# ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЮ ДЕНЕЖНЫХ СРЕДСТВ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА (AML/CFT) ПЛАТФОРМЫ Get Crypto

## 1.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

### 1.1. Отмывание денежных средств (AML)

Отмывание денежных средств (AML) — процесс придания правомерного вида доходам, полученным в результате преступной деятельности, с целью их легализации. Под преступной деятельностью понимаются деяния, предусмотренные Уголовным кодексом РФ (в частности, статьей 174 УК РФ "Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем") и иными нормами, признанными РФ, включая международные стандарты (например, рекомендации ФАТФ).

**В рамках настоящей Политики под AML понимаются:**

- Любые действия, направленные на сокрытие происхождения, источника или права собственности на цифровые активы, полученные преступным путем;
- Использование сервисов Операторов ОП для операций с активами, связанными с преступлениями (мошенничество, коррупция, торговля запрещенными товарами);
- Сокрытие информации о бенефициарах, источниках средств или целях транзакций в обход процедур KYC/AML, проводимых Операторами ОП;
- Проведение операций, нарушающих требования ст. 7.1–7.3 Федерального закона № 115-ФЗ (уклонение от идентификации, верификации, отчетности).

**К AML также относятся:**

- Участие, пособничество или содействие в легализации преступных доходов;
- Использование инструментов анонимизации (миксеры, тумблеры) без проведения EDD Оператором ОП.

***Примечание:***

- *Выявление и предотвращение AML — обязанность Операторов ОП, которые обязаны внедрять процедуры KYC, EDD и мониторинга в соответствии с ФЗ-115 и ФАТФ.*
- *Платформа контролирует соблюдение Операторами AML-требований через аудит, но не участвует в проведении транзакций или проверке активов.*

### 1.2. Финансирование терроризма (CFT)

Финансирование терроризма (CFT) — это предоставление или сбор средств, Цифровых Активов или иных финансовых ресурсов с целью их использования для совершения террористических актов, поддержки террористических организаций или отдельных лиц, связанных с терроризмом. Под террористической деятельностью понимаются деяния, предусмотренные статьей 205 Уголовного кодекса Российской Федерации ("Террористический акт") и Федеральным законом № 35-ФЗ "О противодействии терроризму", а также статья 205.1 УК РФ ("Содействие террористической деятельности").

**В настоящей Политике под финансированием терроризма понимаются:**

- любые операции с Цифровыми Активами, направленные на прямое или косвенное финансирование террористической деятельности;
- использование Платформы для сбора, перевода или обмена Цифровых Активов в интересах террористических организаций или лиц, включенных в перечни террористов и экстремистов, утвержденные в соответствии с законодательством РФ и международными стандартами;
- умышленное сокрытие информации о целях и участниках транзакций, связанных с финансированием терроризма;
- любую деятельность, которая прямо может быть квалифицирована как "финансирование терроризма" по любому применимому праву, включая законодательство РФ и международные стандарты.

Легализация средств, полученных преступным путем, и финансирование терроризма далее совместно именуются «**Запрещенными Операциями**».

### 1.3. Подозрительные Транзакции

Подозрительные Транзакции — операции с цифровыми активами, которые имеют признаки, указывающие на возможное отмывание денежных средств, финансирование терроризма или иные противоправные действия, выявленные Операторами ОП в ходе мониторинга. К ним относятся:

- Транзакции, не соответствующие обычной деятельности Пользователя или профилю риска, установленному Оператором ОП;
- Операции, связанные с цифровыми активами, происхождение которых невозможно установить в рамках процедур EDD, проводимых Оператором ОП;
- Транзакции с участием лиц/организаций, включенных в перечни террористов, экстремистов или санкционные списки Росфинмониторинга, ФАТФ и иных уполномоченных органов;
- Использование «грязных» криптокошельков (связанных с незаконными площадками), идентифицированных через инструменты анализа блокчейна (например, Chainalysis);
- Операции, направленные на уклонение от KYC/AML-процедур, включая применение анонимных инструментов (mixers, tumblers) или подставных лиц;
- Транзакции с аномальными параметрами (сумма, частота, география), превышающие пороги, установленные ст. 6 Федерального закона № 115-ФЗ;
- Любые иные операции, подпадающие под критерии подозрительности, закрепленные во внутренних правилах Операторов ОП в соответствии с:
  (i) Федеральным законом № 115-ФЗ;
  (ii) Приказами и Постановлениями регуляторов;
  (iii) Рекомендациями ФАТФ (включая Правило 15).

Примерный перечень подозрительных операций приведен в Приложении № 1 к настоящей Политике.

***Примечание:***

*Критерии подозрительности определяются Операторами ОП на основании законодательства РФ и международных стандартов. Платформа не проводит мониторинг транзакций, но контролирует наличие у Операторов процедур их выявления.*

### 1.4. Политически значимые лица (PEP)

Политически значимые лица (PEP) — физические лица, занимающие или занимавшие в течение последних 12 месяцев высокие государственные должности, а также их близкие родственники и доверенные лица. К PEP также относятся лица, имеющие прямые или косвенные связи с офшорными юрисдикциями, включая:

- владение активами (включая цифровые) через юридические структуры, зарегистрированные в офшорных зонах;
- осуществление операций с использованием счетов или сервисов, базирующихся на территориях, признанных в соответствии с международными стандартами (включая рекомендации ФАТФ) как зоны с повышенными рисками AML/CFT;
- установление деловых или финансовых отношений с организациями, связанными с офшорами.

Проверка PEP осуществляется Операторами ОП с использованием аккредитованных источников данных (коммерческие базы, сервисы, одобренные Росфинмониторингом). Платформа не предоставляет доступ к базам PEP, но контролирует наличие у Операторов ОП процедур их проверки

### 1.5. Подход, основанный на оценке рисков

Подход, основанный на оценке рисков (Risk-Based Approach (RBA)) — методология, при которой меры AML/CFT адаптируются в зависимости от уровня риска, связанного с конкретным пользователем, транзакцией или юрисдикцией. Применяется в соответствии с Рекомендацией 1 ФАТФ.

### 1.6. Санкционные юрисдикции

Санкционные юрисдикции (Sanctioned Jurisdictions) — страны или территории, включенные в перечни ФАТФ, ООН, ЕС, США (OFAC) или РФ как зоны повышенного риска отмывания денег, финансирования терроризма или распространения ОМУ. Примеры: Иран, Северная Корея, Сирия.

### 1.7. Высокорисковые активы

Высокорисковые активы (High-Risk Assets) — цифровые активы, которые:

- Имеют признаки анонимности (например, Monero, Zcash, Dash);
- Не имеют регулярного аудита резервов, подтверждающего обеспечение эмитентом (проводимого независимой организацией не реже 1 раза в 6 месяцев);

- Выпущены эмитентами, не раскрывающими информацию о бенефициарных владельцах или юрисдикции регистрации.

**1.8. Комплаенс (compliance)**

Комплаенс — это система мер, направленных на обеспечение соблюдения Операторами Обменных пунктов (ОП) требований законодательства РФ, включая Федеральный закон № 115-ФЗ, № 259-ФЗ, а также международных стандартов AML/CFT (рекомендации ФАТФ).

**В рамках функционала Платформы комплаенс включает:**

**1.8.1. Контроль за соблюдением Операторами ОП процедур AML/CFT**, включая:

- Проверку выполнения Операторами ОП требований по идентификации и верификации пользователей (KYC);
- Мониторинг отчетности Операторов ОП о подозрительных операциях;
- Обеспечение доступа Операторов ОП к базам данных Росфинмониторинга (списки террористов, PEP, санкционные перечни) (если применимо согласно функционалу Сервиса Оператора);

**1.8.2. Взаимодействие с регуляторами:**

- Уведомление Росфинмониторинга и иных уполномоченных органов о нарушениях со стороны Операторов ОП;
- Предоставление регуляторам данных о приостановленных/заблокированных Операторах ОП;

**1.8.3. Техническая поддержка Операторов ОП:**

- Предоставление API для интеграции Операторов ОП с внешними системами мониторинга транзакций (по запросу);
- Платформа не участвует в анализе транзакций, а лишь обеспечивает техническую совместимость решений.

***Примечание:***

- *Платформа не проводит KYC, не хранит данные верификации и не осуществляет мониторинг транзакций напрямую — эти функции выполняют Операторы ОП (ст. 1253.1 ГК РФ, п. 2 ст. 5 ФЗ-259);*
- *Реализация мер, соответствующих рекомендациям ФАТФ, включая "Правило путешествия" (Travel Rule), а именно — требование, согласно которому информация об отправителе и получателе транзакции передается вместе с транзакцией для обеспечения прозрачности и предотвращения отмывания денежных средств, применяется Операторами ОП при проведении транзакций с цифровыми активами (п. 5.4 ФЗ-259). Примеры данных, передаваемых Операторами ОП: «имя отправителя/получателя, номер кошелька, сумма, дата, цель транзакции».*

**1.9. Информационный сервис**

Информационный сервис — комплекс услуг Платформы по сравнению курсов и организации взаимодействия между Пользователями и Операторами ОП, без осуществления операций с цифровой валютой, её хранения или прямого контроля над транзакциями.

**Обязанности по AML/CFT в рамках сервиса:**

- Возложены на Операторов ОП как на субъектов, непосредственно проводящих операции с цифровыми активами (ст. 7.2 ФЗ-115).

**1.10. Ответственное лицо по AML/CFT**

Ответственное лицо по AML/CFT — сотрудник Платформы, осуществляющий контроль за соблюдением Операторами ОП требований AML/CFT, включая:

- Проверку включения в договоры с Операторами условий о проведении KYC, проверок PEP и списков террористов;
- Мониторинг выполнения Операторами обязательств по уведомлению Росфинмониторинга о подозрительных операциях;
- Организацию аудита процедур AML/CFT Операторов;
- Взаимодействие с надзорными органами по вопросам нарушений со стороны Операторов.

***Примечание:***

- *Ответственное лицо не проводит верификацию пользователей и не анализирует транзакции — эти функции выполняют Операторы ОП.*

**1.11. Гарантийный депозит (Security Deposit)** — денежные средства, внесенные Оператором ОП в качестве обеспечения исполнения обязательств по договору (ст. 329 ГК РФ).

Удержание депозита возможно только:

- по решению суда;
- по соглашению сторон, оформленному дополнительным протоколом.

Гарантийный депозит регулируется разделом 11.3 настоящей Политики.

**1.12. Обеспечение** — совокупность мер и активов (включая гарантийный депозит), направленных на исполнение обязательств Оператором ОП перед Платформой и пользователями. Регулируется ст. 329 ГК РФ и может включать залог, банковскую гарантию или иные формы, предусмотренные договором.

**1.13. Штрафные санкции** (Penalty Fees) — меры финансового воздействия, применяемые к Оператору ОП за нарушение условий сотрудничества, законодательства РФ или требований AML/CFT (например, штрафы, пени).

***Примечание:***

*Термины «гарантийный депозит», «обеспечение» и «штрафные санкции» не являются взаимозаменяемыми;*

- *Гарантийный депозит — это денежное обеспечение, а штрафные санкции — мера ответственности;*
- *Обеспечение — широкая категория, включающая как депозит, так и иные способы гарантии обязательств.*

**1.14.** Все остальные определения и термины, приведенные в настоящей Политике, имеют значения, присвоенные им в **Пользовательском соглашении** [ссылка]

## 2. ВВЕДЕНИЕ

### 2.1. Общие положения

Настоящая Политика AML/CFT (далее — «**Политика**») определяет порядок противодействия отмыванию доходов (**AML**), финансированию терроризма (**CFT**) и идентификации клиентов (**KYC**) для участников экосистемы Платформы Get Crypto (далее — «**Платформа**»).

**Роль Платформы:**

- Платформа является информационным посредником (ст. 1253.1 ГК РФ) и предоставляет сервис для сравнения курсов обменных пунктов цифровой валюты (далее — «**Операторы ОП**»).
- Платформа не является стороной сделок, не хранит цифровые активы и не контролирует транзакции между Пользователями и Операторами ОП.

**Ограничения:**

Платформа запрещает операции с:

- Анонимными криптовалютами (Monero, Zcash, Dash, Grin);
- Токенами, эмитенты которых не проводят регулярный аудит резервов (не реже 1 раза в 6 месяцев) или не раскрывают данные о бенефициарных владельцах.

Данное ограничение связано с внутренней политикой Платформы, а не прямым требованием закона (ст. 14 ФЗ-259).

### 2.2. Цель Политики

Цель Политики — минимизация рисков использования сервисов Платформы для незаконной деятельности, защита пользователей и обеспечение соответствия российским и международным стандартам AML/CFT.

#### 2.2.1. Информирование о рисках:

Операции с цифровыми активами связаны с повышенными рисками, включая волатильность курсов, мошенничество и технические сбои. Платформа рекомендует пользователям самостоятельно оценивать риски перед проведением транзакций. GetCrypto не несет ответственности за убытки, вызванные указанными факторами.

### 2.3. Нормативная база

Политика разработана в соответствии с:

**Основные законы РФ:**

- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте»,
- Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральный закон от 27.07.2006 N 152-ФЗ “О персональных данных”;

**Подзаконные акты:**

- Постановление Правительства РФ от 30.06.2012 № 667 «Об утверждении требований к правилам внутреннего контроля»;
- Приказ Росфинмониторинга от 07.09.2022 N 192 «Об утверждении Порядка проведения Федеральной службой по финансовому мониторингу контрольных мероприятий в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения»;
- Положение Банка России от 15.10.2015 N 499-П "Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"
- Указание Банка России от 07.11.2022 N 6308-У "О внесении изменений в нормативные акты Банка России в сфере требований к правилам внутреннего контроля кредитных организаций и некредитных финансовых организаций в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"

**Международные стандарты, конвенции и рекомендации:**

- Рекомендации ФАТФ (FATF). Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения, включая Правило 12 (риски PEP) и Правило 15 (обязанности посредников);
- Конвенцию ООН против коррупции (ратифицирована ФЗ № 40-ФЗ от 08.03.2006);
- Конвенцию Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности (Страсбург, 1990, ратифицирована ФЗ № 62-ФЗ от 28.05.2001);
- Рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), применяемые в рамках ФЗ № 115-ФЗ.

**Иные документы:**

- Федеральный закон от 06.03.2006 N 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 28.12.2012 N 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан РФ»;
- Постановление Правительства РФ от 19.02.2022 N 219 «Об утверждении Положения о контроле (надзоре) в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения»
- Постановление Правительства РФ от 11.04.2023 N 585 "Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере идентификации и (или) аутентификации"
- «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ст. 174, 205, 205.1);
- «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 N 230-ФЗ (ст. 1253.1);

**2.4. Распределение ответственности**

**2.4.1. Операторы ОП** несут полную ответственность за:

- Проведение KYC/AML-проверок Пользователей;
- Мониторинг транзакций и уведомление регуляторов о подозрительных операциях;
- Проверку клиентов по спискам террористов/PEP (ст. 7.2 ФЗ-115).

2.4.2. **Платформа** ограничивается:

- Аудитом документального соответствия процедур Операторов ОП требованиям законодательства. Данный аудит не освобождает Операторов ОП от ответственности за фактическое соблюдение AML/CFT-требований;
- Блокировкой Операторов ОП при выявлении системных нарушений.

**2.5. Обработка данных Пользователей**

**2.5.1. Персональные данные, собираемые Платформой:**

При регистрации Пользователь предоставляет минимальный набор персональных данных: ФИО и адрес электронной почты (ст. 3 ФЗ № 152-ФЗ).

**2.5.2. Соблюдение требований 152-ФЗ:**

Платформа обрабатывает данные исключительно для:

- Идентификации Пользователя в системе;
- Связи с Пользователем (уведомления, поддержка);
- Контроля соблюдения условий Пользовательского соглашения.

Обработка осуществляется с согласия Пользователя, выраженного при регистрации (п. 1 ст. 6 ФЗ-152) и в соответствии с **Политикой конфиденциальности Платформы** [ссылка]

**2.5.3. Распределение ответственности:**

- Платформа не запрашивает и не хранит документы, подтверждающие личность Пользователя (паспорт, адрес проживания), финансовые реквизиты или иную sensitive-информацию;
- Операторы ОП обязаны проводить полную верификацию Пользователей (включая паспортные данные, подтверждение адреса) в рамках своих AML/KYC-процедур.

**2.5.4. Защита данных:**

Платформа обеспечивает безопасность предоставленных данных с использованием шифрования, ограничения доступа и иных мер, предусмотренных ст. 19 ФЗ-152.

**2.6. Связь с иными документами**

Политика связана и является неотъемлемой частью:

- Пользовательского соглашения [ссылка]
- Политики Конфиденциальности [ссылка]
- Политики Платформы в отношении Cookie-Файлов [ссылка]

## 3. ОСНОВНЫЕ ПРИНЦИПЫ

Платформа придерживается следующих принципов:

**3.1. Соблюдение законодательства:**

Операторы ОП обязаны соблюдать требования законодательства РФ в области AML/CFT, включая Федеральный закон № 115-ФЗ, № 259-ФЗ, а также иные нормативные акты, в т.ч. рекомендации Банка России.

**Платформа:**

- контролирует включение в договоры с Операторами условий о соблюдении AML/CFT;
- обеспечивает доступ Операторов к актуальным регуляторным требованиям.

**3.2. Идентификация клиентов:**

**Операторы ОП обязаны:**

- проводить идентификацию и верификацию (KYC) Пользователей в соответствии с требованиями ФЗ-115 и ФЗ-259;
- предоставлять Платформе обезличенное подтверждение выполнения KYC по запросу.

**3.3. Мониторинг транзакций:**

**Операторы ОП обязаны:**

- осуществлять мониторинг транзакций для выявления подозрительных операций;
- использовать инструменты анализа блокчейна (например, Chainalysis, Elliptic, MixBytes и/или др.) для отслеживания «грязных» криптоактивов.

**3.4. Контроль за Операторами ОП:**

Платформа осуществляет:

- Регулярный аудит документального соответствия процедур Операторов ОП требованиям AML/CFT. Аудит направлен на проверку формального наличия процедур и не подразумевает оценки их фактического применения или эффективности;
- проверку наличия у Операторов ОП процедур KYC, EDD и отчетности;
- приостановку сотрудничества с Операторами ОП, нарушающими Политику.

**3.5. Конфиденциальность:**

**Операторы ОП:**

- несут ответственность за обработку персональных данных Пользователей в соответствии с ФЗ-152;
- обязаны обеспечить защиту данных, полученных в рамках KYC/AML.

**Платформа:**

- не хранит и не обрабатывает персональные данные Пользователей, за исключением минимальной информации, необходимой для идентификации в системе и связи с Пользователем (п. 2.5.2. Политики).

**3.6. Применение подхода, основанного на оценке рисков (RBA):**

Платформа и Операторы ОП обязаны:

3.6.1. Классифицировать пользователей по категориям риска (низкий, средний, высокий) на основе:

- Юрисдикции регистрации/пребывания;
- Объема и частоты транзакций;
- Используемых активов (высокорисковые/низкорисковые).

3.6.2. Адаптировать меры AML/CFT:

- Для **низкого риска**: упрощенная верификация (KYC Level 1);
- Для **высокого риска**: EDD, ежедневный мониторинг транзакций, ограничение лимитов.

3.6.3. Ежеквартально пересматривать профили рисков.

**3.7. Контроль доступа Операторов ОП к базам PEP**

Платформа:

3.7.1. Проверяет во время аудита, что Операторы ОП используют актуальные коммерческие базы данных PEP или сервисы, соответствующие требованиям:

- Приказ Росфинмониторинга от 29.06.2012 № 192 «Об утверждении требований к внутреннему контролю»;
- Рекомендации ФАТФ (Правило 12);

3.7.2. Требует от Операторов ОП документального подтверждения наличия договоров с провайдерами баз данных PEP;

3.7.3. Не предоставляет доступ к базам PEP и не участвует в их анализе.

## 4. ИДЕНТИФИКАЦИЯ И ВЕРИФИКАЦИЯ (KYC) ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

**4.1. Регистрация:**

**Операторы ОП обязаны запрашивать у Пользователей:**

- ФИО, дату рождения, контактные данные;
- паспортные данные и адрес проживания;
- ИНН (при наличии).

**4.2. Верификация:**

**4.2.1. Операторы ОП проводят верификацию, включая:**

- проверку сканов документов (паспорт/удостоверение, подтверждение адреса (счет за коммунальные услуги, выписка из банка, договор аренды);
- использование автоматизированных сервисов (например, Sumsub).

**4.2.2. Дополнительные документы:**

Операторы ОП вправе запрашивать у Пользователей:

- подтверждение источника средств;
- справки о занятости;
- иные документы в соответствии с профилем риска (например, фотографии с паспортом, видео-верификация и др.)

Пользователи обязаны предоставить Оператору ОП дополнительные документы в течение 72 часов с момента запроса.

**4.2.3. Проверка через сторонние сервисы:**

**Операторы ОП обязаны:**

- самостоятельно получать доступ к базам данных через лицензированных провайдеров (например, СКРИН или Контур) и иными источниками;
- использовать кредитные бюро и сервисы верификации личности.

**4.2.4. Меры при нарушении сроков предоставления документов:**

**Операторы ОП обязаны:**

- приостанавливать операции Пользователя до завершения проверки;
- уведомлять Платформу о случаях отказа в предоставлении документов.

**4.3. Упрощенная идентификация:**

**Операторы ОП вправе применять упрощенную процедуру для операций до 15 000 руб**. (например, подтверждение через SMS или электронную почту), если это не противоречит ст. 7.4 ФЗ-115.

## 5. ИДЕНТИФИКАЦИЯ И ВЕРИФИКАЦИЯ (KYC) ДЛЯ ОПЕРАТОРОВ ОП

**5.1. Регистрация**

**Оператор ОП обязан предоставить:**

- Реквизиты юридического лица (Наименование, ИНН, ОГРН, юридические и фактические адреса, контакты, данные руководителя);
- Информацию о бенефициарных владельцах (ФИО, паспортные данные, ИНН, доля участия, документы, подтверждающие статус бенефициара);
- Документы, подтверждающие невозможность установления бенефициара (при отсутствии) - подтверждение невозможности установления, приложить описание предпринятых мер по установлению бенефициарного владельца.

**5.2. Верификация**

**Оператор ОП обязан:**

5.2.1. Предоставить документы о **легитимности деятельности** (Устав, Учредительный договор, Протокол собрания учредителей, Лицензии, Выписки из ЕГРЮЛ и др.)

- Документы должны быть предоставлены в оригиналах или нотариально заверенных копиях
- Электронные копии должны быть подписаны квалифицированной электронной подписью
- Документы должны быть действительны на момент подачи: (i) документы, подтверждающие легитимность деятельности, паспортные данные и лицензии - до истечения срока действия, (ii) выписка из ЕГРЮЛ - 30 дней с момента получения;

5.2.2. Подтвердить **соблюдение AML/CFT** (внутренние политики, система мониторинга, обучение персонала), в т.ч. наличие доступа к аккредитованным базам данных PEP (например, предоставить договор с провайдером или скриншоты интерфейса системы проверки);

5.2.3. Обновлять данные в течение 3 рабочих дней при изменениях.

**Платформа:**

- Проводит первичную (при Листинге) и периодическую проверку документов Оператора ОП;
- Вправе запросить актуальные документы в любое время.

**5.3. Ответственное лицо по AML/KYC** (п.1.10):

**Ответственное лицо Оператора ОП** осуществляет:

- Контроль за идентификацией пользователей;
- Аудит мер AML/CFT;
- Принятие решений о дополнительной верификации.

## 6. ПРОТИВОДЕЙСТВИЕ ОТМЫВАНИЮ ДОХОДОВ (AML) И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА (CFT)

**6.1. Мониторинг транзакций**

**Операторы ОП обязаны:**

- Вести журнал операций и отслеживать подозрительные транзакции (включая операции от 600 000 руб. и операции, связанные с PEP);

- Приостанавливать подозрительные транзакции и уведомлять Росфинмониторинг **в течение 1 рабочего дня с момента их обнаружения**;
- Использовать инструменты анализа блокчейна (например, Chainalysis, Elliptic, MixBytes);
- использовать RBA для анализа транзакций с учетом рисков, связанных с юрисдикциями и активами.

**Платформа:**

- Предоставляет Операторам API для интеграции с системами мониторинга;
- Не участвует в анализе транзакций.

**6.2. Контроль за Операторами ОП**

**Платформа:**

6.2.1. Проверяет Операторов перед Листингом и проводит аудит документального соответствия их внутренних политик AML/CFT требованиям ФЗ-115 и настоящей Политики;

6.2.2. Блокирует Операторов за нарушения AML/CFT, не принимая на себя функции надзорного органа;

6.2.3. Требует от Операторов ОП самостоятельно уведомлять Росфинмониторинг о выявленных нарушениях в установленные законом сроки.

6.2.4. Не осуществляет проверку транзакций, списков террористов/PEP и иные действия, входящие в зону ответственности Операторов ОП.

**6.3. Санкционные юрисдикции**

Платформа:

6.3.1. Блокирует доступ Пользователей и Операторов ОП, находящихся в юрисдикциях, включенных в:

- Перечень ФАТФ («черный» и «серый» списки);
- Санкционные списки РФ (утвержденные Указами Президента РФ и Приказами Минфина);
- Перечни OFAC, ЕС, ООН.

Примеры: Иран, Северная Корея, Сирия.

6.3.2. Автоматически определяет местоположение Пользователей по IP-адресу и данным геолокации;

6.3.3. Немедленно прекращает сотрудничество с Операторами ОП, зарегистрированными в санкционных юрисдикциях.

6.3.4. Механизмы приостановки операций и проверки

При выявлении доступа Пользователя/Оператора ОП из санкционной юрисдикции (Приложение №3):

6.3.4.1. Приостановка операций:

- Все операции Пользователя/Оператора ОП временно приостанавливаются.
- Средства, связанные с подозрительными транзакциями, замораживаются до завершения проверки.

6.3.4.2. Ручная проверка:

В течение 24 часов Ответственное лицо Платформы проводит дополнительную проверку, включая:

- Анализ данных геолокации (IP-адрес, история входов);
- Сверку с актуальными перечнями санкционных юрисдикций (ФАТФ, Минфин РФ);
- Запрос у Оператора ОП подтверждения легитимности операций (при необходимости).

6.3.4.3. Итоги проверки:

Если факт доступа из санкционной юрисдикции подтвержден:

- Аккаунт блокируется на основании ст. 15.3 ФЗ-149 (требование регулятора/решение суда);
- Платформа уведомляет Оператора ОП о необходимости направления отчета в Росфинмониторинг.

Если факт не подтвержден:

- Операции возобновляются, средства размораживаются;
- Пользователь/Оператор ОП получает уведомление о снятии ограничений.

6.3.4.4. Уведомление:

Информация о приостановке/блокировке направляется на email с указанием:

- Оснований (ссылки на перечни ФАТФ/Минфина);
- Порядка обжалования.

**6.4. Высокорисковые активы**

Запрещены к обращению:

6.4.1. Активы с анонимными протоколами (полный список — в Приложении №4);

6.4.2. Токены, эмитенты которых:

- Не опубликовали отчеты о резервах за последние 6 месяцев;
- Не раскрыли данные о руководстве и юрисдикции регистрации.

6.4.2. Операторы ОП обязаны:

- Исключить высокорисковые активы из списка предлагаемых услуг;
- Проводить Enhanced Due Diligence (EDD) для транзакций со стейблкоинами, эмитированными в санкционных юрисдикциях.

Подробный перечень высокорисковых активов приведен в Приложении №4 к Политике.

## 7. ОБРАБОТКА И ЗАЩИТА ДАННЫХ

**7.1. Конфиденциальность:**

- Операторы ОП обязаны хранить данные пользователей в зашифрованном виде и соблюдать ФЗ-152;
- Платформа хранит только данные Операторов ОП (реквизиты, документы), не обрабатывая персональные данные Пользователей, за исключением необходимых для идентификации («минимальные данные»)

**7.2. Срок хранения:**

- Операторы ОП хранят данные 5 лет (согласно ФЗ-115);
- Платформа хранит данные Операторов ОП до прекращения договора.

**7.3. Передача данных:**

- Операторы ОП передают данные уполномоченным органам;
- Платформа передает только информацию о блокировках Операторов (п. 6.2.2. Политики).

## 8. ОБЯЗАННОСТИ ОПЕРАТОРОВ ОП

**8.1. Соблюдение AML/CFT:**

Операторы ОП обязаны:

- Проводить идентификацию и верификацию Пользователей;
- Проверять клиентов на принадлежность к спискам террористов, экстремистов, санкционным спискам и PEP;
- Осуществлять мониторинг транзакций и документировать подозрительные операции;
- Предоставлять Платформе подтверждение соблюдения требований AML/CFT по запросу.

**8.1.1. Проверка списков террористов, экстремистов и санкционных лиц**

Операторы ОП:

(i) Проверяют Пользователей на принадлежность к следующим спискам Росфинмониторинга:

- Перечень лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму (https://www.fedsfm.ru/documents/terr-list);
- Перечень лиц, в отношении которых имеются сведения об их причастности к распространению оружия массового уничтожения (https://www.fedsfm.ru/documents/omu-list-1);
- Список лиц, в отношении которых межведомственной комиссией по противодействию финансированию терроризма приняты решения о применении мер по замораживанию (блокированию) денежных средств или иного имущества.

(ii) При выявлении совпадения:

- Немедленно приостанавливают операции;
- Уведомляют Росфинмониторинг в течение 1 рабочего дня;
- Хранят документацию 5 лет.

Критерии подозрительных операций приведены в Приложении № 1 к Политике.

**8.1.2. Проверка PEP**

Операторы ОП обязаны:

- Использовать аккредитованные базы данных (например, Dow Jones, Refinitiv World-Check) или сервисы, интегрированные с реестрами Росфинмониторинга, для идентификации PEP;
- Проводить усиленную проверку (EDD) в отношении:

(i) Действующих и бывших PEP (включая их близких родственников и доверенных лиц);
(ii) Лиц, связанных с юрисдикциями, включенными в «серые списки» ФАТФ;

- Не использовать офшорные юрисдикции как единственный критерий риска — оценка проводится на основе комплексных данных;
- Фиксировать результаты проверок и предоставлять их Платформе в обезличенной форме для аудита.

**8.1.3. Публикация лицензий:**

Операторы ОП обязаны публиковать ссылки на свои лицензии/разрешения в открытом доступе:

- Для РФ — в реестре операторов обмена цифровых активов Банка России (https://cbr.ru);
- Для иностранных юрисдикций — в реестрах уполномоченных регуляторов (например, FinCEN для США, FCA для Великобритании).

**8.1.4. Уведомление регуляторов**
Операторы ОП обязаны:

- Самостоятельно направлять в Росфинмониторинг и иные уполномоченные органы отчеты о подозрительных операциях в соответствии со ст. 7 ФЗ-115;
- Предоставлять Платформе копии уведомлений, направленных регуляторам, в течение 3 рабочих дней с даты отправки.

**8.2. Обучение сотрудников**

Операторы ОП обязаны:

8.2.1. Проводить обучение сотрудников по вопросам AML/CFT:

- Регулярные тренинги
- Тестирование знаний
- Инструктажи по новым требованиям

8.2.2. Обеспечивать внутренний аудит эффективности мер:

- Регулярные проверки
- Тестирование систем

## 9. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

**9.1. Общие обязательства**

Пользователь обязан:

9.1.1. Информировать Оператора ОП об изменении персональных данных;

9.1.2. Предоставлять достоверную информацию;

9.1.3. Сотрудничать с Оператором ОП при проверках;

9.1.4. Соблюдать запрет на обход санкций:

- не использовать Платформу для обхода санкций, установленных законодательством РФ или международными регуляторами (ФАТФ)

9.1.5. Сообщать о нарушениях:

- незамедлительно информировать Платформу о подозрительных действиях Операторов ОП через форму обратной связи или email: [ссылка]

**9.2. Дополнительная информация**

По запросу Оператора ОП Пользователь обязан предоставить:

- Подтверждение источника средств;
- Документы для верификации — в течение 24–72 часов.

## 10. ОТВЕТСТВЕННОСТЬ ПЛАТФОРМЫ

**10.1. Контроль за Операторами ОП**

Платформа:

- Проводит аудит документации и систем мониторинга Операторов ОП в целях проверки их формального соответствия требованиям законодательства. Данный аудит не гарантирует полного соблюдения Операторами ОП норм AML/CFT и не освобождает их от ответственности за нарушения;
- Не анализирует персональные данные Пользователей.

**10.2. Блокировка нарушителей**

- Платформа блокирует Операторов ОП за нарушения AML/CFT;
- Требует от Оператора ОП направить уведомление в Росфинмониторинг в порядке, предусмотренном ст. 7 ФЗ-115;
- Фиксирует факт нарушения в реестре инцидентов для внутреннего аудита.

**10.3. Сотрудничество с правоохранительными органами и регуляторами**

**10.3.1. Платформа обязуется:**

- Перенаправлять запросы уполномоченных органов РФ (Росфинмониторинг, МВД, Генпрокуратура) и международных регуляторов (ФАТФ, OFAC) в рамках соглашений о взаимной правовой помощи (MLA), ратифицированных РФ, к Операторам ОП, которые непосредственно проводят операции с цифровыми активами;
- Предоставлять регуляторам только обезличенную информацию о блокировках Операторов (наименование, ИНН, дата приостановки).

**10.3.2. Ограничения:**

- Передача персональных данных Пользователей запрещена (ст. 7 152-ФЗ). Исключение — случаи, прямо предусмотренные ФЗ-115 (например, расследование терроризма);
- Платформа не предоставляет регуляторам данные о проверках PEP, проведенных Операторами ОП. Такая информация запрашивается напрямую у Операторов ОП как субъектов, ответственных за проведение KYC/AML.

Данные о транзакциях с запрещенными активами передаются Операторами ОП в Росфинмониторинг в форме, утвержденной Приложением №2.

## 11. САНКЦИИ ЗА НАРУШЕНИЯ

Для Операторов ОП:

**11.1. Предупредительные меры** (за незначительные/первичные нарушения):

- Временное ограничение доступа к расширенным функциям;
- Понижение рейтинга в системе Платформы (если применимо).

**11.2. Ограничительные меры** (за повторные нарушения):

- Временная блокировка аккаунта на срок до 30 дней.

**11.3. Гарантийный депозит как обеспечение обязательств**

**11.3.1. Правовая природа гарантийного депозита**
Гарантийный депозит — денежные средства, внесенные Оператором ОП в качестве обеспечения исполнения обязательств по договору (ст. 329 ГК РФ). Удержание депозита возможно только:

- По решению суда, вступившему в законную силу;
- По письменному соглашению сторон, оформленному дополнительным приложением к договору.

**Примечание:**

- Гарантийный депозит не является штрафом, пеней или иной мерой ответственности.
- Возврат депозита осуществляется в безусловном порядке, за исключением случаев, предусмотренных п. 11.3.2.

**11.3.2. Основания для удержания гарантийного депозита**
Платформа вправе инициировать удержание депозита исключительно при наличии:

- Судебного акта, обязывающего Оператора ОП возместить убытки/нарушения;
- Добровольного согласия Оператора ОП, выраженного в дополнительном соглашении к Договору.

**Удержание недопустимо:**

- В одностороннем порядке на основании внутренних актов Платформы.

**11.3.3. Условия возврата депозита**
Гарантийный депозит подлежит возврату:

- В полном объеме — при отсутствии вступившего в силу судебного решения об удержании;
- В части, не покрытой судебными требованиями — если удержание санкционировано судом.

**Срок возврата:**

- 30 календарных дней с даты прекращения договора или завершения судебного спора.

**11.3.4. Порядок возврата**

- Возврат осуществляется тем же платежным методом, которым депозит был внесен.
- Комиссии за возврат регулируются договором с Оператором ОП.

**11.3.5. Спорные ситуации**

- Споры об удержании/возврате депозита разрешаются в судебном порядке.
- При наличии судебного иска возврат приостанавливается до окончания разбирательства.

**11.4. Окончательные меры** (за систематические/критические нарушения):

- Делистинг;
- Постоянная блокировка аккаунта;
- Включение в черный список.

## 12. СИСТЕМЫ МОНИТОРИНГА

Операторы ОП обязаны:

**12.1. Внедрять инструменты анализа блокчейна**, включая:

- Системы отслеживания транзакций (например, Chainalysis, Elliptic, MixBytes и/или др.);
- Механизмы выявления «грязных» криптоактивов (связанных с незаконными операциями);
- Регулярное обновление баз данных о рискованных адресах/кошельках.

**12.2. Осуществлять специальный мониторинг стейблкоинов,** проверяя:

- Соответствие эмитента критериям Банка России (прозрачность, аудит резервов);
- Отсутствие признаков использования стейблкоинов в схемах обхода AML/CFT-контроля.

**12.3. Организовывать ручной контроль через службу комплаенса**, включающий:

- Проверку подозрительных операций, выявленных автоматическими системами;
- Анализ жалоб пользователей и расследование инцидентов;
- Документирование действий и уведомление Росфинмониторинга при необходимости;
- Оперативное приостановление транзакций с высоким риском.

## 13. УПРАВЛЕНИЕ РИСКАМИ

**13.1. Риски комплаенс**

Операторы ОП управляют рисками, связанными с верификацией пользователей и мониторингом транзакций, включая регулярное тестирование AML/CFT-процедур.

**13.2. Регуляторные риски**

Платформа обновляет Политику в соответствии с изменениями законодательства и проводит внутренние аудиты для оценки соответствия требованиям ФЗ-115, ФЗ-259.

**13.3. Операционные риски**

Операторы ОП предотвращают фиктивные обменные пункты и манипуляции с курсами через EDD и анализ паттернов транзакций.

**13.4. Репутационные риски**

Платформа и Операторы ОП минимизируют использование сервисов для незаконной деятельности и отслеживают негативные упоминания для оперативного реагирования.

## 14. ВЗАИМОДЕЙСТВИЕ С ОПЕРАТОРАМИ ОП

**14.1. Обмен информацией:**

- Операторы ОП обязаны уведомлять Платформу о **фактах** блокировок пользователей в течение 24 часов;
- Платформа запрашивает у Операторов ОП **обезличенные данные** о подозрительных операциях для анализа рисков;
- Передача персональных данных Пользователей запрещена.

**14.2. Технические механизмы:**

- Взаимодействие осуществляется через API и системы электронного документооборота;
- Автоматические уведомления отправляются при операциях, превышающих 600 000 рублей (ст. 6 ФЗ-115).

**14.3. Аудит и проверки:**

- Платформа проводит ежеквартальные аудиты соблюдения Операторами требований AML/CFT;
- При выявлении нарушений инициируется внеплановая проверка.

## 15. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

**15.1. Изменения в Политике:**

Платформа оставляет за собой право вносить изменения в Политику, в том числе при изменении законодательства. Пользователи и Операторы ОП уведомляются об изменениях по email. Изменения вступают в силу через 10 календарных дней после публикации, если иное не требуется для соблюдения законодательства РФ. В исключительных случаях (угроза нарушения законодательства, требования регулятора) изменения могут вступать в силу немедленно.

**15.2. Разрешение споров:**

Споры, возникающие в связи с применением настоящей Политики, разрешаются в судах Российской Федерации.

**15.3. Контактная информация и обратная связь:**

Форма обратной связи на сайте

Электронная почта: [ссылка]

**15.4. ПРИЛОЖЕНИЯ:**

**15.4.1. Приложение №1: Перечень подозрительных операций;**

**15.4.2. Приложение №2: Форма отчета о подозрительных операциях для Операторов ОП;**

**15.4.3. Приложение №3: Санкционные юрисдикции;**

**15.4.4. Приложение №4: Запрещенные высокорисковые активы.**

---

Дата вступления в силу: [дата]

Версия Политики: 1.0

**ПРИЛОЖЕНИЕ №1**

**к Политике AML/CFT платформы Get Crypto**

# ПЕРЕЧЕНЬ ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЙ

**1. Операции, не соответствующие обычной деятельности:**

1.1. Транзакции, существенно отличающиеся по объему от типичных операций пользователя
1.2. Операции с необычными суммами, не соответствующими масштабу деятельности
1.3. Транзакции, не имеющие очевидной экономической цели
1.4. Операции с необоснованной сложностью структуры

**2. Операции с подозрительным происхождением активов:**

2.1. Транзакции с использованием активов, полученных преступным путем("грязных" криптоактивов) (ст. 174, 174.1 УК РФ)

2.2. Операции с кошельками, фигурировавшими на незаконных площадках
2.3. Переводы от лиц, включенных в санкционные списки
2.4. Операции с активами, происхождение которых невозможно установить

**3. Операции с аномальной частотой:**

3.1. Частые мелкие переводы от разных отправителей
3.2. Серии быстрых транзакций между разными кошельками
3.3. Регулярные крупные переводы в течение короткого периода
3.4. Многочисленные операции с короткими интервалами

**4. Операции с признаками уклонения от идентификации:**

4.1. Использование анонимных данных
4.2. Применение псевдонимных адресов
4.3. Предоставление недостоверной информации
4.4. Отказ от верификации при подозрительной активности

**5. Операции с признаками легализации:**

5.1. Транзакции с "мешками" (mixers) или "tumblers"
5.2. Операции с использованием P2P-площадок без надлежащей верификации
5.3. Переводы на счета, связанные с незаконными товарами
5.4. Транзакции с офшорными зонами, включенными в перечни Росфинмониторинга

**6. Операции с признаками финансирования терроризма:**

6.1. Транзакции с лицами из перечней террористов (перечни Росфинмониторинга)
6.2. Переводы на счета экстремистских организаций
6.3. Операции с территориями, признанными зонами деятельности террористических группировок
6.4. Транзакции с известными финотделениями террористов

**7. Операции с признаками мошенничества:**

7.1. Транзакции с использованием подставных лиц
7.2. Операции с похищенными криптоактивами
7.3. Переводы в рамках схем Ponzi
7.4. Транзакции с фишинговых сайтов

**8. Операции с признаками нарушения законодательства:**
8.1. Транзакции с запрещенными товарами
8.2. Переводы для финансирования незаконной деятельности
8.3. Операции с нарушением санкционных ограничений
8.4. Транзакции с целью уклонения от налогов

**9. Операции с запрещенными юрисдикциями и высокорисковыми активами:**

9.1. Транзакции с пользователями/кошельками из санкционных юрисдикций. Списки санкционных юрисдикций приведены на официальных сайтах Минфина РФ https://minfin.gov.ru/ и ФАТФ https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

9.2. Использование высокорисковых активов (Monero, Zcash, Dash) без проведения EDD;
9.3. Переводы через миксеры/тумблеры в запрещенные юрисдикции.

***Примечание:***

*Территории, связанные с террористическими группировками, определяются на основании актуальных перечней Росфинмониторинга и Постановлений Правительства РФ.*

*Офшорные зоны идентифицируются в соответствии с перечнями, опубликованными Росфинмониторингом и ФАТФ.*

*Актуальные перечни санкционных юрисдикций и высокорисковых активов приведены в Приложениях №3 и №4.*

*Данный перечень не является исчерпывающим. Все выявленные подозрительные операции должны быть немедленно зафиксированы и проанализированы в соответствии с установленными процедурами.*

**ПРИЛОЖЕНИЕ №2**

**к Политике AML/CFT платформы Get Crypto**

**ФОРМА ОТЧЕТА О ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЯХ ДЛЯ ОПЕРАТОРОВ ОБМЕННЫХ ПУНКТОВ**

# ОТЧЕТ О ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЯХ

**1. Общие сведения об операции**

1.1. Признак подозрительной операции:

☐ Несоответствие операции целям деятельности

☐ Аномальный характер операции

☐ Необоснованная сложность структуры операции

☐ Отсутствие экономического смысла

☐ Иной признак (указать):

1.2. Дата совершения операции:

1.3. Дата выявления подозрительной операции:

1.4. Код вида операции:

1.5. Код признака необычной операции:

1.6. Идентификатор подозрительной деятельности:

1.7. Сумма операции:

**2. Специфические сведения о цифровой валюте**

2.1. Тип стейблкоина:

☐ USDT (Tether)

☐ USDC (USD Coin)

☐ BUSD (Binance USD)

☐ TUSD (TrueUSD)

☐ GUSD (Gemini Dollar)

☐ EURST (Euro Tether)

☐ Иной (указать)

2.1.1. Высокорисковые активы:

☐ Monero (XMR)

☐ Zcash (ZEC)

☐ Dash (DASH)

☐ Иные токены без аудита эмитента (указать название):

2.2. Адрес кошелька отправителя:

- Криптовалютная сеть:
- Адрес кошелька:

2.3. Адрес кошелька получателя:

- Криптовалютная сеть:
- Адрес кошелька:

2.4. Txid транзакции:

2.5. Количество задействованных кошельков:

2.6. Связанные транзакции (если применимо):

- Txid предыдущей транзакции:
- Txid последующей транзакции:

**3. Сведения об участниках операции**

3.1. Отправитель средств:

- ФИО/Название организации
- Страна регистрации/проживания
- Идентификационный номер/ИНН
- Контактные данные

**3.2. Получатель средств:**

- ФИО/Название организации
- Страна регистрации/проживания
- Идентификационный номер/ИНН
- Контактные данные

**3.3. Бенефициарный владелец (если применимо):**

- ФИО/Название организации
- Страна регистрации/проживания
- Идентификационный номер/ИНН
- Контактные данные

**4. Описание подозрительной операции**

4.1. Краткое описание сути операции:

4.2. Причины, по которым операция считается подозрительной:

**5. Документы по операции**

5.1. Приложить копии:

- Документов, подтверждающих личность участников
- Документов, связанных с операцией
- Иных релевантных документов

**6. Заключение**

6.1. Предполагаемая сумма легализации:

6.2. Предполагаемая стадия легализации:

☐ Размещение

☐ Расслоение

☐ Интеграция

Дата составления отчета:

Должность:

ФИО:

Подпись:

*Примечание: Оператор ОП обязан самостоятельно направить отчет в Росфинмониторинг в сроки, установленные ст. 7 ФЗ-115.*

**ПРИЛОЖЕНИЕ №3**

**к Политике AML/CFT платформы Get Crypto**

# САНКЦИОННЫЕ ЮРИСДИКЦИИ

**1. Ссылки на официальные перечни:**

Перечень Минфина РФ, доступный по ссылке на официальном сайте Минфина РФ: https://minfin.gov.ru/

Черный и серый списки ФАТФ, доступный по ссылке на официальном сайте: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

Санкционные списки ЕС, доступные по ссылке: https://www.sanctionsmap.eu/#/main

Списки OFAC, доступные по ссылке: https://ofac.treasury.gov/

**2. Примеры стран:**

Иран, Северная Корея, Сирия, Мьянма.

**3. Порядок обновления:**

Списки актуализируются ежеквартально. Ответственное лицо по AML/CFT обязано проверять изменения.

**ПРИЛОЖЕНИЕ №4**

**к Политике AML/CFT платформы Get Crypto**

# ЗАПРЕЩЕННЫЕ ВЫСОКОРИСКОВЫЕ АКТИВЫ

**1. Криптовалюты с повышенной анонимностью:**

- Monero (XMR);
- Zcash (ZEC);
- Dash (DASH);
- Grin (GRIN);
- Beam (BEAM).

**2. Токены без аудита эмитента:**

- Примеры: токены, выпущенные анонимными командами;
- Токены без аудита резервов запрещены, только если аудит не проведен за последние 6 месяцев

**3. Порядок идентификации:**

- Использование инструментов Chainalysis, Crystal Blockchain и/или других;
- Ежемесячная сверка с реестром Банка России.