Утверждена Решением
единственного участника
от 3 ноября 2025 года

ЗАО «Руба Кей Джи»

Программа внутреннего контроля в целях противодействия финансированию террористической деятельности и легализации (отмыванию) преступных доходов, а также на противодействие финансированию экстремистской деятельности, финансированию организованных групп или преступных сообществ и финансированию распространения оружия массового уничтожения

Бишкек 2025

Содержание

1. Общие положения

1.1. Настоящая Программа внутреннего контроля (далее – Программа) разработана Эмитентом виртуальных активов (далее – Эмитент) с целью соблюдения требований законодательства Кыргызской Республики, включая Закон Кыргызской Республики «О виртуальных активах» от 21 января 2022 года № 12, Постановление Кабинета Министров Кыргызской Республики от 16 сентября 2022 года № 514 «Об утверждении Положения об эмиссии (выпуске), обращении виртуальных активов и о порядке ведения Единого государственного реестра эмиссий виртуальных активов», а также с учётом международных стандартов и рекомендаций Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ).

1.2. Эмитент действует как от собственного имени, так и в интересах клиентов, от лица которых может осуществлять выпуск или погашение виртуальных активов. В обоих случаях Эмитент несёт ответственность за проведение надлежащих проверок, мониторинг операций и фиксирование всех данных в объёме, достаточном для последующей передачи ОФ «Альянс Фаундейшн», уполномоченным государственным органам и иным компетентным организациям.

1.3. Программа определяет следующие меры:

1. выявление, оценка, мониторинг, управление, снижение и документирование рисков;
2. проведение процедур KYC (Know Your Customer), KYB (Know Your Business) и KYT (Know Your Transaction);
3. идентификация и верификация клиентов, их представителей и бенефициарных владельцев;
4. анализ кошельков и транзакций с фиксацией уровня риска, результатов проверки и статуса адресов на момент анализа;
5. ведение реестра клиентов, сделок, транзакций и кошельков;
6. хранение сведений и документов, включая риск скоринг клиентов и транзакций, а также результаты всех проверок;
7. применение мер в отношении высокорискованных клиентов и кошельков;
8. применение процедур приостановки операций и заморозки активов в случае выявления санкционных или подозрительных связей;
9. обеспечение прозрачности эмиссии;
10. предоставление информации и документов ОФ «Альянс Фаундейшн» и уполномоченным органам при необходимости;
11. обеспечение конфиденциальности информации и ограничение доступа к ней.

1.4. Программа основывается на следующих принципах:

1. конфиденциальность информации о клиентах, бенефициарах, транзакциях и внутренних процедурах Эмитента;
2. добросовестность и прозрачность всех действий Эмитента при выпуске, погашении виртуальных активов;
3. риск-ориентированный подход к управлению клиентами и транзакциями;
4. исключение вовлечения Эмитента и его сотрудников в легализацию преступных доходов, финансирование терроризма и экстремизма;
5. обязательность документирования всех процедур проверки и принятых решений;
6. приоритет сохранения репутации Эмитента и Фонда ОФ «Альянс Фаундейшн» над коммерческими интересами в случае сомнительных ситуаций.

1.5. Настоящая Программа регулирует:

1. внутреннее взаимодействие сотрудников Эмитента в сфере управления рисками;
2. порядок обмена данными и информацией с Фондом в рамках договорных отношений;
3. взаимодействие с государственными органами Кыргызской Республики, включая Службу регулирования и надзора за финансовым рынком при Министерстве экономики и коммерции КР.

1.6. Положения, не урегулированные настоящей Программой, определяются в соответствии с действующим законодательством Кыргызской Республики и применимой международной практикой.

1.7. В случае изменения законодательства или стандартов в сфере виртуальных активов и ПФТД/ЛПД Эмитент руководствуется актуальными нормами до внесения соответствующих изменений в настоящую Программу.

2. Термины и определения

2.1. Для целей настоящей Программы применяются следующие термины:

1. Эмитент виртуальных активов (Эмитент) — юридическое лицо, осуществляющее выпуск и погашение виртуальных активов от имени клиента, а также ответственное за проведение KYC, KYB, KYT процедур и фиксацию всей информации, связанной с клиентами и транзакциями, в объёме, необходимом для предоставления Фонду и (или) уполномоченным органам.

2. Виртуальный актив (ВА) — совокупность данных в электронной форме, имеющая стоимость и являющаяся цифровым выражением имущественных и/или неимущественных прав, создаваемая с использованием технологии распределённого реестра.

3. Клиент — физическое или юридическое лицо, а также их представители и бенефициарные владельцы, вступающие в отношения с Эмитентом в целях приобретения или использования виртуальных активов.

4. Бенефициарный владелец — физическое лицо (физические лица), которое в конечном итоге (через цепочку владения и контроля) прямо или косвенно (через третьих лиц) владеет правом собственности или контролирует клиента либо физическое лицо, от имени или в интересах которого совершается операция (сделка)

5. Идентификация — установление идентификационных данных о клиенте и (или) бенефициарном владельце.

6. Верификация — подтверждение достоверности идентификационных данных клиента и (или) бенефициарного владельца.

7. Надлежащая проверка (Due Diligence, DD) — комплекс мер по идентификации и верификации клиента, установлению бенефициарных владельцев, а также анализу источников средств и целей взаимодействия.

8. Расширенная проверка (Enhanced Due Diligence, EDD) — углублённая проверка клиентов и операций, применяемая в отношении лиц и сделок с повышенным уровнем риска.

9. KYC (Know Your Customer) — процедуры идентификации и проверки физических лиц — клиентов Эмитента.

10. KYB (Know Your Business) — процедуры проверки юридических лиц — клиентов Эмитента.

11. KYT (Know Your Transaction) — процедуры анализа транзакций и криптовалютных адресов клиентов с использованием специализированных платформ.

12. Подозрительная операция (сделка) — операция, вызывающая подозрения по признакам отсутствия очевидного экономического смысла либо наличия признаков легализации доходов или финансирования терроризма.

13. Высокорискованные страны — государства и территории, которые не применяют или применяют в недостаточной степени международные стандарты по ПОД/ФТ, а также оффшорные зоны.

14. Публичное должностное лицо (PEP) — лицо, выполняющее или выполнявшее значительные государственные, политические или международные функции, а также его близкие родственники и связанные лица.

15. Санкционный перечень — списки физических и юридических лиц, в отношении которых применяются международные или национальные санкции.

16. Уполномоченный орган в сфере ВА — Служба регулирования и надзора за финансовым рынком при Министерстве экономики и коммерции Кыргызской Республики.

2.2. Термины, не указанные в настоящей Программе, применяются в значении, установленном законодательством Кыргызской Республики.

3. Структура системы внутреннего контроля в целях ПФТД/ЛПД

3.1. Для целей ПФТД/ЛПД у Эмитента формируется следующая структура внутреннего контроля:

1. Руководитель Эмитента (Генеральный директор):

а) определяет адекватную и эффективную политику в сфере ПФТД/ЛПД;
б) утверждает Программу внутреннего контроля и иные внутренние документы;
в) обеспечивает функционирование системы внутреннего контроля;
г) утверждает назначение и освобождение Комплаенс офицера;

2. Комплаенс офицер Эмитента:

а) внедряет и контролирует исполнение политики и процедур в сфере ПФТД/ЛПД;
б) проводит KYC, KYB и KYT процедуры при онбординге и в ходе обслуживания клиентов;
в) фиксирует результаты проверок (идентификация, верификация, анализ кошельков и транзакций, присвоение уровня риска);
г) формирует внутренние отчёты о подозрительных операциях (ISTR);
д) ведёт реестр клиентов, транзакций и кошельков, включая риск скоринг и историю проверок;
е) организует хранение документов и данных в соответствии с требованиями законодательства;
ж) готовит и передаёт Фонду по его запросу полные пакеты данных о клиентах и операциях;
з) взаимодействует с руководством и при необходимости инициирует внутренние расследования.

3.2. Каждый сотрудник Эмитента, вовлечённый в процессы онбординга, проверки и сопровождения клиентов, обязан:

1. соблюдать внутренние процедуры ПФТД/ЛПД;
2. фиксировать подозрительные операции и передавать информацию Комплаенс офицеру;
3. обеспечивать конфиденциальность сведений, полученных в ходе работы.

3.3. Эмитент несёт ответственность за полноту и корректность проведённых KYC/KYB/KYT процедур, а также за ведение реестров клиентов и сделок в объёме, достаточном для их последующей проверки или передачи по запросу.

4. Меры по выявлению, оценке, снижению и документированию рисков

4.1. Эмитент в лице Комплаенс офицера применяет риск-ориентированный подход, предусматривающий:

1. применение усиленных мер проверки при высоком уровне риска;
2. применение упрощённых мер проверки при низком уровне риска;
3. обязательное применение усиленных мер при наличии подозрений на ПФТД/ЛПД вне зависимости от формальной классификации.

4.2. Внутренние требования Эмитента предусматривают оценку риска клиента до установления деловых отношений и в ходе их сопровождения.

Классификация рисков:

1. Страновые риски — оценка юрисдикции клиента и контрагентов (санкции, оффшорный статус, уровень коррупции, наличие мер ПОД/ФТ).
2. Клиентские риски — статус клиента (физическое/юридическое лицо), наличие бенефициарных владельцев, связь с публичными должностными лицами (PEP), структура собственности.
3. Операционные риски — риски, связанные с продуктами, услугами, транзакциями или каналами взаимодействия (тип эмиссии, назначение токенов, особенности транзакций, риск кошельков).

4.3. При оценке риска Комплаенс офицер учитывает:

1. идентификационные данные клиента, его представителя и бенефициаров;
2. результаты проверки клиента и кошельков по санкционным перечням и базам KYT;
3. выявление связей клиента или бенефициаров с ПДЛ и высокорисковыми структурами;
4. сведения о целях установления и предполагаемом характере деловых отношений;
5. источники происхождения средств и экономический смысл операций;
6. результаты анализа транзакций и истории адресов в блокчейне;
7. данные о предыдущем взаимодействии с клиентом (поведение, репутация).

4.4. Решение о присвоении уровня риска (низкий / средний / высокий / критический) принимается на основании мотивированного заключения Комплаенс офицера.

4.5. Высокий и критический уровень риска требует применения следующих мер:

1. расширенной проверки (EDD), включая запрос дополнительных данных и документов;
2. установления источника происхождения средств;
3. постоянного мониторинга транзакций (KYT) и обновления досье клиента;
4. возможного отказа в обслуживании или приостановления операций до завершения анализа.

4.6. Все результаты проверки фиксируются в реестре Эмитента:

1. данные клиента, бенефициаров, представителей;
2. присвоенный уровень риска и дата его установления;
3. отчёт о KYT проверке кошельков и транзакций;
4. внутренние комментарии Комплаенс офицера;
5. итоговое решение и ответственное лицо.

4.7. Пересмотр уровня риска осуществляется:

1. при появлении новых данных о клиенте или его бенефициарах;
2. при изменении транзакционной активности;
3. по итогам периодических проверок, не реже одного раза в год.

4.8. Эмитент несёт ответственность за полноту оценки рисков клиентов и обязуется при необходимости передавать Фонду полные данные из реестров (KYC/KYB/KYT, риск скоринг, историю транзакций и кошельков) для проверки.
4.9. Эмитент учитывает риск кошельков. Высокорискованными считаются адреса, которые:

1. связаны с финансированием терроризма, даркнет рынками, миксерами, мошенничеством или киберпреступностью;
2. включены в международные санкционные списки;
3. участвуют в транзакциях с критическим уровнем риска по результатам анализа KYT;

4.10. При выявлении клиента или кошелька, относящегося к категории высокого риска, Эмитент:

1. отказывает в эмиссии или сжигании токенов с использованием данного адреса;
2. фиксирует выявленные риски и запросы документов;
3. запрашивает у клиента пояснения и подтверждение источников средств;
4. принимает внутреннее решение о дальнейшем сотрудничестве.

4.11. Решение о продолжении или прекращении отношений с клиентом высокого риска принимается Руководителем Эмитента совместно с Комплаенс офицером. Приоритет отдаётся минимизации правовых и репутационных рисков.

4.12. Эмитент ведёт внутренний реестр случаев выявления высокорискованных кошельков, в который включаются:

1. сведения о клиенте;
2. адреса кошельков;
3. описание выявленных признаков;
4. применённые меры и итоговое решение.

5. Надлежащая проверка клиентов (KYC/KYB) и транзакций (KYT)

5.1. Надлежащая проверка клиентов (НПК) является ключевым элементом внутреннего контроля Эмитента и включает:

1. идентификацию и верификацию клиентов;
2. сбор информации о целях и характере деловых отношений;
3. установление и проверку бенефициарных владельцев;
4. анализ источника происхождения средств (при необходимости – запрос дополнительных данных и подтверждающих документов);
5. документирование и хранение всех полученных данных;
6. мониторинг и обновление информации на протяжении всего срока отношений;
7. анализ транзакций и кошельков с использованием процедур KYT.

5.2. Эмитент применяет НПК как в отношении клиентов, с которыми он взаимодействует. Эмитент несёт ответственность за полноту и качество проверок как в отношении себя, так и в отношении своих клиентов перед Фондом.

5.3. KYT: проверка транзакций и кошельков

5.3.1. Эмитент проверяет кошельки и транзакции клиентов до эмиссии и сжигания токенов — проверка адреса кошелька, на который планируется выпуск или с которого планируется сжигание.

5.3.2. Проверка проводится с использованием специализированных сервисов.

5.3.3. Риски классифицируются:

1. низкий — адрес безопасен, транзакции стандартные;
2. средний — косвенные связи с рисковыми адресами, требуется ручная проверка;
3. высокий — прямая связь с рисковыми адресами, эмиссия или операция приостанавливается;
4. критический — связь с санкционными кошельками, даркнетом, террористическим финансированием; операции блокируются.

5.3.4. При выявлении риска Эмитент вправе запросить у клиента:

1. сведения о назначении операции;
2. подтверждение источника происхождения средств;
3. пояснения о целях транзакции.

5.4. Дополнительные положения
Эмитент обязан идентифицировать клиента, не допускается выпуск и сжигание токенов с использованием анонимных кошельков.
Идентификация клиентов и бенефициаров проводится через заполнение анкет (бумажных или электронных).
Обновление анкет возможно дистанционно, с использованием ЭЦП или других надёжных каналов.
Все документы должны быть действительными на момент предоставления.
В отношении ПДЛ применяются усиленные меры: обязательное анкетирование, установление источника средств, разрешение Руководителя Эмитента и постоянный мониторинг.

Эмитент фиксирует все результаты KYC, KYB и KYT в реестре:

1. данные клиента и его представителей;
2. сведения о бенефициарах;
3. риск скоринг;
4. историю транзакций и кошельков на момент проверки;
5. принятые решения.

5.5. Эмитент вправе отказать в обслуживании или исполнении распоряжения клиента, если:

1. документы не предоставлены или являются недостоверными;
2. выявлены признаки связи с отмыванием доходов или финансированием терроризма;
3. кошельки клиента признаны высокорисковыми.

6. Применение целевых финансовых санкций и приостановление операций (сделок)

6.1. Эмитент обязан применять меры по замораживанию и приостановлению операций в отношении клиентов, их представителей, бенефициарных владельцев и используемых ими кошельков, если они:

1. включены в национальные или международные санкционные перечни;
2. связаны с финансированием терроризма, экстремизма, распространением оружия массового уничтожения;
3. идентифицированы как высокорискованные в результате анализа KYT.

6.2. Проверка санкционных совпадений и уровня риска проводится:

1. при онбординге клиента;
2. перед эмиссией токенов на кошелёк клиента;
3. перед сжиганием (погашением) токенов клиента;
4. в ходе регулярного мониторинга.

6.3. В случае выявления совпадения с санкционным перечнем или при присвоении критического риска Эмитент:

1. без уведомления клиента приостанавливает операции по эмиссии и погашению виртуальных активов;
2. фиксирует меры в реестре замороженных активов/приостановленных операций и уведомляет Руководителя Эмитента;
3. инициирует внутреннее расследование и принимает решение о дальнейшем взаимодействии.

6.4. В случае выявления высокого риска (например, кошелёк клиента имеет связь с даркнетом, миксерами, мошенничеством или хакерскими инцидентами), Эмитент:

1. приостанавливает эмиссию или обращение токенов на данный кошелёк;
2. запрашивает у клиента дополнительные документы и сведения о происхождении средств;
3. принимает решение о возможном возобновлении операций после внутренней оценки рисков.

6.5. Разблокирование активов или возобновление операций осуществляется исключительно на основании:

1. внутреннего решения Руководителя Эмитента совместно с Комплаенс офицером;
2. официальных указаний уполномоченных органов Кыргызской Республики.

6.6. Эмитент ведёт внутренний реестр замороженных и приостановленных активов, который включает:

1. сведения о клиенте;
2. адреса кошельков;
3. дату и основания приостановки операций/замораживания активов;
4. принятые меры;
5. дату и основания размораживания активов и восстановления обслуживания клиента на выпуск и погашение виртуальных активов.

6.7. В отсутствие детализированных инструкций регулятора в сфере виртуальных активов Эмитент руководствуется:

1. рекомендациями FATF и лучшей международной практикой;
2. собственными внутренними процедурами управления рисками;
3. принципом предосторожности и защиты деловой репутации.

6.8. При работе от имени клиента Эмитент несёт ответственность перед Фондом за проведение всех необходимых проверок (KYC/KYB/KYT) и документирование принятых решений.

6.9. Все случаи замораживания или приостановления фиксируются и хранятся не менее 5 лет с возможностью последующей передачи информации в Фонд или уполномоченные органы по запросу.

7. Хранение информации и документов, обеспечение конфиденциальности сведений

7.1. Эмитент обязан хранить:

1. анкеты клиентов, анкеты бенефициаров, а также переписку и копии документов, полученные в результате проведения процедур KYC/KYB, — не менее 5 лет после прекращения деловых отношений или завершения операции;
2. сведения и документы обо всех операциях с виртуальными активами, включая эмиссию, сжигание и трансфер токенов, — не менее пяти лет после завершения операции;
3. отчёты по результатам оценки риска, KYT анализа транзакций и внутренние заключения — не менее 5 лет после их составления;
4. внутренние журналы, реестры сделок и досье клиентов — в том объёме, который позволяет восстановить полную историю взаимодействия и операций.

7.2. Хранимые сведения должны обеспечивать возможность:

1. восстановления цепочки операций клиента;
2. отслеживания источника и движения средств;
3. использования информации в качестве доказательства при необходимости.

7.3. Эмитент обеспечивает конфиденциальность информации, включая:

1. персональные данные клиентов и их представителей;
2. сведения о бенефициарных владельцах;
3. данные о кошельках и транзакциях;
4. результаты проверок KYC, KYB, KYT.

7.4. Доступ к информации имеют только уполномоченные сотрудники Эмитента. Разглашение сведений третьим лицам не допускается, за исключением случаев, прямо предусмотренных законодательством или договором с Фондом.

7.5. Документы могут храниться в бумажной и/или электронной форме.

7.6. Обязанность соблюдать конфиденциальность сохраняется за сотрудниками Эмитента и после прекращения их трудовых отношений.

8. Предоставление информации и документов в уполномоченные органы и Фонд

8.1. Эмитент несёт ответственность за проведение надлежащей проверки себя и своих клиентов (KYC, KYB, KYT), а также за формирование и хранение досье, реестра сделок и результатов анализа транзакций.

8.2. По запросу Фонда или уполномоченных органов Эмитент предоставляет:

1. сведения о клиентах, их представителях и бенефициарах;
2. анкеты и документы, подтверждающие их идентификацию;
3. результаты риск оценки и присвоенные уровни риска;
4. историю транзакций и операций с виртуальными активами (включая отчёты KYT);
5. реестр эмиссий, сжиганий токенов;
6. внутренние отчёты по операциям, признанным высокорискованными;

8.3. Передача информации и документов осуществляется:

1. по официальным запросам Фонда;
2. в рамках исполнения договорных обязательств между Эмитентом и Фондом;
3. по запросам уполномоченных государственных органов Кыргызской Республики.

8.4. Информация предоставляется:

1. на бумажном носителе с подписью уполномоченного лица (и печатью при необходимости);
2. в электронной форме.

8.5. Эмитент фиксирует факты передачи информации, включая:

1. дату и время передачи;
2. орган или организацию получателя;
3. перечень переданных материалов;
4. должность и ФИО ответственного сотрудника.

8.6. Конфиденциальность передаваемых данных обеспечивается путём:

1. ограничения доступа к ним только для сотрудников, участвующих в подготовке;
2. хранения копий переданных документов в защищенном архиве;
3. запрета на разглашение факта и содержания передачи третьим лицам.

8.7. Нарушение требований по сохранности и конфиденциальности информации влечёт дисциплинарную и/или правовую ответственность.

9. Заключительные положения

9.1. Настоящая Программа утверждается учредителем (Руководителем) Эмитента и подлежит пересмотру по мере необходимости.

9.2. Все изменения и (или) дополнения к Программе оформляются в виде новой редакции внутреннего нормативного документа (ВНД) и доводятся до сведения сотрудников Эмитента.

9.3. При отсутствии изменений и дополнений Комплаенс офицер обязан уведомить учредителя (Руководителя) о действующей редакции Программы и подтвердить её актуальность.

9.4. По вопросам, не урегулированным настоящей Программой, Эмитент руководствуется:

1. законодательством Кыргызской Республики;
2. внутренними документами Эмитента;
3. обязательствами перед Фондом и клиентами в части KYC, KYB и KYT.

9.5. В случае если отдельные положения Программы вступят в противоречие с действующим законодательством Кыргызской Республики, применяются нормы законодательства до внесения соответствующих изменений в Программу.