (д) обмен необеспеченных цифровых активов на необеспеченные цифровые активы (крипто-крипто) не осуществляется; операции совершаются Оператором от собственного имени и за собственные средства (пункт 27 Правил НБ № 45).

7.2. Сквозной процесс (14 шагов)

Шаг 1. Предторговые проверки

Система проверяет: (а) активный статус клиента; (б) наличие средств на балансе; (в) применимые лимиты (категориальные + ПОД/ФТ-пороги); (г) допустимость необеспеченного цифрового актива (актив включён в перечень 73 НЦА); (д) статус торгов (открыт / приостановлен / заблокирован)

Шаг 2. Запрос котировки (получение котировки)

Клиент запрашивает курс обмена. Система формирует котировку на базе: — средневзвешенного курса из независимых источников (Binance Kazakhstan / CoinGecko / Coinbase / TradingView); — Спред Оператора (см. Гл. 11): базовое значение 0,8 % в каждую сторону от средневзвешенного курса; — Комиссия Оператора (см. Гл. 12); Котировка валидна 30 секунд (идентификатор котировки + метка времени + срок действия)

Шаг 3. Подтверждение заказа

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

Клиент подтверждает заказ — фиксирует курс на 30 секунд. Создаётся идентификатор заказа, статус «ожидает исполнения». В реестре операций фиксируются: клиент, пара, направление, объём, курс, комиссия, время

Шаг 4. Проверка ПОД/ФТ в реальном времени

Система проверяет в реальном времени:
— Не превышает ли операция лимит (категориальный, ПОД/ФТ-порог);
— Адрес назначения (для вывода средств) — проверка через провайдер анализа транзакций (кандидат после комплексной проверки) (оценка риска);
— Соответствие профилю клиента (поведенческие правила мониторинга транзакций — 18 правил);
При красном флаге — операция приостанавливается до решения руководителя комплаенс-контроля

Шаг 5. Обновление внутреннего реестра

При успешной проверке — обновление внутреннего реестра: списание активов с баланса клиента-источника, зачисление на технический счёт Оператора для последующей сделки

Шаг 6. Решение о хеджировании/предварительном фондировании

Казначейство определяет источник покрытия:
(а) внутренний рынок (другой клиент с противоположной сделкой);
(б) собственная ликвидность — горячий кошелёк;
(в) хедж через лицензированные биржи цифровых активов и зарубежных лицензированных провайдеров — после получения лицензии и заключения договоров, в объёме не более 50 % согласно пункту 41 Правил НБ № 45; до заключения договоров покрытие осуществляется исключительно из собственной ликвидности (вариант (б));
Цель: минимизация открытой позиции, удержание P&L в коридоре $\pm 0,1\%$

Шаг 7. Внешний расчёт (если требуется)

При покрытии через внешнюю площадку (после заключения договоров) — формирование ордера через программный интерфейс (API) с лимитной ценой не хуже котировки клиента + спред

Шаг 8. Внутренний расчёт (зачисление клиенту)

Зачисление приобретённого актива на сегрегированный кошелёк клиента во внутреннем реестре

Шаг 9. Правило передачи данных об отправителе и получателе перевода (для внешних транзакций свыше эквивалента 500 000 тенге)

При выводе на внешний адрес провайдера услуг цифровых активов — обмен данными по протоколу TRP / TRISA / Notabene: IVMS-101 формат (отправитель: ФИО, ИИН, адрес; получатель: ФИО, адрес кошелька)

Шаг 10. Трансляция транзакции в блокчейн

Формирование транзакции в блокчейне через горячий кошелёк:
— проверка достаточности баланса горячего кошелька;
— подпись транзакции в защищённой среде (до перехода на кастодиального провайдера — единоличная подпись (собственное хранение) с контролем доступа по Главе 21; после перехода — мультиподпись 2 из 3);
— трансляция в пул неподтверждённых транзакций сети;
— ожидание подтверждений (3 для BTC, 12 для ETH, 1 для TRX);
В случае нехватки ликвидности на горячем кошельке — пополнение из резервных кошельков Оператора (после внедрения многоуровневой структуры хранения — перемещение средств из тёплого уровня, Глава 21)

Шаг 11. Отслеживание подтверждений

Система отслеживает подтверждения он-чейн. Клиенту отправляются промежуточные уведомления (в обработке → подтверждено). После N подтверждений — статус заказ = «исполнено»

Шаг 12. Посделочная реконсиляция

Сверка: внутренний реестр с он-чейн балансом и балансом СЕХ (если применялся хедж). Допустимое расхождение < 0,001 BTC (экв.) — иначе эскалация на Казначейство

Шаг 13. Уведомление клиента

Пуш-уведомление + e-mail (опционально SMS) с деталями: курс, сумма, комиссия, время, хэш транзакции (для внешнего вывода)

Шаг 14. Отчётность и архивирование

Запись в журнал операций; ежедневная агрегация для отчёта НБ РК; архив транзакции — 5 лет

7.3. Целевые показатели

Метрика	Целевое значение
Время от подтверждения заказа до внутреннего расчёта	< 5 секунд (P95)
Время от подтверждения заказа до он-чейн подтверждения (BTC)	< 60 минут (P95)
Проскальзывание (отклонение фактического курса от котированного)	< 0,2% (P95)
Доля несостоявшихся сделок	< 0,5%
Внутридневное отклонение открытой позиции (P&L)	< 0,1%

ГЛАВА 8. БИЗНЕС-ПРОЦЕСС «ДЕПОЗИТ / ВЫВОД СРЕДСТВ»

8.1. Депозит НЦА (зачисление с внешнего адреса)

Шаги:

- 1) Клиент запрашивает в личном кабинете адрес для зачисления определённого НЦА. До перехода на кастодиального провайдера зачисление осуществляется на адрес Оператора в соответствующей сети блокчейн согласно Реестру адресов кошельков (Приложение № 2); поступление привязывается к клиенту по уникальному идентификатору заявки (идентификатор заказа), а в сетях с поддержкой идентификатора платежа (назначение tag, служебная записка) — также по нему; в иных сетях — по сопоставлению заявленной клиентом транзакции (сумма, хэш, адрес отправителя из профиля идентификации клиента). После перехода на кастодиального провайдера (BitGo Trust Company) уникальные адреса для каждого клиента генерируются через программный интерфейс (API) кастодиана (HD-паттерн, выделенный адрес на клиента).
- 2) Адрес отображается клиенту с предупреждением о минимальной сумме (чтобы избежать пылевых атак) и об обязательном использовании именно этой сети (например, USDT-TRC20 vs USDT-ERC20).
- 3) При поступлении транзакции в блокчейн — система обнаруживает её через блокчейн-обозреватель и помещает в очередь зачислений (в обработке).
- 4) После N подтверждений (BTC: 3, ETH: 12, TRX: 1, BNB: 15, SOL: 32):
 - проверка адреса отправителя через провайдер анализа транзакций (кандидат после комплексной проверки) (оценка риска);
 - если оценка риска > высокий — операция блокируется, активы возвращаются отправителю (минус газ), формируется сообщение о подозрительной операции;
 - если оценка риска = низкий/средний — зачисление на внутренний баланс клиента, перевод избытка на резервное хранение (после внедрения многоуровневой структуры — перемещение средств в холодный уровень по достижении порога, Глава 21).
- 5) Уведомление клиента; запись в журнал зачислений.

8.2. Вывод НЦА (на внешний адрес)

Шаги:

- 1) Клиент инициирует вывод: выбирает НЦА, указывает сумму и адрес назначения.
- 2) проверка владения адресом для некастодиальных кошельков при переводе свыше эквивалента 500 000 тенге: подтверждение владения адресом — микро-депозит или подпись сообщения (для адресов с поддержкой).
- 3) правило передачи данных об отправителе и получателе перевода (для провайдера услуг цифровых активов — получателя): обмен данными через TRP/TRISA/Notabene.

4) проверка ПОД/ФТ в реальном времени: проверка адреса назначения через провайдер анализа транзакций (кандидат после комплексной проверки).

5) 2FA подтверждение клиентом (TOTP / SMS / ссылку по электронной почте).

6) период охлаждения для новых получателей: для впервые используемых внешних адресов при сумме свыше эквивалента 5 000 000 тенге — задержка 24 часа.

7) Подпись транзакции в защищённой среде (до перехода на кастодиального провайдера — единоличная подпись (собственное хранение) с контролем доступа; после перехода — мультиподпись 2 из 3 для горячих, 3 из 5 для тёплых кошельков).

8) Трансляция транзакции и отслеживание подтверждений; уведомление клиента.

8.3. Депозит фиата (KZT)

1) Клиент инициирует депозит KZT в личном кабинете — указывает сумму.

2) Система формирует платёжное поручение с уникальным идентификатором платежа (идентификатор клиента + одноразовый код).

3) Клиент совершает перевод со своего банковского счёта на отдельный операционный (клиентский) банковский счёт Оператора в банке второго уровня (открывается до начала клиентских операций в соответствии с Главой 27 настоящих Правил; реквизиты доводятся до клиента в личном кабинете) с указанием идентификатора платежа в назначении платежа.

4) При поступлении средств: автоматическая сверка по идентификатору платежа; ПОД/ФТ-проверка плательщика; зачисление на внутренний KZT-баланс клиента в течение 30 минут после поступления; при сложности идентификации — ручная проверка комплаенс.

8.4. Вывод фиата (KZT)

1) Клиент инициирует вывод KZT, указывая реквизиты своего банковского счёта (собственного, не третьего лица).

2) Сверка ФИО банковского счёта с ФИО клиента (по идентификации клиента). При несовпадении — отказ.

3) ПОД/ФТ-проверка; для новых реквизитов > 1 000 000 ₸ — задержка 24 часа.

4) Формирование платёжного поручения; авторизация в интернет-банке обслуживающего банка.

5) Норматив (SLA) вывода KZT: T+0 (в течение того же рабочего дня) для сумм < 10 млн ₸; T+1 — для сумм > 10 млн ₸.

ГЛАВА 9. БИЗНЕС-ПРОЦЕСС «ПОДАЧА СООБЩЕНИЙ О ПОДОЗРИТЕЛЬНЫХ И ПОРОГОВЫХ ОПЕРАЦИЯХ»

9.1. Триггеры формирования сообщения о подозрительной операции

Сообщение о подозрительной операции формируется при наступлении одного из следующих событий:

- (а) Хит по санкционному списку (OFAC/UN/EU/UK/KZ-KFM/RU-Rosfin/CH-SECO);
- (б) Совпадение с перечнем ФТФР КФМ РК;
- (в) Сработка одного из 18 правил мониторинга транзакций с приоритетом высокий/критический;
- (г) Адрес провайдера услуг цифровых активов-контрагента имеет оценку риска «высокий» или «критический» в провайдере анализа транзакций (кандидат после комплексной проверки);
- (д) Признаки дробления операций (см. п. 5.2);
- (е) Отказ клиента от предоставления сведений об источнике происхождения средств и благосостояния при запросе углублённой проверки клиента;
- (ж) Обоснованное подозрение работника о связи операции с легализацией преступных доходов или финансированием терроризма;
- (з) Операция превышает порог пороговой операции, установленный пунктом 1 статьи 4 Закона Республики Казахстан «О ПОД/ФТ/ФРОМУ», без обоснования профиля клиента.

9.2. Триггеры формирования сообщения о пороговой операции

Сообщение о пороговой операции формируется:

- при совершении операции, подлежащей финансовому мониторингу, в размере, равном или превышающем пороговое значение, установленное статьёй 4 Закона Республики Казахстан «О ПОД/ФТ/ФРОМУ», — в порядке и сроки, установленные указанным Законом;
- внутренние дополнительные триггеры усиленного контроля (не заменяют требования Закона): достижение неквалифицированным клиентом суточного лимита 7 000 000 ₸;
- суммарный объём операций одного клиента свыше 50 000 000 тенге за календарный месяц.

9.3. Сквозной процесс формирования сообщения о подозрительной операции (10 шагов)

Шаг 1. Срабатывание триггера в системе мониторинга транзакций (автоматически) или инициация работником вручную (через защищённую форму).

Шаг 2. Формирование внутреннего сигнала с приоритетом и описанием.

Шаг 3. Расследование проводит ответственный работник по ПОД/ФТ/комплаенс в течение 24 часов:

- изучение истории операций клиента;

- повторная проверка документов идентификации клиента;
- сбор он-чейн контекста через провайдер анализа транзакций (кандидат после комплексной проверки) / Chainalysis;
- интервью с работником (если триггер ручной).

Шаг 4. Принятие решения ответственным работником по ПОД/ФТ: «Подозрительно» / «Не подозрительно». Все случаи документируются в журнале расследований.

Шаг 5. При «Подозрительно»:

- приостановка операций клиента (блокировка счёта);
- заполнение формы сообщения о подозрительной операции в формате АФМ РК;
- согласование с руководителем комплаенс-контроля.

Шаг 6. Отправка сообщения о подозрительной операции в АФМ РК через защищённый канал (не позднее 24 часов с момента квалификации операции как подозрительной).

Шаг 7. Принцип «запрет на разглашение» — категорический запрет на уведомление клиента о факте подачи сообщения о подозрительной операции (Закон о ПОД/ФТ/ФРОМУ).

Шаг 8. Ожидание решения АФМ РК; при отсутствии указаний в течение 7 рабочих дней — возможное снятие блокировки по решению руководителя комплаенс-контроля.

Шаг 9. Архивирование материалов расследования и сообщения о подозрительной операции — 5 лет (Закон «О ПОД/ФТ») / 10 лет (внутренний регламент).

Шаг 10. Включение случая в ежеквартальный отчёт руководителя комплаенс-контроля; окончательное решение — за Директором.

9.4. SLA и контрольные точки

Точка	SLA	Эскалация
От триггера до начала расследования	< 2 часа	руководитель комплаенс-контроля
От начала до решения	< 24 часа	руководитель комплаенс-контроля + Директор
От решения «Подозрительно» до отправки в АФМ	< 24 часа	руководитель комплаенс-контроля + Директор
Общая длительность процесса	< 48 часов	Единственный участник

ГЛАВА 10. РЕГЛАМЕНТ РАБОТЫ, НОРМАТИВЫ ОБСЛУЖИВАНИЯ (SLA), КАНАЛЫ ПОДДЕРЖКИ

10.1. Режим работы платформы

С даты начала оказания услуг (после получения лицензии) платформа доступна 24/7/365 за исключением запланированных технических работ. Внутренний регламент операционной службы: 24/7 на 1 линии поддержки, 8/5 на эскалационных линиях. В соответствии с пунктом 36 Правил НБ № 45 Оператор обеспечивает непрерывность функционирования интернет-ресурса, мобильного приложения и цифровой инфраструктуры, а также конфиденциальность, целостность и доступность данных цифровых систем Оператора. Целевой уровень доступности публичных цифровых сервисов — не ниже 99,5 % (за исключением плановых работ и обстоятельств непреодолимой силы); целевые показатели восстановления: RPO не более 24 часов, RTO не более 8 часов для критичных систем. Меры обеспечения непрерывности (резервирование инфраструктуры, ежедневное резервное копирование, тестирование восстановления, планы аварийного восстановления) приведены в Главе 23 настоящих Правил и плане непрерывности деятельности Оператора.

10.2. Каналы поддержки

Канал	Доступность	Тип запросов	SLA ответа
Чат в личном кабинете	24/7	Все виды запросов	< 5 минут
E-mail support@ausu.kz	24/7	Сложные запросы, документы	< 4 часов
Телефон +7 707 767 17 06	Пн-Пт 09:00-21:00	Срочные блокировки	< 1 минуты
Telegram-bot	24/7	Базовая поддержка, частые вопросы	< 2 минут
Письменное обращение в офис	Пн-Пт 09:00-18:00	Официальные заявления	< 10 раб. дней

10.3. Регламентные технические работы

Плановые работы (планируются с уведомлением за 48 часов): ночное окно 02:00–04:00 по времени Шымкента (UTC+5). Длительность одной сессии — не более 2 часов. Совокупно — не более 4 часов в месяц.

ГЛАВА 11. КУРСООБРАЗОВАНИЕ, СПРЕД, ОРАКУЛЫ ЦЕН

11.1. Источники цен (оракулы)

Справедливый рыночный курс формируется как средневзвешенная цена из четырёх независимых источников:

- Binance Kazakhstan (публичный программный интерфейс (API) лицензированной в РК площадки);
- CoinGecko (публичный агрегатор);
- Coinbase (публичный программный интерфейс (API));
- TradingView (верификация на резкие отклонения).

Если расхождение между источниками $> 1\%$ — котировки временно отключаются до выяснения причин (автоматический останов торгов).

11.2. Спред Оператора

Базовый спред Оператора — $0,8\%$ в каждую сторону (покупка/продажа) от средневзвешенного курса.

По категориям пар спред устанавливается в следующих диапазонах:

Категория пары	Спред (покупка/продажа)	Пример
Топ-10 НЦА (BTC, ETH и др.) ↔ KZT	$0,3\% - 0,8\%$	BTC/KZT
Топ-50 НЦА ↔ KZT	$0,5\% - 1,0\%$	XRP/KZT
Прочие НЦА перечня ↔ KZT	$1,0\% - 2,0\%$	Согласно перечню
НЦА ↔ иностранная валюта (USD/EUR, безналично, только клиенты-нерезиденты)	$0,3\% - 1,0\%$	BTC/USD

11.3. Окно валидности котировки

Котировка валидна 30 секунд с момента отображения клиенту. При волатильности $> 5\%$ за 1 час — окно сокращается до 15 секунд (волатильный режим).

ГЛАВА 12. ТАРИФЫ И КОМИССИИ

12.1. Структура комиссий

Услуга	Тариф	Минимум	Максимум
Обмен KZT → криптоактив	0,30 %	500 ₸	—
Обмен криптоактив → KZT	0,30 %	500 ₸	—
Обмен USD/EUR/RUB/CNY → криптоактив (нерезиденты)	0,30 %	эквивалент 500 тенге	—
Зачисление криптоактива	0 %	—	—
Зачисление KZT	0 %	—	—
Вывод BTC	0,0005 BTC	—	—
Вывод ETH	0,005 ETH	—	—
Вывод USDT (TRC-20)	1 USDT	—	—
Вывод USDT (ERC-20)	15 USDT	—	—
Вывод KZT	0,1 %	500 ₸	50 000 ₸
Хранение при неактивности счёта свыше 12 месяцев	0,01 % в месяц	500 тенге	—

Минимальные суммы операций:

Тип операции	Минимум
Зачисление криптоактива	эквивалент 2 500 тенге (защита от пылевых переводов)
Зачисление KZT	1 000 ₸
Обмен KZT ↔ криптоактив	5 000 ₸
Вывод криптоактива	эквивалент 10 000 тенге + сетевая комиссия
Вывод KZT	5 000 ₸

Программа лояльности (скидка от базового тарифа): при ежемесячном обороте свыше 50 000 000 тенге комиссии снижаются на 30 %, свыше 500 000 000 тенге — на 50 %. Скидка применяется автоматически с первого числа месяца, следующего за расчётным.

ГЛАВА 13. ЗАЩИТА ПРАВ ПОТРЕБИТЕЛЕЙ И ЖАЛОБЫ

13.1. Принципы защиты прав потребителей

Оператор реализует требования Закона Республики Казахстан «О защите прав потребителей»:

- (а) право клиента на полную и достоверную информацию о тарифах, рисках, условиях обслуживания;
- (б) право на безопасность активов (сегрегация учёта, многоуровневый контроль доступа; после перехода на кастодиальную инфраструктуру — мультиподпись и страховое покрытие кастодиана);
- (в) право на доступ к собственным средствам без необоснованных ограничений;
- (г) право на справедливое рассмотрение жалоб.

13.2. Порядок подачи и рассмотрения жалобы

Шаги:

- 1) Подача через любой из 5 каналов поддержки (см. п. 10.2).
- 2) Регистрация в реестр жалоб (присвоение тикета, фиксация SLA).
- 3) Категоризация:
 - Уровень 1 (информационный) — SLA ответа < 24 часа;
 - Уровень 2 (операционный — задержка зачисления, тех. вопрос) — SLA < 3 раб. дня;
 - Уровень 3 (финансовый — потеря средств, неправильный курс) — SLA < 10 раб. дней;
 - Уровень 4 (регуляторный — нарушение ПОД/ФТ, ПД) — SLA < 30 кал. дней с обязательным уведомлением руководителя комплаенс-контроля + Юриста.
- 4) Расследование с привлечением соответствующих ответственных работников.
- 5) Ответ клиенту в письменной форме с указанием решения и обоснования.
- 6) Если клиент не удовлетворён — эскалация на Директора; клиент вправе обратиться в Национальный Банк Республики Казахстан и (или) в уполномоченный орган в сфере защиты прав потребителей.
- 7) Архивирование жалобы — 5 лет.

13.3. Судебная защита и иные способы защиты прав

Клиент сохраняет право на:

- возмещение причинённого по вине Оператора ущерба исходя из фактически причинённого клиенту ущерба, с возвратом денег и (или) необеспеченных цифровых активов клиенту;
- обращение в Национальный Банк Республики Казахстан — орган, осуществляющий регулирование, контроль и надзор за деятельностью операторов обмена необеспеченных цифровых активов;

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

— судебную защиту по месту нахождения Оператора (г. Шымкент).

ГЛАВА 14. КОНФИДЕНЦИАЛЬНОСТЬ И ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. Категории обрабатываемых ПД

Категория	Состав данных	Правовое основание
Идентификационные	ФИО, ИИН, дата рождения, гражданство, УДО (серия, номер, дата выдачи)	Закон «О ПОД/ФТ» ст. 5; согласие клиента
Контактные	E-mail, телефон, адрес регистрации, адрес проживания	Договорные обязательства; согласие клиента
Биометрические	Фото селфи, видео проверки живости, биометрический шаблон лица	Явное согласие клиента (Закон РК «О персональных данных и их защите»)
Финансовые	Источник средств, банковские реквизиты, история операций	Закон «О ПОД/ФТ»; договорные обязательства
Поведенческие	IP-адрес, геолокация, история сессий, цифровой отпечаток устройства	Законный интерес (информационная безопасность)
Налоговые	сертификат налогового резидентства, FATCA/CRS-статус	Кодекс РК «О налогах и других обязательных платежах в бюджет» (Налоговый кодекс); CRS/FATCA

14.2. Сроки хранения

Все категории ПД хранятся в течение действия отношений с клиентом и 5 (пяти) лет после прекращения отношений (Закон о ПОД/ФТ/ФРОМУ). Для биометрических данных — отдельный срок 3 года после последней авторизации.

14.3. Право на удаление и портативность

Клиент имеет право:

- (а) на доступ к собственным ПД (запрос обрабатывается в течение 30 дней);
- (б) на исправление неточных данных;
- (в) на удаление — после истечения обязательного срока хранения (5 лет);
- (г) на переносимость — выгрузка истории операций в CSV/JSON.

ГЛАВА 15. ХРАНЕНИЕ ЗАПИСЕЙ И АРХИВИРОВАНИЕ

15.1. Реестры, ведомые Оператором

Реестр	Содержание	Срок хранения
реестр клиентов	Все клиенты с их статусами и категориями	5 лет после прекращения
журнал операций	Все обменные операции (идентификатор заказа, время, объём, курс, комиссия)	5 лет
журнал зачислений и выводов	Все депозиты и выводы с он-чейн хэшами	5 лет
Архив документов идентификации/стандартной проверки клиента	Документы идентификации и анкеты	5 лет после прекращения
журнал расследований	Расследования по триггерам мониторинга транзакций	10 лет
Архив сообщений о подозрительных и пороговых операциях	Отправленные сообщения в АФМ РК	10 лет
реестр жалоб	Все жалобы клиентов и решения	5 лет
Реестр адресов кошельков	Реестр кошельков с приватными ключами (зашифровано)	Бессрочно
журнал реконсиляции	Ежедневные результаты реконсиляции	5 лет
журнал отчётности	Отчёты НБ РК и АФМ РК	5 лет

В соответствии с пунктом 31 Правил НБ № 45 Оператор хранит сведения о сделках с цифровыми активами и сведения, полученные по результатам надлежащей проверки, не менее 5 (пяти) лет со дня прекращения деловых отношений с клиентом.

15.2. Техническая реализация архивирования

Архив располагается на 2-х типах хранилищ:

- Оперативный архив (1 год) — PostgreSQL + объектное S3-хранилище на инфраструктуре PS Cloud Services (резидент Республики Казахстан);
- Долгосрочный архив (>1 года) — S3-хранилище PS Cloud Services с шифрованием AES-256-GCM + WORM-режим (однократная запись, многократное чтение).

Резервные копии: ежедневная инкрементальная + еженедельная полная; хранятся в географически удалённом ЦОД (Алматы) в течение 30 дней.

ГЛАВА 16. ВНУТРЕННИЙ КОНТРОЛЬ И МОНИТОРИНГ

16.1. Линии защиты

Линия	Кто	Что
1-я линия	Операционные работники, ИТ	Первичный контроль в процессе работы: идентификация клиента, ПОД/ФТ, технические проверки
2-я линия	комплаенс, управление рисками	Независимая проверка эффективности контролей 1-й линии; расследования по мониторингу транзакций; KRI/КПЭ
3-я линия	Внутренний аудитор	Независимая оценка эффективности всех контролей; ежегодные аудиты по утверждённому плану

16.2. Ключевые контроли (ключевые показатели контроля)

КПЭ-001: 100% операций проверены по правилам ПОД/ФТ (ежедневная сверка сигналов и сделок);

КПЭ-002: Реконсиляция внутреннего реестра vs он-чейн — ежедневно, отклонение < 0,001 BTC;

КПЭ-003: санкционный скрининг — 100% клиентов, ежедневное обновление списков;

КПЭ-004: контроль целостности ключей и схемы подписи кошельков — ежемесячная тестовая транзакция для всех кошельков (после внедрения мультиподписи — проверка кворума подписей);

КПЭ-005: целостность резервных копий — еженедельный тестирование восстановления;

КПЭ-006: норматив обслуживания поставщиков (SLA) — ежемесячный отчёт по всем критическим вендорам.

ГЛАВА 17. ПРЕКРАЩЕНИЕ УСЛУГ И РАСТОРЖЕНИЕ ДОГОВОРА

17.1. Основания для прекращения по инициативе Оператора

- (а) санкционное совпадение по клиенту (немедленно);
- (б) отказ клиента от углублённой проверки клиента при наличии триггеров (30 дней);
- (в) неактивность счёта > 24 месяцев с балансом > 0 (с уведомлением за 90 дней);
- (г) систематическое нарушение клиентом условий обслуживания (3+ предупреждения);
- (д) указание правоохранительных органов или АФМ РК;
- (е) утрата лицензии Оператором (с уведомлением за 30 дней + порядок возврата активов).

17.2. Основания по инициативе клиента

Клиент вправе в любой момент: (а) подать заявление о расторжении; (б) запросить вывод всех активов и удаление аккаунта; (в) реализовать право на портативность данных (CSV/JSON-выгрузка).

17.3. Процедура расторжения

- 1) Заявление от клиента или решение Оператора с обоснованием.
- 2) Расчёт и возврат остатков активов на указанные клиентом адреса (в пределах 14 рабочих дней).
- 3) Сохранение записей и архивов в течение установленных сроков (см. Гл. 15).
- 4) Удаление активных учётных данных в системе; обезличивание ПД по истечении 5 лет.

ГЛАВА 18. ПОРЯДОК И УСЛОВИЯ РАБОТЫ ФИЗИЧЕСКИХ ОТДЕЛЕНИЙ И ПУНКТОВ САМООБСЛУЖИВАНИЯ

(пункт 23 подпункт 4 Правил НБ № 45; пункты 34, 36, 38, 39)

18.1. Общие положения (пункт 34 Правил НБ № 45)

Оператор осуществляет операции по продаже необеспеченных цифровых активов за наличную национальную валюту посредством физических отделений и (или) пунктов самообслуживания, а также безналичным способом посредством мобильного приложения или иного дистанционного способа обслуживания (пункт 34 Правил НБ № 45), а именно посредством:

- 1) физических отделений, открываемых по адресам, утверждённым Единственным участником Оператора;
- 2) пунктов самообслуживания (криптоматов), размещаемых в общественных местах;
- 3) безналичным способом — посредством веб-сайта ausu.kz, мобильного приложения или иного дистанционного способа обслуживания.

18.2. Требования к физическому отделению (пункт 38 Правил НБ № 45)

Каждое физическое отделение Оператора соответствует требованиям:

- 1) отделение является отдельно стоящим зданием либо находится внутри коммерческих или офисных помещений (зданий); не допускается размещение в жилых помещениях, на стихийных рынках, в передвижных торговых точках;
- 2) отделение оборудовано охранной сигнализацией с подключением к пульту охраны, а также тревожной кнопкой для экстренного вызова частной охранной организации; на каждом рабочем месте кассира установлена тревожная кнопка скрытного нажатия;
- 3) в отделении на видимом для обозрения клиентами месте размещаются данные об Операторе — полное наименование, БИН, юридический адрес, номер и дата лицензии НБ РК, контактные данные (телефон, e-mail, сайт);
- 4) работник Оператора проводит идентификацию клиента перед проведением каждой его операции в соответствии с Законом РК «О ПОД/ФТ/ФРОМУ»: предъявление клиентом удостоверения личности (УДО), фиксация данных УДО в системе Оператора, фотографирование документа (с согласия клиента), сверка фото на УДО с клиентом визуально и через систему распознавания лиц.

Дополнительные внутренние требования Оператора к физическим отделениям:

- наличие системы видеонаблюдения с записью и хранением видеоархива не менее 90 (девяноста) календарных дней;
- наличие сейфа Класса I и выше для хранения наличных денежных средств свыше 1 000 000 ₸;

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

— наличие резервного электропитания (ИБП) для бесперебойной работы кассового программного обеспечения;

— наличие пожарной сигнализации, огнетушителей.

18.3. Требования к пункту самообслуживания (криптомату) (пункт 39 Правил НБ № 45)

Каждый пункт самообслуживания Оператора соответствует требованиям:

- 1) пункт самообслуживания осуществляет передачу данных о проведённых операциях Оператору в режиме реального времени по защищённому каналу связи (VPN, TLS 1.3) с отображением статуса операции в централизованной системе мониторинга;
- 2) пункт самообслуживания имеет защиту от взлома: антивандальный корпус, сейф для денежных средств, охранный замок, датчик движения и вскрытия корпуса с передачей сигнала в централизованную систему мониторинга и в частную охранную организацию;
- 3) в пункте самообслуживания на видимом для обозрения клиентами месте размещаются данные о владельце пункта самообслуживания — полное наименование, БИН, номер и дата лицензии НБ РК, контактные данные, телефон службы поддержки 24/7;
- 4) оборудование проводит идентификацию клиента перед проведением каждой его операции: считывание УДО клиента через слот сканирования; распознавание лица клиента через встроенную видеокамеру; сверка биометрических данных с ЦОИД через программный интерфейс (API)-подключение Оператора;
- 5) проведение сервисного обслуживания пункта самообслуживания в соответствии с регламентом сервисного обслуживания: профилактика — не реже 1 раза в квартал; инкассация — не реже 1 раза в месяц либо при заполнении купюроприёмника на 80 %; устранение технических неисправностей — в течение 24 часов; обновление программного обеспечения — по согласованному графику.

18.4. Мониторинг в режиме реального времени (пункт 36 Правил НБ № 45)

Оператор обеспечивает в режиме реального времени мониторинг состояния физических отделений и пунктов самообслуживания:

- 1) статус функционирования (доступен / недоступен / в обслуживании / в инкассации);
- 2) количество наличных средств в кассе физического отделения и в купюроприёмнике пункта самообслуживания;
- 3) отображение статуса и сведений об оказанной услуге в личном кабинете клиента (при условии открытия личного кабинета): номер операции, дата и время, сумма, хэш транзакции в блокчейне.

Централизованная система мониторинга обеспечивает информирование Ответственного работника по ИТ-инфраструктуре в течение 5 минут с момента сбоя или нештатной ситуации в физическом отделении или пункте самообслуживания.

18.5. График ввода в эксплуатацию

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

На дату подачи заявления о выдаче лицензии Оператор деятельность оператора обмена необеспеченных цифровых активов не осуществляет: подготовлены демонстрационный интернет-ресурс ausu.kz и мобильное приложение. Оказание услуг начинается исключительно после получения лицензии Национального Банка Республики Казахстан и осуществляется дистанционным способом посредством интернет-ресурса ausu.kz и мобильного приложения.

Открытие первого физического отделения планируется в течение 12 (двенадцати) календарных месяцев с даты выдачи лицензии; адрес физического отделения определяется решением единственного участника с соблюдением требований пункта 38 Правил НБ № 45.

Установка первых пунктов самообслуживания планируется в течение 18 (восемнадцати) календарных месяцев с даты выдачи лицензии.

О каждом случае открытия физического отделения или установки пункта самообслуживания Оператор уведомляет Национальный Банк РК в течение 5 (пяти) рабочих дней с приложением документов, подтверждающих соблюдение требований пунктов 38-39 Правил НБ № 45.

ГЛАВА 19. ПОРЯДОК И СРОКИ ЗАВЕРШЕНИЯ РАСЧЁТОВ ПО СДЕЛКАМ

(пункт 23 подпункт 5 Правил НБ № 45; пункты 33, 37, 40)

19.1. Жизненный цикл расчёта (пункт 33 Правил НБ № 45)

Жизненный цикл одной обменной операции состоит из следующих этапов:

Этап 1. Заявка клиента и котировка. Клиент в личном кабинете либо в физическом отделении формирует заявку с указанием вида операции (покупка/продажа), НЦА, объёма. Оператор предоставляет котировку, валидную в течение 30 секунд.

Этап 2. Подтверждение заявки. При согласии клиента с котировкой формируется заявка с уникальным идентификатором (идентификатор заказа) и присваивается статус «ожидает исполнения».

Этап 3. Получение Оператором актива от клиента:

— при покупке клиентом НЦА — клиент перечисляет денежные средства на банковский счёт Оператора (для дистанционных операций) либо вносит наличные деньги через кассу физического отделения / купюроприёмник пункта самообслуживания (только в KZT);

— при продаже клиентом НЦА — клиент переводит НЦА на адрес кошелька Оператора.

Этап 4. Встречное исполнение Оператором. Оператор передаёт клиенту встречное исполнение в течение 2 (двух) рабочих дней с момента получения от клиента денег или цифровых активов:

— при покупке клиентом НЦА — Оператор переводит НЦА на адрес кошелька клиента (внутренний кошелёк в Личном кабинете либо внешний адрес);

— при продаже клиентом НЦА — Оператор перечисляет денежные средства на банковский счёт клиента (только безналичный способ).

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

Этап 5. Документирование операции (пункт 40 Правил НБ № 45). После оказания услуги Оператор выдаёт клиенту документ, подтверждающий совершение операции (квитанция в электронном виде в личном кабинете с возможностью загрузки в PDF, дублирование на e-mail клиента; в физическом отделении — также бумажный чек с QR-кодом для проверки операции в личном кабинете).

19.2. Контрольный срок расчёта (пункт 33 Правил НБ № 45)

Срок встречного исполнения по сделке — не более 2 (двух) рабочих дней с момента получения Оператором денежных средств или цифровых активов от клиента.

Целевой (фактический) срок исполнения для дистанционных операций:

— при покупке клиентом НЦА за безналичные KZT — не более 30 минут с момента зачисления денег на банковский счёт Оператора;

— при продаже клиентом НЦА — не более 60 минут с момента подтверждения входящей транзакции в блокчейне (N подтверждений: 3 для BTC, 12 для ETH, 1 для TRX).

В случае невозможности исполнения в контрольный срок (технический сбой, санкционное совпадение, расследование ПОД/ФТ) — операция возвращается клиенту с восстановлением исходного актива; уведомление клиента — в течение 4 часов; обоснование задержки фиксируется в Реестре задержанных операций.

19.3. Зачисление наличных на банковский счёт (пункт 37 Правил НБ № 45)

Остатки наличных денежных средств, поступивших в физические отделения и пункты самообслуживания, зачисляются на собственный банковский счёт Оператора (хозяйственный счёт KZ598853010011580000 в АО «ДБ «Казахстан-Зираат Интернешнл Банк» (далее — КЗИ Банк)) не реже 1 (одного) раза в месяц.

Внутренний регламент инкассации устанавливает более частую периодичность:

— ежедневная инкассация при остатке наличных > 5 000 000 ₸;

— еженедельная инкассация при остатке наличных от 1 000 000 ₸ до 5 000 000 ₸;

— ежемесячная инкассация при остатке < 1 000 000 ₸.

19.4. Учёт операций и реконсиляция

Оператор ведёт ежедневный учёт операций в Реестре операций с цифровыми активами с указанием: идентификатор заказа, дата и время, ИИН/паспорт клиента, НЦА, объём, курс, комиссия, способ исполнения, хэш транзакции в блокчейне, статус.

Ежедневная реконсиляция включает:

1) сверка внутреннего реестра балансов клиентов с балансами кошельков Оператора в каждой сети блокчейн (по каждому НЦА);

2) сверка движения денежных средств на банковских счетах Оператора с данными внутреннего реестра;

3) сверка инкассированных наличных с данными физических отделений и пунктов самообслуживания.

Расхождения фиксируются в Журнале реконсиляции, исследуются работником финансовой службы под контролем Директора и устраняются в течение 1 рабочего дня.

ГЛАВА 20. ИСТОЧНИКИ ПОПОЛНЕНИЯ ЛИКВИДНОСТИ И РЕАЛИЗАЦИЯ ИЗЛИШНЕЙ ЛИКВИДНОСТИ

(пункт 23 подпункт 6 Правил НБ № 45; пункт 41)

20.1. Принципы управления ликвидностью

1) Поскольку Оператор совершает операции от собственного имени и за собственные средства (пункт 27 Правил НБ № 45), Оператор обязан поддерживать достаточный уровень ликвидности в каждом виде НЦА и в национальной/иностранной валюте для своевременного встречного исполнения по сделкам клиентов в течение 2 рабочих дней.

2) Оператор устанавливает минимальные и максимальные уровни остатков по каждому НЦА (лимиты остатков) и осуществляет пополнение или реализацию излишков для поддержания целевого уровня.

3) Управление ликвидностью осуществляется Ответственным работником по управлению рисками совместно с Директором Оператора.

20.2. Источники пополнения ликвидности в НЦА

1) Эмитенты НЦА — приобретение НЦА у эмитентов в соответствии с пунктом 41 абзац 1 Правил НБ № 45;

2) Провайдеры услуг цифровых активов, имеющие лицензию (разрешение) регулирующих органов иностранных государств — приобретение НЦА у лицензированных иностранных провайдеров (Binance, Coinbase, Kraken, OKX, Bitget и иные) в объёме, не превышающем 50 (пятьдесят) процентов от общего объёма приобретаемых либо продаваемых НЦА провайдерам услуг цифровых активов в течение 6 (шести) последних календарных месяцев — пункт 41 абзац 2 Правил НБ № 45;

3) Покупка НЦА у клиентов Оператора — по сделкам в рамках основной деятельности (только безналично, пункт 35 Правил НБ № 45);

4) перераспределение собственной ликвидности между кошельками Оператора в разных сетях блокчейн (без совершения операций обмена с третьими лицами вне подпунктов 1)–3) настоящего пункта).

20.3. Контроль соблюдения лимита 50 % (пункт 41 абзац 2 Правил НБ № 45)

Ответственный работник по управлению рисками ежемесячно (не позднее 10 числа месяца, следующего за отчётным) рассчитывает по каждому НЦА:

$V_{\text{лиц}}$ = объём НЦА, приобретённый у лицензированных иностранных провайдеров за последние 6 месяцев;

$V_{\text{общ}}$ = общий объём НЦА, приобретённый/проданный провайдерам услуг ЦА за последние 6 месяцев;

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

Доля лицензированных = $V_{\text{лиц}} / V_{\text{общ}} \times 100 \%$.

Если доля приближается к 45 % — формируется красный флаг; запрещается дальнейшее приобретение у лицензированных провайдеров до выравнивания. Если доля превышает 50 % — Ответственный работник по управлению рисками обязан в 5-дневный срок сформировать отчёт о нарушении лимита и план корректирующих действий.

20.4. Реализация излишней ликвидности в НЦА

При превышении максимального уровня запасов по конкретному НЦА Оператор реализует излишек путём:

- 1) продажи НЦА клиентам Оператора (внутренний рынок);
- 2) продажи НЦА эмитентам (при наличии программы выкупа у эмитента);
- 3) продажи НЦА лицензированным иностранным провайдерам в пределах лимита 50 %;
- 4) реализации излишка в порядке подпунктов 1)–3) настоящего пункта с последующим приобретением более ликвидных НЦА (BTC, ETH, USDT) у эмитентов либо лицензированных иностранных провайдеров в пределах лимита 50 % и хранением в составе резерва ликвидности.

20.5. Резерв ликвидности в национальной валюте

Оператор поддерживает на хозяйственном банковском счёте в КЗИ Банке резерв ликвидности в национальной валюте в размере, обеспечивающем встречное исполнение обязательств перед клиентами на горизонте не менее 7 (семи) календарных дней — без необходимости реализации НЦА. Минимальный неснижаемый остаток — 30 000 000 ₸.

20.6. Запрет привлечения заёмных средств для обеспечения ликвидности

Оператор не привлекает заёмные средства (займы, кредиты, овердрафты) для обеспечения ликвидности по операциям с клиентами. Все операции финансируются исключительно за счёт собственных средств (уставного капитала, нераспределённой прибыли).

ГЛАВА 21. ПОРЯДОК И УСЛОВИЯ ОТКРЫТИЯ И ВЕДЕНИЯ КОШЕЛЬКОВ ЦИФРОВЫХ АКТИВОВ

(пункт 23 подпункт 8 Правил НБ № 45; пункты 28, 32)

21.1. Виды кошельков (пункт 28 Правил НБ № 45)

Оператор хранит необеспеченные цифровые активы (как собственные, так и активы клиентов) на холодных и горячих кошельках цифровых активов. Приведённая ниже трёхуровневая структура распределения активов (холодный / тёплый / горячий) является целевой и внедряется после получения лицензии и перехода на кастодиального провайдера — BitGo Trust Company (альтернативы: Fireblocks, Ledger Enterprise). По состоянию на дату подачи заявления Оператор хранит необеспеченные цифровые активы на горячих (операционных) кошельках согласно Реестру адресов кошельков (Приложение № 2), что соответствует пункту 28 Правил НБ № 45, допускающему хранение на холодных и (или) горячих кошельках:

Вид кошелька	Доля от объёма активов	Назначение	Технология
Холодный	Не менее 85 %	Долгосрочное хранение основной массы клиентских активов	Изолированные аппаратные кошельки (Ledger Vault / Trezor Safe); мультиподпись 3 из 5; ключи хранятся в физических сейфах в разных географических точках
Тёплый	5-10 %	Промежуточный буфер между холодным и горячим	мультиподпись 3 из 5; офлайн-подпись с подключением только для подписания
Горячий	Не более 15 %	Оперативное обслуживание операций клиентов	мультиподпись 2 из 3; авто-подпись с лимитом разовой операции; перемещение средств в тёплый/холодный уровень при превышении 15 % порога

21.2. Безопасность мнемонических фраз и приватных ключей (пункт 32 Правил НБ № 45)

В соответствии с пунктом 32 Правил НБ № 45 Оператор обеспечивает безопасность и надлежащее хранение мнемонических фраз и приватных ключей кошельков цифровых активов клиентов.

Конкретные меры:

- 1) Не раскрытие клиентам. Оператор не раскрывает клиентам мнемонические фразы и приватные ключи кошельков цифровых активов и несёт ответственность перед клиентами за их сохранность (абзац 2 пункта 32);
- 2) Защищённая среда. Мнемонические фразы, приватные ключи, пароли к личному кабинету и кошелькам цифровых активов клиентов хранятся Оператором в защищённой среде, исключающей несанкционированный доступ третьих лиц (абзац 3 пункта 32). На дату подачи заявления защищённая среда обеспечивается изолированным хранением мнемонических фраз на физических носителях в сейфе, шифрованием устройств и контролем доступа; по мере масштабирования и перехода на кастодиальную инфраструктуру — аппаратными модулями класса HSM (аппаратный модуль безопасности) и изолированными средами для холодных кошельков;
- 3) Криптографическая защита. Оператор внедряет комплекс организационно-технических мер защиты информации, включая применение средств криптографической защиты (абзац 4 пункта 32): AES-256-GCM шифрование баз данных, TLS 1.3 для каналов связи, мультиподпись 2 из 3 и 3 из 5 (после перехода на кастодиальную инфраструктуру);
- 4) Доступ работников. Доступ к указанным сведениям предоставляется уполномоченным работникам Оператора на основании трудового договора с работником, должностной инструкции работника и (или)

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

приказа руководителя Оператора на предоставление доступа работнику (абзац 5 пункта 32). Перечень работников с доступом утверждается приказом Директора и пересматривается ежеквартально;

5) Учёт действий. Оператор ведёт учёт всех действий, совершённых с указанными сведениями, включая их передачу, копирование и уничтожение (абзац 6 пункта 32). Журнал ведётся в SIEM-системе с фиксацией: дата и время, работник, действие, идентификатор кошелька (без раскрытия ключа);

6) Отзыв доступа. Доступ к сведениям подлежит немедленному ограничению или отзыву в случаях увольнения работника и (или) изменения должностных обязанностей (абзац 7 пункта 32). Процедура отзыва доступа выполняется в день уведомления HR-отдела о факте увольнения / изменения должности.

21.3. Личный кабинет клиента (пункт 32 абзац 8 Правил НБ № 45)

Доступ к личному кабинету клиента осуществляется с помощью логина и пароля, которые могут быть изменены либо восстановлены (при утере) в случае обращения клиента и после подтверждения его личности Оператором согласно пункту 30 Правил.

Процедура восстановления доступа:

- 1) клиент обращается через службу поддержки с заявлением о восстановлении доступа;
- 2) Оператор проводит идентификацию клиента через ЦОИД (для резидентов РК) либо через биометрическую верификацию по сторонним сервисам (для нерезидентов);
- 3) при успешной идентификации — клиент получает временный пароль по зарегистрированному e-mail / SMS;
- 4) при первом входе клиент обязан изменить временный пароль и активировать 2FA.

21.4. Открытие кошельков клиентов

Кошелёк цифровых активов клиента открывается автоматически при первой операции в соответствующем НЦА; на стороне Оператора — в HD-схеме (иерархический детерминированный кошелёк) с производным адресом от мастер-ключа Оператора, привязанным к идентификатору клиента (идентификатор клиента). Адреса генерируются индивидуально для каждого клиента в каждой сети блокчейн.

ГЛАВА 22. АДРЕСА КОШЕЛЬКОВ ЦИФРОВЫХ АКТИВОВ ОПЕРАТОРА

(пункт 23 подпункт 10 Правил НБ № 45)

22.1. Реестр адресов кошельков

Оператор ведёт Реестр адресов кошельков цифровых активов Оператора с указанием названия сети блокчейн, на которой открыты кошельки цифровых активов. Полный реестр приведён в Приложении № 2 к настоящим Правилам.

22.2. Состав реестра

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

По состоянию на дату подачи заявления Оператором открыты горячие (операционные) кошельки (собственное хранение) в 11 (одиннадцати) сетях блокчейн, обеспечивающие обслуживание 45 (сорока пяти) из 73 необеспеченных цифровых активов перечня (Приложение № 1); реестр ведётся в разрезе каждой пары «актив — сеть блокчейн» (49 записей). Полный реестр адресов с указанием названия сети блокчейн приведён в Приложении № 2. Кошельки в иных сетях блокчейн открываются по мере операционной готовности после получения лицензии с обновлением Реестра. Обслуживание операций с НЦА из перечня, для которых кошелёк цифровых активов не открыт, начинается с момента открытия соответствующего кошелька и обновления Реестра; до этого момента заявки по такому активу информационной системой Оператора не принимаются, о чём клиент информируется в интерфейсе платформы. Целевая трёхуровневая структура хранения (холодный / тёплый / горячий) внедряется после получения лицензии и перехода на кастодиального провайдера — BitGo Trust Company (альтернативы: Fireblocks, Ledger Enterprise). Реестр включает кошельки в следующих сетях:

№	Название сети блокчейн	Применимые НЦА (примеры)
1	Bitcoin	BTC
2	Ethereum (ERC-20)	ETH, USDT, USDC, DAI, LINK, SHIB, PEPE, UNI, AAVE, CRV, LDO, GRT, QNT, IMX, FET, NEXO, ONDO, USDE, SKY, WLD, LEO, BGB, OKB, KCS, GT, TUSD, PYUSD, RLUSD, EURC, CRO
3	BNB Chain (BEP-20)	BNB, CAKE, ASTER
4	Polygon	POL
5	Arbitrum One	ARB
6	Optimism	OP
7	Base	AERO
8	Avalanche C-Chain	AVAX
9	Mantle	MNT
10	Tron (TRC-20)	TRX, USDT (TRC-20)
11	Solana (SPL)	SOL, BONK, PUMP, RENDER, PYUSD (SPL), USDC (SPL), EURC (SPL)

22.3. Формат записи в реестре

Каждая запись в Реестре адресов кошельков содержит: НЦА (тикер); сеть блокчейн; категория (холодный / тёплый / горячий); адрес кошелька; дата открытия; тип ключа (одиночный / мультиподпись 2 из 3 / мультиподпись 3 из 5); владелец процесса; статус (активный / закрыт / в инкассации).

22.4. Порядок обновления реестра

Реестр обновляется не позднее 1 (одного) рабочего дня после открытия нового кошелька, закрытия существующего кошелька, изменения типа подписи. Утверждение изменений в реестре производится приказом Директора Оператора. Сводный реестр направляется в Национальный Банк РК по запросу в рамках надзорной деятельности.

ГЛАВА 23. ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

23.1. Срок хранения информации об инцидентах кибербезопасности (пункт 43 Правил НБ № 45)

Оператор хранит информацию об инцидентах кибербезопасности в полном объёме, а не только технические логи. К информации об инцидентах кибербезопасности относятся: записи Журнала учёта инцидентов кибербезопасности (глава 23.3); Карты инцидентов кибербезопасности по каждому инциденту (глава 23.4); материалы расследования инцидента (первопричина, хронология, затронутые активы); сведения о принятых неотложных и корректирующих мерах; отчёты по итогам инцидента (после инцидента разбор); уведомления, направленные в Национальный Банк Республики Казахстан (глава 23.6); а также технические логи и события кибербезопасности (глава 23.8). Срок хранения всей перечисленной информации об инцидентах кибербезопасности составляет не менее 5 (пяти) лет с момента регистрации инцидента в Журнале учёта. Хранение осуществляется в защищённом архиве с шифрованием AES-256-GCM, контролем доступа и защитой от модификации (WORM-хранилище).

23.2. Порядок принятия неотложных мер по устранению инцидента (пункт 44 Правил НБ № 45)

Оператором определяется следующий порядок принятия неотложных мер к устранению инцидента кибербезопасности, его причин и последствий:

Шаг 1. Обнаружение и регистрация (T0 — момент обнаружения). Инцидент обнаруживается автоматически SIEM-системой либо вручную работником. В течение 15 минут — регистрация в Журнале инцидентов с присвоением уровня (низкий / средний / высокий / критический).

Шаг 2. Изоляция (T0 + 30 минут). Ответственный работник по ИТ-инфраструктуре изолирует затронутые сегменты сети, отключает скомпрометированные учётные записи, прекращает скомпрометированные процессы.

Шаг 3. Анализ и устранение причин (T0 + 2 часа). Формируется группа реагирования с участием Ответственного работника по ИТ-инфраструктуре, Ответственного работника по ПОД/ФТ и, при необходимости, внешнего подрядчика по кибербезопасности. Анализируется первопричина.

Шаг 4. Восстановление сервисов (T0 + 4-12 часов). Восстановление затронутых сервисов из резервных копий, патч уязвимости, замена скомпрометированных учётных данных / ключей.

Шаг 5. Уведомление Национального Банка РК (T0 + до 24 часов). См. главу 23.6 настоящих Правил.

Шаг 6. Уведомление клиентов (при необходимости). Если инцидент затронул данные или активы клиентов — уведомление в личном кабинете, e-mail, на сайте.

Шаг 7. Разбор после инцидента (T0 + 5 рабочих дней). Полный отчёт об инциденте; план корректирующих мер; обновление документации и регламентов.

23.3. Журнал учёта инцидентов кибербезопасности (пункт 45 Правил НБ № 45)

Оператор ведёт Журнал учёта инцидентов кибербезопасности с отражением всей информации об инциденте кибербезопасности, принятых мерах и предлагаемых корректирующих мерах. Журнал ведётся в электронной форме с поддержкой целостности (хеш-цепочка) и непрерывного аудит-трейла.

Состав записи в Журнале:

- уникальный идентификатор инцидента;
- дата и время регистрации, обнаружения, устранения;
- уровень критичности;
- описание инцидента;
- затронутые активы и сервисы;
- принятые неотложные меры;
- первопричина;
- корректирующие меры (план + ответственный + срок);
- ссылка на Карту инцидента (см. п. 23.4).

23.4. Карта инцидента кибербезопасности (пункт 46 Правил НБ № 45)

На каждый инцидент кибербезопасности заполняется отдельная Карта инцидента кибербезопасности, которая включает сведения по:

- 1) описание инцидента (характер, способ обнаружения, затронутые системы);
- 2) дата и время возникновения, обнаружения и устранения инцидента;
- 3) возникшие последствия (нарушение конфиденциальности / целостности / доступности; финансовый ущерб; ущерб клиентам; ущерб репутации);
- 4) ущерб (количественная оценка в денежном выражении при возможности);
- 5) принятые меры (с указанием ответственных лиц и сроков).

Шаблон Карты инцидента утверждён внутренним регламентом Оператора и прилагается к Журналу учёта инцидентов.

23.5. Управление рисками кибербезопасности (пункт 47 Правил НБ № 45)

Оператор управляет рисками кибербезопасности с указанием:

- наименования риска;
- описания риска;
- причины возникновения;
- приемлемого уровня риска;
- плана мероприятий по его минимизации;

по отношению к цифровым объектам Оператора (веб-сайт ausu.kz, мобильное приложение, базы данных, кошельки цифровых активов, инфраструктура размещения).

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

Реестр рисков кибербезопасности ведётся в составе общего Реестра рисков Оператора и пересматривается ежеквартально.

23.6. Уведомление НБ РК об инцидентах (пункт 49 Правил НБ № 45)

Оператор направляет в Национальный Банк Республики Казахстан в произвольной форме уведомление о произошедших инцидентах кибербезопасности в течение 24 (двадцати четырёх) часов с момента их обнаружения с приложением Карты инцидента кибербезопасности.

Состав уведомления:

- наименование Оператора, БИН, номер лицензии;
- описание инцидента;
- дата и время обнаружения;
- затронутые системы и сервисы;
- предварительная оценка ущерба и количество затронутых клиентов;
- принятые меры;
- контактное лицо для дополнительной информации;
- Карта инцидента кибербезопасности (прилагается к уведомлению).

Направление уведомления осуществляется через защищённый канал связи с НБ РК (e-mail с ЭЦП либо иной согласованный канал).

23.7. Консолидация информации (пункт 48 Правил НБ № 45)

Информация об инцидентах кибербезопасности, полученная в ходе мониторинга деятельности по обеспечению кибербезопасности, подлежит консолидации, систематизации и хранению. Консолидация осуществляется в SIEM-системе с автоматической агрегацией по типу инцидента, источнику, уровню критичности.

23.8. Меры обеспечения кибербезопасности (пункт 50 Правил НБ № 45)

Оператор обеспечивает следующие меры (по подпунктам пункта 50):

1) Идентификация, аутентификация и авторизация пользователей (подпункт 1 пункта 50).

- клиенты: ЦОИД-биометрия (резиденты РК) или Sumsb (нерезиденты) + двухфакторная аутентификация (2FA) — TOTP/SMS;
- работники: централизованная служба каталогов с MFA; ролевая модель доступа (RBAC); привилегированный доступ через бастион-узел с журналированием.

2) Регистрация и хранение событий кибербезопасности (подпункт 2 пункта 50).

- SIEM-система с агрегацией событий из всех источников (приложение, БД, сетевое оборудование, OS-логи, кошельки);

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

— срок хранения логов кибербезопасности — не менее 5 лет;

— защита логов от модификации (WORM-хранилище).

3) Защита информации от несанкционированного доступа, утечки, модификации, уничтожения и блокирования (подпункт 3 пункта 50).

— TLS 1.3 для всех сетевых каналов;

— AES-256-GCM шифрование баз данных и архивов в покое;

— межсетевой экран, WAF и DDoS-защита на инфраструктуре PS Cloud Services (резидент Республики Казахстан);

— EDR на всех конечных устройствах работников;

— DLP-системы для предотвращения утечек.

4) Резервное копирование и восстановление информации (подпункт 4 пункта 50).

— ежедневное инкрементальное резервное копирование баз данных; еженедельное полное;

— хранение резервных копий в географически удалённом ЦОД (основной — г. Алматы, резервный — г. Астана);

— еженедельное тестирование восстановления;

— RPO (целевая точка восстановления) — 15 минут для критических данных; RTO (целевое время восстановления) — 2 часа для критических процессов.

5) Соблюдение требований законодательства Республики Казахстан «О персональных данных и их защите» при обработке персональных данных на платформе (подпункт 5 пункта 50).

— все персональные данные обрабатываются на территории Республики Казахстан (Закон РК «О персональных данных и их защите»);

— получение явного согласия субъекта ПД на обработку;

— обеспечение прав субъекта ПД (доступ, исправление, удаление, переносимость);

— назначение Ответственного работника по защите ПД;

— ведение Реестра обработки ПД;

— уведомление субъектов ПД и Уполномоченного органа о фактах нарушения (утечка данных) в течение 24 часов.

6) Безопасное совершение сделок (подпункт 6 пункта 50).

— все сделки совершаются с MFA-подтверждением клиента;

— подпись блокчейн-транзакций — в защищённой среде (после перехода на кастодиальную инфраструктуру — мультиподпись 2 из 3 для горячих, 3 из 5 для тёплых и холодных);

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

— проверка и скоринг уровня риска адреса получателя через сервис анализа транзакций (TRM Labs / Chainalysis; до подключения — по официальным открытым источникам) до подписания транзакции — в порядке главы 24 настоящих Правил;

— период удержания 24 часа для впервые используемых внешних адресов с суммой > 5 000 000 тенге;

— правило передачи данных об отправителе и получателе перевода для операций > 500 000 тенге.

23.9. Внешний подрядчик по кибербезопасности

Ответственным за информационную безопасность Оператора является ответственный работник по информационной безопасности: политика ИБ, контроль внедрения мер защиты, координация реагирования на критические инциденты, взаимодействие с Национальным Банком по инцидентам кибербезопасности. Независимый аудит информационной безопасности (включая тестирование на проникновение) проводится внешним специализированным подрядчиком в сфере информационной безопасности, привлекаемым на договорной основе после получения лицензии по результатам отбора и комплексной проверки. Оперативные функции ИТ-инфраструктуры выполняет штатный работник Оператора — ИТ-администратор.

ГЛАВА 24. ОПИСАНИЕ ПОРЯДКА И МЕХАНИЗМОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ АНАЛИЗА И КОНТРОЛЯ ОПЕРАЦИЙ

(пункт 23 подпункт 7 Правил НБ № 45; пункт 51)

24.1. Состав системы анализа и контроля операций (пункт 51 Правил НБ № 45)

Система анализа и контроля операций Оператора включает следующие компоненты, установленные пунктом 51 Правил НБ № 45:

24.2. Мониторинг и отслеживание операций с цифровыми активами, включая выявление подозрительных действий клиентов (подпункт 1 пункта 51).

Реализация:

— автоматический мониторинг всех операций в системе мониторинга транзакций с применением 18 правил выявления подозрительных операций (см. Правила внутреннего контроля по ПОД/ФТ);

— ведение единого Журнала операций клиентов с фиксацией даты, времени, клиента, типа операции, объёма, направления, риск-балла, статуса;

— ежедневный отчёт Ответственного работника по ПОД/ФТ о выявленных подозрительных операциях.

24.3. Мониторинг транзакций в реальном времени и уведомление ответственного лица за соблюдение Закона о ПОД/ФТ/ФРОМУ (подпункт 2 пункта 51).

Реализация:

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

— все транзакции пропускаются через модуль мониторинга транзакций до их исполнения; при срабатывании правила приоритет=высокий операция приостанавливается до решения Ответственного работника по ПОД/ФТ;

— уведомления Ответственному работнику по ПОД/ФТ направляются через внутреннюю систему уведомлений информационной платформы Оператора и корпоративную электронную почту в течение 60 секунд с момента срабатывания правила; использование внешних мессенджеров для передачи сведений, связанных с ПОД/ФТ/ФРОМУ, не допускается;

— решение по приостановленной операции принимается в течение 24 часов; при невозможности — операция возвращается с восстановлением исходного актива.

24.4. Проведение оценки кошелька цифрового актива клиента и присвоения уровня риска кошельку цифровых активов клиента (подпункт 3 пункта 51).

Реализация:

— каждый внешний адрес кошелька, с которого/на который проводится операция, проверяется через сервис скоринга цифровых активов TRM Labs (либо Chainalysis) с присвоением уровня риска: низкий / средний / высокий / критический;

— уровень риска кошелька клиента отображается в карточке клиента и влияет на разрешение операции:

- низкий — операция разрешается;
- средний — дополнительная проверка Ответственным работником по ПОД/ФТ;
- высокий — приостановление операции, углублённая проверка клиента;
- критический — отказ в операции, формирование сообщения о подозрительной операции в АФМ РК.

24.5. Проведение анализа кошелька цифрового актива клиента на предмет использования сервисов, повышающих анонимность операции и усложняющих определение цепочки держателей цифрового актива (подпункт 4 пункта 51).

Реализация:

— автоматическая проверка адресов на признаки использования миксеров (Tornado Cash, Wasabi, Samourai), коин-джоинов, обменных сервисов без идентификации клиента, внебиржевых площадок повышенного риска через TRM Labs;

— проверка транзакций анонимных монет (Monero, Zcash — экранированные) — автоматический отказ в операции;

— проверка цепочки на глубину до 5 переходов; при обнаружении источника, связанного с миксером, санкционным адресом или инцидентом взлома — операция блокируется.

24.6. Технические компоненты

Компонент	Назначение	Поставщик / Технология
модуль мониторинга транзакций	Применение 18 ПОД/ФТ-правил	Собственная разработка на

	в реальном времени	платформе PostgreSQL + Python; интеграция с TRM Labs
скоринг риска кошельков	Скоринг адресов кошельков	TRM Labs программный интерфейс (API) (резервно — Chainalysis)
санкционный скрининг	Проверка по 7 санкционным спискам	Sumsb + WorldCheck
проверка ПДЛ	Проверка публичных должностных лиц (ПДЛ) и связанных с ними лиц	WorldCheck / Dow Jones
правило передачи данных об отправителе и получателе перевода	Обмен данными отправителя/получателя при операциях > 500 000 тенге	Notabene (планируется к подключению после лицензии)
SIEM	Сбор и анализ событий безопасности	Wazuh / Elastic Security
Интеграция с Антифрод-центром	Передача данных в Антифрод-центр НБ	программный интерфейс (API)-подключение в течение 30 дней после лицензии

24.7. Пороговые значения автоматического контроля

Триггер	Порог	Действие системы
Совокупная сумма операций за 30 дней	эквивалент 25 000 000 тенге (НКИ) / 125 000 000 тенге (КИ)	Запрос актуального источника средств (источник происхождения средств)
Разовая операция	эквивалент 7 500 000 тенге (НКИ) / 50 000 000 тенге (КИ)	Повторный санкционный скрининг и проверка лимитов
Серия операций с признаками дробления (дробление операций)	более 3 операций на суммы 4 000 000–7 499 999 тенге за 72 часа	Автоматическое формирование сигнала для ответственного работника по ПОД/ФТ
Перевод на внешний (некастодиальный) кошелёк	свыше эквивалента 500 000 тенге (Рекомендация ФАТФ 16)	Запрос подтверждения владения кошельком
Операция с высокорисковой юрисдикцией	любая сумма	Обязательная углублённая проверка клиента; юрисдикции из чёрного списка ФАТФ — отказ

ГЛАВА 25. ИНФОРМАЦИЯ О РИСКАХ НА ИНТЕРНЕТ-РЕСУРСЕ

(пункт 29 Правил НБ № 45)

25.1. До совершения клиентом операции Оператор доводит до его сведения информацию о рисках, связанных с покупкой, продажей, и владением необеспеченными цифровыми активами, которая содержит, но не ограничивается:

1) указание на то, что необеспеченные цифровые активы не являются средством платежа (подпункт 1 пункта 29);

2) указание на то, что необеспеченные цифровые активы не обеспечиваются государством и приобретение необеспеченных цифровых активов может привести к полной потере денег и иных

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов · стр. 52 из 67

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

объектов гражданских прав (в том числе в результате волатильности стоимости необеспеченных цифровых активов, технических сбоев (ошибок), совершения противоправных действий, включая хищение) (подпункт 2 пункта 29);

3) указание на то, что лица, осуществляющие операции с необеспеченными цифровыми активами через операторов обмена необеспеченных цифровых активов, самостоятельно несут ответственность за изменение стоимости необеспеченного цифрового актива (подпункт 3 пункта 29).

25.2. Информация о рисках размещается на главной странице интернет-ресурса Оператора (ausu.kz) или на отдельной странице этого интернет-ресурса с принятием мер по привлечению к ней внимания его посетителей (контрастные баннеры, всплывающее окно при первом посещении, обязательный чекбокс ознакомления при регистрации).

ГЛАВА 26. ЗАПРЕТ НА УСТАНОВЛЕНИЕ ДЕЛОВЫХ ОТНОШЕНИЙ

(пункты 20, 52 Правил НБ № 45)

26.1. Не допускается установление деловых отношений Оператором с (пункт 52 Правил НБ № 45):

1) физическими лицами, не достигшими 18 (восемнадцати) лет (подпункт 1 пункта 52). Контроль — обязательное предоставление УДО при регистрации, проверка даты рождения через ЦОИД;

2) иными лицами, включёнными в перечень организаций и лиц, связанных с финансированием терроризма и экстремизма, а также в перечень организаций и лиц, связанных с финансированием распространения оружия массового уничтожения в соответствии с Законом о ПОД/ФТ/ФРОМУ (подпункт 2 пункта 52). Контроль — ежедневная сверка с перечнем КФМ РК через WorldCheck / Sumsb.

26.2. Дополнительные ограничения (пункт 20 Правил НБ № 45 — применимо к учредителю; аналогично применяется Оператором к клиентам):

— лицам, не имеющим безупречной деловой репутации;

— лицам, зарегистрированным (проживающим) в государстве (на территории), которое не выполняет либо недостаточно выполняет рекомендации ФАТФ (чёрный список ФАТФ).

ГЛАВА 27. РАЗДЕЛЬНЫЕ БАНКОВСКИЕ СЧЕТА

(пункт 42 Правил НБ № 45)

27.1. Оператор использует разные банковские счета для хозяйственной деятельности компании и для осуществления операций, предусмотренной лицензией:

1) Хозяйственный банковский счёт № KZ598853010011580000 в АО «ДБ «Казахстан-Зираат Интернешнл Банк» (КЗИ Банк) — для зарплаты, налогов, аренды, ИТ-расходов, профессиональных услуг, выплат акционерам и иной хозяйственной деятельности;

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

2) Операционный банковский счёт для расчётов с клиентами — открывается отдельно после получения лицензии в КЗИ Банке либо ином банке второго уровня РК; используется исключительно для зачисления / списания денежных средств в рамках лицензированной деятельности;

3) Сводный реестр банковских счетов Оператора ведётся в Документе о порядке взаимодействия с банком второго уровня и обновляется в течение 3 рабочих дней после открытия / изменения / закрытия счёта.

27.2. Денежные средства, поступившие от клиентов в рамках расчётов по лицензированной деятельности, не используются для финансирования операционных расходов Оператора, выплат участникам, кредитования аффилированных лиц или иных целей, не связанных с исполнением обязательств перед клиентами.

ГЛАВА 28. УТВЕРЖДЕНИЕ И ПЕРЕСМОТР ПРАВИЛ

(пункт 23 подпункт 13 Правил НБ № 45)

28.1. Настоящие Правила утверждены Решением Единственного участника ТОО «Ausu» № 2 от «2» июля 2026 года и введены в действие со 2 июля 2026 года (Приказ № 2 от 2 июля 2026 года). Услуги, для оказания которых требуется лицензия, предоставляются клиентам исключительно после получения лицензии Национального Банка Республики Казахстан.

28.2. Изменения и дополнения в настоящие Правила вносятся Решением Единственного участника по предложению Директора Оператора либо Ответственного работника по управлению рисками.

28.3. Плановый пересмотр Правил осуществляется не реже 1 (одного) раза в год; внеплановый — при изменении применимого законодательства Республики Казахстан, изменении бизнес-модели Оператора, по требованию НБ РК.

28.4. Об изменениях в настоящие Правила, затрагивающих интересы клиентов, Оператор уведомляет клиентов не позднее чем за 14 (четырнадцать) календарных дней до вступления изменений в силу — путём публикации в личном кабинете, на сайте, по e-mail.

ПОДПИСИ И УТВЕРЖДЕНИЕ

Настоящие Правила утверждены Решением Единственного участника ТОО «Ausu»:

Дата утверждения: «2» июля 2026 года

Номер Решения: № 2

Единственный участник ТОО «Ausu»

М.П.

ПРИЛОЖЕНИЕ № 1. ПЕРЕЧЕНЬ РАЗРЕШЁННЫХ НЕОБЕСПЕЧЕННЫХ ЦИФРОВЫХ АКТИВОВ

(пункт 57 Правил НБ № 45)

В соответствии с пунктом 57 Правил НБ № 45 Оператор обслуживает операции по покупке и (или) продаже следующих видов необеспеченных цифровых активов (73 актива). Перечень утверждён Решением Единственного участника № 2 от 2 июля 2026 года и приведён ниже:

№	Тикер	Полное наименование	Основная сеть	Консенсус / тип	Уровень	Категория
1	BTC	Bitcoin	Bitcoin	PoW	Уровень 1	Крупная сеть
2	ETH	Ethereum	Ethereum	PoS	Уровень 1	Крупная сеть
3	USDT	Tether USD	Несколько сетей (ERC-20, TRC-20)	Стейблкоин	Уровень 1	Стейблкоин
4	XRP	XRP	XRP Ledger	RPCA	Уровень 1	Крупная сеть
5	BNB	BNB	BNB Chain	PoSA	Уровень 1	Крупная сеть
6	SOL	Solana	Solana	PoH+PoS	Уровень 1	Крупная сеть
7	USDC	USD Coin	Несколько сетей (ERC-20, SPL)	Стейблкоин	Уровень 1	Стейблкоин
8	TRX	TRON	Tron	DPoS	Уровень 1	Крупная сеть
9	DOGE	Dogecoin	Dogecoin	PoW (AuxPoW)	Уровень 1	Крупная сеть
10	ADA	Cardano	Cardano	Ouroboros PoS	Уровень 1	Крупная сеть
11	BCH	Bitcoin Cash	Bitcoin Cash	PoW	Уровень 1	Крупная сеть
12	LINK	Chainlink	Ethereum	Oracle	Уровень 1	Децентрализованные финансы
13	LEO	UNUS SED LEO	Ethereum	Биржевой токен	Уровень 1	Биржевой токен
14	XLM	Stellar Lumens	Stellar	SCP	Уровень 1	Платежи
15	SUI	Sui	Sui	Narwhal/	Уровень 1	Крупная

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

				Bullshark		сеть
16	LTC	Litecoin	Litecoin	PoW (Scrypt)	Уровень 2	Крупная сеть
17	AVAX	Avalanche	Avalanche C-Chain	Avalanche Consensus	Уровень 2	Крупная сеть
18	DAI	Dai	Ethereum	Стейблкоин (CDP)	Уровень 2	Стейблкоин
19	HBAR	Hedera	Hedera	Hashgraph	Уровень 2	Крупная сеть
20	SHIB	Shiba Inu	Ethereum	Токен	Уровень 2	Мем-токен
21	TON	Toncoin	TON	PoS	Уровень 2	Крупная сеть
22	CRO	Cronos	Cronos / Ethereum	PoSA	Уровень 2	Биржевой токен
23	DOT	Polkadot	Polkadot	NPoS	Уровень 2	Крупная сеть
24	UNI	Uniswap	Ethereum	Управление	Уровень 2	Децентрализованные финансы
25	MNT	Mantle	Mantle	L2 Optimistic	Уровень 2	Сеть 2-го уровня
26	TAO	Bittensor	Bittensor	Yuma Consensus	Уровень 2	ИИ и данные
27	PEPE	Pepe	Ethereum	Токен	Уровень 2	Мем-токен
28	AAVE	Aave	Ethereum	Кредитование	Уровень 2	Децентрализованные финансы
29	BGB	Bitget Token	Ethereum	Биржевой токен	Уровень 2	Биржевой токен
30	OKB	OKB	Ethereum / X Layer	Биржевой токен	Уровень 2	Биржевой токен
31	NEAR	NEAR Protocol	NEAR	PoS (Nightshade)	Уровень 2	Крупная сеть
32	ETC	Ethereum Classic	Ethereum Classic	PoW	Уровень 2	Крупная сеть
33	USDE	Ethena USDe	Ethereum	Синтетический стейблкоин	Уровень 2	Стейблкоин
34	ASTER	Aster	BNB Chain	Токен DEX	Уровень 2	Децентрализованные финансы
35	ICP	Internet Computer	ICP	Chain Key	Уровень 2	Вычисления
36	WLD	Worldcoin	World Chain / Optimism	Токен	Уровень 2	Идентификация
37	KCS	KuCoin Token	Ethereum	Биржевой токен	Уровень 2	Биржевой токен
38	SKY	Sky	Ethereum	Управление	Уровень 2	Децентрализованные финансы

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

39	POL	Polygon Ecosystem Token	Polygon	PoS	Уровень 2	Сеть 2-го уровня
40	APT	Aptos	Aptos	PoS (BFT)	Уровень 2	Крупная сеть
41	ONDO	Ondo	Ethereum	RWA	Уровень 3	Реальные активы (RWA)
42	KAS	Kaspa	Kaspa	PoW (GHOSTDA G)	Уровень 3	Сеть 1-го уровня
43	RLUSD	Ripple USD	Ethereum / XRP Ledger	Стейблкоин	Уровень 3	Стейблкоин
44	PYUSD	PayPal USD	Ethereum / Solana	Стейблкоин	Уровень 3	Стейблкоин
45	ATOM	Cosmos	Cosmos Hub	Tendermint BFT	Уровень 3	Крупная сеть
46	ARB	Arbitrum	Arbitrum One	L2 Optimistic	Уровень 3	Сеть 2-го уровня
47	ALGO	Algorand	Algorand	PPoS	Уровень 3	Крупная сеть
48	RENDER	Render	Solana	Сеть GPU	Уровень 3	ИИ и данные
49	FIL	Filecoin	Filecoin	PoS	Уровень 3	Хранение
50	VET	VeChain	VeChain	PoA 2.0	Уровень 3	Цепочки поставок
51	FLR	Flare	Flare	FBA	Уровень 3	Сеть 1-го уровня
52	BONK	Bonk	Solana	Токен	Уровень 3	Мем-токен
53	XDC	XDC Network	XDC Network	XDPOS	Уровень 3	Корпоративный
54	QNT	Quant	Ethereum	Интероперабельность	Уровень 3	Инфраструктура
55	PUMP	Pump.fun	Solana	Платформенный токен	Уровень 3	Платформа
56	GT	GateToken	Ethereum	Биржевой токен	Уровень 3	Биржевой токен
57	SEI	Sei	Sei	Twin-Turbo BFT	Уровень 3	Сеть 1-го уровня
58	STX	Stacks	Bitcoin L2	PoX	Уровень 3	Сеть 2-го уровня
59	CAKE	PancakeSwap	BNB Chain	DEX	Уровень 3	Децентрализованные финансы
60	FET	Fetch.ai (ASI)	Ethereum / Cosmos	ИИ	Уровень 3	ИИ и данные
61	NEXO	Nexo	Ethereum	Токен ЦеФи	Уровень 3	Централизованные финансы
62	OP	Optimism	Optimism	L2 Optimistic	Уровень 3	Сеть 2-го уровня

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

63	XTZ	Tezos	Tezos	LPoS	Уровень 3	Крупная сеть
64	CRV	Curve DAO Token	Ethereum	Управление	Уровень 3	Децентрализованные финансы
65	CHZ	Chiliz	Chiliz Chain	PoSA	Уровень 3	Спорт
66	IMX	Immutable	Ethereum	ZK-Rollup	Уровень 3	Сеть 2-го уровня
67	LDO	Lido DAO	Ethereum	Ликвидный стейкинг	Уровень 3	Децентрализованные финансы
68	AERO	Aerodrome Finance	Base	DEX	Уровень 3	Децентрализованные финансы
69	INJ	Injective	Injective	Tendermint	Уровень 3	Децентрализованные финансы
70	TUSD	TrueUSD	Ethereum / Tron	Стейблкоин	Уровень 3	Стейблкоин
71	GRT	The Graph	Ethereum	Индексация	Уровень 3	Децентрализованные финансы
72	TIA	Celestia	Celestia	PoS (DA)	Уровень 3	Инфраструктура
73	EURC	Euro Coin	Ethereum / Solana	Стейблкоин	Уровень 3	Стейблкоин

Всего в перечне: 73 необеспеченных цифровых актива.

Перечень соответствует пункту 57 Правил НБ № 45 и изменяется исключительно вслед за изменением указанного пункта; актуализация перечня оформляется решением единственного участника ТОО «Ausu». При исключении НЦА из перечня клиенты уведомляются не менее чем за 30 (тридцать) календарных дней; в течение указанного срока клиенту обеспечивается возможность вывода НЦА на внешний адрес. Операции с необеспеченными цифровыми активами, не предусмотренными перечнем, не осуществляются — клиенту предоставляется отказ (пункт 58 Правил НБ № 45). Обслуживание активов перечня, по которым кошелек ещё не открыт, начинается с момента открытия кошелька и обновления Реестра (Приложение № 2). Значения граф «Уровень» и «Категория» носят справочно-операционный характер (управление ликвидностью и операционная готовность) и не являются критериями допуска активов к обмену.

ПРИЛОЖЕНИЕ № 2. РЕЕСТР АДРЕСОВ КОШЕЛЬКОВ ЦИФРОВЫХ АКТИВОВ ОПЕРАТОРА

(пункт 23 подпункт 10 Правил НБ № 45)

Адреса кошельков цифровых активов Оператора с указанием названия сети блокчейн, на которой открыты кошельки цифровых активов (по состоянию на дату подачи заявления):

№	Актив (тикер)	Сеть блокчейн	Адрес кошелька Оператора	Тип / модель
1	BTC	Bitcoin	bc1q5xpp54c0wajx4c33xsm7hsgyne8p4t2hw2usy8	Горячий (операционный); некастодиальное хранение
2	ETH	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
3	USDT	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
4	USDC	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
5	DAI	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
6	LINK	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
7	SHIB	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
8	PEPE	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
9	UNI	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
10	AAVE	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
11	CRV	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
12	LDO	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbe84A	Горячий (операционный); некастодиальное хранение
13	GRT	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a33	Горячий (операционный);

			6Ad704bbE84A	некастодиальное хранение
14	QNT	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
15	IMX	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
16	FET	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
17	NEXO	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
18	ONDO	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
19	USDE	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
20	SKY	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
21	WLD	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
22	LEO	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
23	BGB	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
24	OKB	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
25	KCS	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
26	GT	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a33	Горячий (операционный);

			6Ad704bbE84A	некастодиальное хранение
27	TUSD	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
28	PYUSD	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
29	RLUSD	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
30	EURC	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
31	CRO	Ethereum (ERC-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
32	BNB	BNB Chain (BEP-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
33	CAKE	BNB Chain (BEP-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
34	ASTER	BNB Chain (BEP-20)	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
35	POL	Polygon	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
36	ARB	Arbitrum One	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
37	OP	Optimism	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
38	AERO	Base	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
39	AVAX	Avalanche C-Chain	0x306B46EFdb934017d0dD22192a33	Горячий (операционный);

			6Ad704bbE84A	некастодиальное хранение
40	MNT	Mantle	0x306B46EFdb934017d0dD22192a336Ad704bbE84A	Горячий (операционный); некастодиальное хранение
41	TRX	Tron (TRC-20)	TEzPXsRP4Kaid1JDWyJo9zJzJgHhTcaKzA	Горячий (операционный); некастодиальное хранение
42	USDT	Tron (TRC-20)	TEzPXsRP4Kaid1JDWyJo9zJzJgHhTcaKzA	Горячий (операционный); некастодиальное хранение
43	SOL	Solana (SPL)	Ek24YdsPSxu3iBobk51Qk2mFnTZgd fYFfscTTBXMWgvs	Горячий (операционный); некастодиальное хранение
44	BONK	Solana (SPL)	Ek24YdsPSxu3iBobk51Qk2mFnTZgd fYFfscTTBXMWgvs	Горячий (операционный); некастодиальное хранение
45	PUMP	Solana (SPL)	Ek24YdsPSxu3iBobk51Qk2mFnTZgd fYFfscTTBXMWgvs	Горячий (операционный); некастодиальное хранение
46	RENDER	Solana (SPL)	Ek24YdsPSxu3iBobk51Qk2mFnTZgd fYFfscTTBXMWgvs	Горячий (операционный); некастодиальное хранение
47	PYUSD	Solana (SPL)	Ek24YdsPSxu3iBobk51Qk2mFnTZgd fYFfscTTBXMWgvs	Горячий (операционный); некастодиальное хранение
48	USDC	Solana (SPL)	Ek24YdsPSxu3iBobk51Qk2mFnTZgd fYFfscTTBXMWgvs	Горячий (операционный); некастодиальное хранение
49	EURC	Solana (SPL)	Ek24YdsPSxu3iBobk51Qk2mFnTZgd fYFfscTTBXMWgvs	Горячий (операционный); некастодиальное хранение

Примечания к Реестру:

1. Сети Ethereum, BNB Chain, Polygon, Arbitrum One, Optimism, Base, Avalanche C-Chain, Mantle используют единый EVM-адрес (BIP-44, тип монеты 60), производный от одного ключа.
2. Мнемонические фразы и приватные ключи кошельков хранятся в защищённой среде согласно пункту 32 Правил НБ № 45 и Главе 21 настоящих Правил.
3. Кошельки в иных сетях блокчейн открываются после получения лицензии по мере операционной готовности; Реестр обновляется в порядке пункта 22.4 Правил.

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

4. Холодные кошельки и кастодиальный провайдер (BitGo Trust Company; альтернативы — Fireblocks, Ledger Enterprise) — после получения лицензии; Реестр дополняется соответствующими адресами.

5. Для UTXO-сетей (Bitcoin) допускается ротация приёмных адресов; в Реестре указан основной приёмный адрес.

ПРИЛОЖЕНИЕ № 3. ТЕСТ КВАЛИФИКАЦИИ КЛИЕНТА (12 ВОПРОСОВ)

(в соответствии с пунктом 54 Правил НБ № 45)

Минимальный проходной балл — 80 (восемьдесят) процентов.

Отметки о принятии рисков (вопросы 4-9) и об ознакомлении (вопрос 10) являются обязательными — отсутствие любой отметки означает непрохождение теста.

Тест квалификации состоит из 12 (двенадцати) вопросов и охватывает все подпункты 1)–10) пункта 54 Правил НБ № 45 (требование о включении не менее 10 (десяти) вопросов соблюдено); минимальный проходной балл — 80 (восемьдесят) процентов. Повторное проведение оценки знаний доступно клиенту через 30 (тридцать) календарных дней после последнего прохождения (пункт 55 Правил НБ № 45); информационная система блокирует досрочную пересдачу.

Зачёт ответов по вопросам 1–3 (оценка опыта): по каждому из вопросов 1–3 засчитывается любой непустой ответ, отражающий фактический опыт клиента; «правильным (зачётным)» признаётся ответ, подтверждающий наличие практического опыта по соответствующему подпункту пункта 54. Выбор любого из перечисленных инструментов в вопросе 3 (в том числе NFT) засчитывается как зачётный ответ. Вопросы 1–3 в совокупности дают 3 балла, вопросы 4–10 — 7 баллов, вопросы 11–12 (вопросы на знание с одним правильным ответом, правильные ответы отмечены) — 2 балла; итого 12 баллов. Обязательным условием прохождения теста является проставление всех отметок о принятии рисков (вопросы 4–9) и об ознакомлении (вопрос 10).

Вопрос 1. Опыт и стаж работы с цифровыми активами (подпункт 1 пункта 54).

Укажите ваш опыт работы с цифровыми активами:

- А. Менее 1 года
- Б. От 1 до 3 лет
- В. От 3 до 5 лет
- Г. Более 5 лет

Вопрос 2. Опыт использования кошельков цифровых активов (подпункт 2 пункта 54).

Какими кошельками цифровых активов вы пользовались (можно выбрать несколько):

А. Биржевой (Binance, Bybit, OKX)

Б. Программный некастодиальный (MetaMask, Trust Wallet, Phantom)

В. Аппаратный (Ledger, Trezor, SafePal)

Г. Не имею опыта

Вопрос 3. Виды инструментов на базе цифровых активов (подпункт 3 пункта 54).

С какими инструментами на базе цифровых активов у вас есть практический опыт операций (можно выбрать несколько):

А. Спот-обмен (купля-продажа за фиат и крипто)

Б. Стейкинг и фарминг

В. ДеФи-протоколы (кредитование, DEX)

Г. Производные инструменты (фьючерсы, опционы, перпы)

Д. NFT

Е. Не имею опыта

Вопрос 4. Принятие риска необратимости операции (подпункт 4 пункта 54).

Я понимаю и принимаю риск, что операции с цифровыми активами необратимы: после подтверждения транзакции в блокчейне отменить или отозвать её невозможно.

☐ Принимаю

Вопрос 5. Принятие риска утраты доступа (подпункт 5 пункта 54).

Я понимаю и принимаю риск, что утрата доступа к кошельку цифровых активов (потеря пароля, приватного ключа, мнемонической фразы) может привести к безвозвратной потере цифровых активов.

☐ Принимаю

Вопрос 6. Принятие риска высокой волатильности (подпункт 6 пункта 54).

Я понимаю и принимаю риск, что цифровые активы характеризуются высокой волатильностью — их стоимость может меняться в десятки и сотни процентов в течение коротких промежутков времени, что может привести к существенным финансовым потерям.

☐ Принимаю

Вопрос 7. Принятие риска отсутствия государственных гарантий (подпункт 7 пункта 54).

Я понимаю и принимаю риск, что необеспеченные цифровые активы не обеспечиваются государством и не являются законным средством платежа. Государство не гарантирует возмещение убытков от операций с цифровыми активами.

☐ Принимаю

Вопрос 8. Принятие риска приостановления операций по ПОД/ФТ (подпункт 8 пункта 54).

Я понимаю и принимаю риск, что Оператор обмена необеспеченных цифровых активов обязан приостановить операции при признании их подозрительными в соответствии с Законом Республики Казахстан о ПОД/ФТ/ФРОМУ; в этом случае мои активы могут быть временно заблокированы до завершения расследования.

☐ Принимаю

Вопрос 9. Принятие риска исключения НЦА из перечня (подпункт 9 пункта 54).

Я понимаю и принимаю риск, что конкретный необеспеченный цифровой актив может быть исключён Оператором из списка обслуживаемых активов, с уведомлением не менее чем за 30 календарных дней; при этом я должен своевременно вывести соответствующие активы.

☐ Принимаю

Вопрос 10. Ознакомление с налоговым, валютным правом и Законом «О ПОД/ФТ» (подпункт 10 пункта 54).

Я ознакомлен с необходимостью соблюдения требований налогового, валютного законодательства, Закона о ПОД/ФТ/ФРОМУ и иных законов Республики Казахстан при совершении операций с цифровыми активами, и обязуюсь их соблюдать.

☐ Ознакомлен

Вопрос 11. Правовой статус необеспеченных цифровых активов (вопрос на знание, один правильный ответ).

Являются ли необеспеченные цифровые активы законным средством платежа на территории Республики Казахстан?

А. Да

Б. Нет (правильный ответ)

В. Да, но только стейблкоины

Вопрос 12. Последствия перевода в неподдерживаемой сети (вопрос на знание, один правильный ответ).

Что произойдёт при переводе цифрового актива на адрес в сети блокчейн, отличной от сети получателя (например, USDT стандарта ERC-20 на адрес сети TRC-20)?

А. Средства автоматически вернутся отправителю

Б. Оператор во всех случаях восстановит средства

В. Средства могут быть безвозвратно утрачены (правильный ответ)

Результат теста сохраняется в карточке клиента в личном кабинете с указанием:

— даты прохождения;

— балла (% правильных ответов);

— статуса (квалифицированный / неквалифицированный);

— фиксации согласия с рисками (с метками времени).

Повторное прохождение теста доступно через 30 (тридцать) календарных дней после последнего прохождения (пункт 55 Правил НБ № 45).

Интерпретация результата теста:

Результат	Категория клиента	Доступ
10–12 правильных (зачётных) ответов из 12 (не ниже 80 %) и все обязательные отметки о принятии рисков	Квалифицированный (КИ)	Операции без лимитов пункта 56; внутренние ПОД/ФТ-лимиты
Менее 10 из 12 либо отсутствие любой обязательной отметки	Неквалифицированный (НКИ)	Лимиты пункта 56: покупка до 7 000 000 ₸/сутки и продажа до 7 000 000 ₸/сутки

ПРИЛОЖЕНИЕ № 4. КАРТА ИНЦИДЕНТА КИБЕРБЕЗОПАСНОСТИ (ФОРМА)

ТОО «Ausu» · Правила осуществления деятельности оператора обмена необеспеченных цифровых активов

Канал выявления	
Описание инцидента	
Затронутые системы	
Категории затронутых данных	
Предварительная классификация и уровень критичности	
Принятые меры локализации	
Последствия и ущерб	
Первопричина	
Корректирующие действия	
Ответственные лица	
Время уведомления Национального Банка	
Приложения и доказательства	
Статус закрытия	

ПРИЛОЖЕНИЕ № 5. ЖУРНАЛ КОНТРОЛЯ ВСТРЕЧНОГО ИСПОЛНЕНИЯ ПО СДЕЛКАМ
(T+2) (ФОРМА)

(пункт 33 Правил НБ № 45: встречное исполнение в течение 2 (двух) рабочих дней с момента получения от клиента денег или цифровых активов)

[illegible]

Настоящие Правила утверждены Решением единственного участника ТОО «Ausu» № 2 от «2» июля 2026 года и введены в действие со 2 июля 2026 года (Приказ № 2 от 2 июля 2026 года).

ПОДПИСИ

Директор ТОО «Ausu» — единственный участник

 / Сахаров Никита Сергеевич /

М.П.

