AML ПОЛІТИКА ОБМІННОГО ПУНКТУ

Політика щодо Протидії Відмиванню Коштів (AML) та Ідентифікації Клієнтів (KYC)

Дата внесення останніх змін: 27 березня 2026 р.

Вступ

Ця політика описує заходи, що вживаються для дотримання міжнародних стандартів у сфері ідентифікації клієнтів (KYC) та запобігання відмиванню коштів (AML). Вона спрямована на забезпечення законності операцій та запобігання використанню платформи для протиправної діяльності.

1. Цілі

1.1. Дотримання чинного законодавства у сфері KYC та AML.

1.2. Запобігання використанню платформи для відмивання коштів, фінансування тероризму та іншої незаконної діяльності.

1.3. Формування ефективних процедур перевірки клієнтів.

2. Основні терміни

2.1. KYC — процедури ідентифікації особи клієнта.

2.2. AML — комплекс заходів щодо виявлення та запобігання легалізації доходів, отриманих злочинним шляхом або спрямованих на фінансування тероризму.

2.3. Dark Market — онлайн-платформи, що поширюють заборонені товари та послуги.

2.4. Санкції — обмеження, запроваджені офіційними структурами щодо країн або фізичних/юридичних осіб.

2.5. Викрадені монети — криптовалютні одиниці, отримані шляхом крадіжки або шахрайства та/або включені до санкційних списків або списків об’єктів кримінального розслідування.

2.6. Шахрайство (scam) — дії, спрямовані на обман користувачів з метою отримання неправомірної вигоди.

2.7. Операції високого ризику — операція, ознаки якої вказують на підвищений ризик відмивання коштів або фінансування тероризму (наприклад, нетипові суми, походження коштів із високоризикових юрисдикцій, зв'язок із санкціями, гемблінг індустрією або іншими підозрілими факторами).

3. Ідентифікація клієнтів

3.1. Користувач зобов'язаний надати документи, що посвідчують особу, на першу вимогу. Оператор залишає за собою право запросити додаткову інформацію для підтвердження особи або аналізу окремої операції. Це може включати паспорт, посвідчення особи, підтвердження адреси, а також використання сторонніх KYC-сервісів.

3.2. Мінімальний перелік документів:

- ідентифікаційний документ (паспорт, закордонний паспорт, ID-картка, водійське посвідчення тощо);
- селфі для підтвердження особи;
- додаткова інформація, необхідна для повної верифікації відповідно до міжнародних стандартів KYC (наприклад, номер телефону, адреса електронної пошти тощо).

4. Механізми контролю

4.1. Для аналізу операцій і виявлення підозрілої активності використовується зовнішній сервіс аналізу транзакцій і чистоти коштів, що надходять.

4.2. Усі транзакції проходять постійний моніторинг для виявлення аномалій або підозрілих схем.

5. Підвищений AML ризик

При виявленні ознак високого рівня ризику Оператор залишає за собою право:

5.1. Тимчасово заблокувати операцію до 14 днів або до завершення розслідування.

5.2. Запросити додаткові документи, фото або відео, що підтверджують особу.

5.3. Вимагати докази походження коштів (скриншот гаманця, історія транзакцій).

5.4. Повернення коштів здійснюється лише після повної верифікації на те саме джерело.

5.5. Запит додаткових матеріалів, що стосуються операції.

5.6. Відхилити виведення коштів на чужі реквізити без пояснення причин.

5.7. Повернення коштів можливе протягом 14 календарних днів після прийняття рішення, за вирахуванням комісії. У разі відсутності відповіді від клієнта протягом 3 місяців кошти не підлягають поверненню.

5.8. Взаємодія здійснюється виключно через e-mail, зазначений у заявці.

5.9. За наявності офіційного запиту від правоохоронних органів кошти можуть бути заморожені.

5.10. У разі виявлення зв’язку коштів із санкціями вони можуть бути заблоковані на невизначений строк.

6. Процедури перевірки

6.1. Оператор розробив систему для виявлення високоризикових транзакцій та іншої протиправної діяльності з урахуванням ризиків відмивання коштів і фінансування тероризму. Зокрема, Оператор має право заморожувати кошти до надання необхідної інформації та завершення перевірок.

6.2. Для зниження ризику заморожування коштів Оператор рекомендує Користувачам:

- заздалегідь проходити власну AML-перевірку перед здійсненням операцій;
- регулярно ознайомлюватися з актуальною редакцією цієї Політики;
- використовувати виключно визнані міжнародні спеціалізовані сервіси для проведення AML-перевірок.

6.3. Оператор здійснює постійний моніторинг усіх транзакцій користувачів для виявлення аномальних або підозрілих операцій.

6.4. Під «підозрілою операцією» розуміється будь-яка транзакція, яка:

- пов’язана з коштами, отриманими внаслідок незаконної діяльності;
- не має очевидної законної мети;

- сприяє здійсненню злочинної діяльності (наприклад, шахрайство, відмивання коштів, фінансування тероризму, корупція чи порушення санкцій).)

6.5. У разі перевищення встановленого порогового рівня AML-ризику або виявлення коштів з високим ризиком (Dark Market, Санкції, Stolen Coins, Scam та ін.), Оператор залишає за собою право:

- призупинити транзакцію або заморозити (утримувати) кошти до завершення розслідування, проведення повної верифікації особи та перевірки фінансової інформації;
- запитувати у користувача фото чи відео з документом, що підтверджує особу;
- запитувати скріншоти або відео з облікового запису крипто-гаманця;
- запитувати інші матеріали та документи, що стосуються операції, включаючи документи одержувача коштів за заявкою;
- відмовити у виведенні коштів на рахунок третіх осіб без пояснення причин.
- У разі ненадання інформації або відсутності відповіді протягом 3 місяців кошти можуть залишатися замороженими. Кошти, заморожені у зв'язку із санкціями, можуть залишатися заблокованими до їх зняття.

6.6. Оператор має право успішно завершити обмінну операцію лише після:

• проведення повної верифікації особи Користувача відповідно до вимог цієї Політики та міжнародних стандартів KYC;

• оцінки ризиків транзакції, включаючи перевірку на зв'язок із високоризиковими джерелами, санкціями, Dark Market, Stolen Coins, Scam та іншими ознаками, визначеними цією Політикою;

• перевірки всіх наданих Користувачем документів та інформації, включаючи ідентифікаційні дані, скріншоти або відео з гаманців, та інші матеріали, якщо транзакція класифікована як високоризикова.

7. Обмежені території та санкції

7.1. Оператор не надає послуги особам, що знаходяться на території або пов'язаних з територіями, таких держав і регіонів як: Республіка Абхазія, Республіка Південна Осетія, Нагірно-Карабахська Республіка, Турецька Республіка Північного Кіпру, Придністровська Молдавська Республіка, а також території, що тимчасово не

контролюються урядом України, включаючи Автономну Республіку Крим, окремі райони Донецької та Луганської областей.

7.2. Оператор не надає послуги особам, включеним у відповідні списки санкцій, включаючи списки Організації Об'єднаних Націй, Європейського Союзу, Казначейства Великобританії та Управління з контролю за іноземними активами США (OFAC). Компанія регулярно перевіряє Користувачів за вказаними списками та залишає за собою право припиняти або припиняти дію будь-якого облікового запису, що становить санкційний ризик.

8. Повідомлення про підозрілі операції

Співробітники здійснюють моніторинг та повідомляють компетентні органи у разі виявлення підозрілих операцій.

9. Заморожування та завершення операцій

9.1. З метою дотримання законодавства у сфері AML та запобігання шахрайству, а також захисту прав та законних інтересів Оператора та її користувачів, Оператор залишає за собою право тимчасово зупиняти або заморожувати операції та засоби Користувача, при виявленні підвищеного ризику, підозрілих транзакцій чи невідповідностей у поданих даних.

До таких випадків можуть належати операції, пов'язані з високоризиковими джерелами, санкційними особами або обмеженими територіями, Dark Market, Stolen Coins, Scam та іншими ознаками, визначеними цією Політикою.

9.2. Повернення коштів або завершення обмінної операції здійснюється лише після успішної верифікації особи Користувача, підтвердження достовірності всіх документів та інформації, наданої Користувачем, а також успішного проходження внутрішньої перевірки операцій службою безпеки.

9.3. Усі звернення, пов'язані із замороженими засобами, приймаються лише через офіційні канали зв'язку, вказані на сайті Оператора, з електронної пошти або Telegram облікового запису, зазначеного Користувачем при поданні Заявки. Кошти можуть залишатися тимчасово утриманими до завершення всіх обов'язкових процедур.

10. Зберігання даних

Усі документи та дані, надані Користувачами, включаючи результати проведеної верифікації, зберігаються не менше ніж п'ять (5) років після завершення відносин з Користувачем. Оператор збирає, зберігає та захищає персональні дані Користувачів, відповідно до застосовних норм про захист даних, а також вимог щодо протидії відмиванню коштів та фінансуванню тероризму. Записи про верифікацію та транзакції надаються компетентним регуляторним або правоохоронним органам виключно за законним запитом.

11. Оновлення політики

Оператор може час від часу вносити зміни до цієї Політики для відображення змін у законодавчих чи нормативних вимогах, а також для покращення внутрішніх процедур. Політика може змінюватись керівництвом Оператора в односторонньому порядку без попередження Користувачів. Всі оновлення публікуються на нашому сайті із зазначенням дати останньої зміни у верхній частині сторінки.

Політика може змінюватися без попередження.

12. Контакти

Якщо у вас є питання щодо цієї Політики або процедури Оператора, звертайтесь через email або Telegram, які вказані в розділі контактів Оператора crypto-bank.exchange.