

Политика AML/KYC

Настоящая Политика AML/KYC («Политика») описывает подход F-Tech, зарегистрированной в Kazakhstan («Компания», «мы», «нас», «наш»), к предотвращению отмывания доходов, финансирования терроризма, обхода санкций, мошенничества и иной незаконной или запрещённой деятельности при использовании сайта <https://kashbi.io>, приложения KashBi, Telegram-бота, Telegram Mini App, web-версии, API, крипто-фиатного кошелька, P2P-платформы и иных связанных сервисов Компании, совместно именуемых «Платформа».

Настоящая Политика является частью Пользовательского соглашения и применяется совместно с Политикой конфиденциальности, правилами P2P-сделок, правилами комиссий, предупреждениями о рисках и иными документами Компании.

Используя Платформу, создавая аккаунт, пополняя баланс, выводя цифровые активы, создавая или принимая P2P-сделку, проходя проверку или иным образом взаимодействуя с Платформой, пользователь подтверждает, что ознакомился с настоящей Политикой и соглашается соблюдать её положения.

Если пользователь не согласен с настоящей Политикой, он должен прекратить использование Платформы.

1. Цель и сфера применения

1.1. Цель Политики

Цель настоящей Политики — установить основные принципы, правила и меры, направленные на:

- предотвращение использования Платформы для отмывания доходов;
- предотвращение финансирования терроризма;
- предотвращение обхода санкций;
- предотвращение мошенничества, скама, фишинга и иной противоправной деятельности;
- выявление и оценку высокорисковых пользователей, операций, адресов и юрисдикций;
- мониторинг операций с цифровыми активами и P2P-сделок;
- выполнение применимых требований законодательства, требований партнёров, поставщиков AML/KYC-сервисов, банков, платёжных провайдеров и компетентных органов;
- защиту пользователей, Компании, Платформы и её деловой репутации.

1.2. Сфера применения

Настоящая Политика применяется ко всем пользователям Платформы, включая пользователей:

- крипто-фиатного кошелька;

- P2P-платформы;
- Telegram Mini App;
- Telegram-бота;
- web-версии;
- функций пополнения и вывода цифровых активов;
- внутренних переводов;
- фиатных операций вне P2P, если такие функции доступны;
- службы поддержки и споров.

1.3. Risk-based подход

Компания применяет риск-ориентированный подход. Это означает, что KYC, AML-проверки, лимиты, запросы документов, усиленная проверка, мониторинг, ограничения и иные меры применяются соразмерно уровню риска пользователя, операции, юрисдикции, платёжного метода, цифрового актива, блокчейн-адреса, поведения пользователя и иных факторов.

Платформа позиционируется как *privacy-first*: Компания стремится минимизировать сбор персональных данных и не запрашивать идентификационные документы без необходимости. При этом *privacy-first* не означает полную анонимность и не исключает обработку данных, проверку пользователя, проверку транзакций, ограничение операций или передачу информации компетентным органам, если это требуется или допускается законом, правилами Платформы, требованиями партнёров или настоящей Политикой.

2. Термины и определения

2.1. AML

AML — меры по противодействию отмыванию доходов, полученных преступным путём, включая выявление, предотвращение, расследование и ограничение операций, связанных с незаконным происхождением средств.

2.2. KYC

KYC — процедура «знай своего клиента», включающая идентификацию, проверку и оценку пользователя, если такая процедура требуется с учётом риска, лимитов, операции, применимого законодательства или требований партнёров.

2.3. CDD

CDD — надлежащая проверка клиента, включающая сбор и анализ информации о пользователе, его активности, источнике средств, целях операций и профиле риска.

2.4. EDD

EDD — усиленная проверка клиента, применяемая к пользователям, операциям или ситуациям повышенного риска. EDD может включать запрос дополнительных документов, подтверждение источника средств, расширенный анализ транзакций, проверку открытых источников, санкционные и PEP-проверки, а также согласование дальнейшего обслуживания на уровне ответственных лиц Компании.

2.5. KYT

KYT — процедура «знай свою транзакцию», включающая анализ операций, блокчейн-адресов, источников средств, поведения пользователя, связанных кошельков, P2P-паттернов и иных данных, относящихся к конкретной операции.

2.6. PEP

PEP — политически значимое лицо, а также члены его семьи и лица, тесно связанные с таким лицом, если такие лица требуют повышенного внимания с точки зрения коррупционных, санкционных, репутационных или иных рисков.

2.7. Санкции

Санкции — экономические, финансовые, торговые, персональные, территориальные или иные ограничительные меры, установленные государствами, международными организациями, компетентными органами или применимые через партнёров Компании.

2.8. Запрещённая юрисдикция

Запрещённая юрисдикция — страна, территория или регион, в отношении которых Компания ограничивает или запрещает обслуживание по причине закона, санкций, высокого AML-риска, требований партнёров, внутренних правил управления рисками или иных обстоятельств.

Перечень запрещённых юрисдикций не обязательно публикуется в настоящей Политике и может определяться в интерфейсе Платформы, внутренних правилах Компании, документах партнёров или отдельных уведомлениях.

2.9. Подозрительная активность

Подозрительная активность — операция, поведение, источник средств, P2P-сделка, адрес, платёжный метод, аккаунт или иной фактор, который может указывать на отмыwanie доходов, финансирование терроризма, обход санкций, мошенничество, скам, использование чужих данных, мультиаккаунтинг, незаконную деятельность или иной неприемлемый риск.

2.10. Red flags / красные флаги

Red flags — признаки или индикаторы, которые могут указывать на повышенный риск или необходимость дополнительной проверки.

3. Организация AML/KYC-контроля

3.1. Ответственные лица

Компания может назначать ответственное лицо или команду, отвечающую за реализацию AML/KYC-процедур, управление рисками, мониторинг транзакций, рассмотрение подозрительной активности, взаимодействие с компетентными органами и поддержание внутренних правил.

3.2. Внутренние правила

Компания разрабатывает и применяет внутренние правила, инструкции, критерии риска, red flags, процедуры проверки, лимиты, сценарии мониторинга и правила принятия решений.

Такие внутренние документы являются конфиденциальной информацией Компании и не подлежат раскрытию пользователям, если раскрытие может повредить эффективности контроля, безопасности Платформы, исполнению закона, правам третьих лиц или интересам расследования.

3.3. Обновление процедур

Компания может обновлять AML/KYC-процедуры с учётом:

- изменений законодательства;
- новых продуктов и функций;
- новых схем мошенничества;
- рекомендаций FATF и иных международных стандартов;
- требований партнёров;
- результатов внутренних проверок;
- инцидентов безопасности;
- изменений санкционных режимов;
- новых типологий отмывания доходов и финансирования терроризма.

4. Оценка рисков

4.1. Общая оценка рисков

Компания может проводить регулярную оценку AML/KYC-рисков, связанных с Платформой, пользователями, продуктами, цифровыми активами, юрисдикциями, каналами доступа, P2P-сделками, платёжными методами, фиатными операциями вне P2P, блокчейн-сетями и поставщиками услуг.

4.2. Факторы риска

При оценке риска Компания может учитывать:

- страну проживания, гражданство, местоположение или IP-географию пользователя;
- тип аккаунта и способ регистрации;
- историю операций;
- суммы и частоту операций;
- используемые цифровые активы и сети;
- блокчейн-адреса отправителей и получателей;
- связь адресов с миксерами, даркнет-рынками, взломами, ransomware, скам-проектами, санкционными адресами или иными высокорисковыми источниками;
- использование P2P-сделок;
- выбранные фиатные платёжные методы;
- поведение в спорах;
- жалобы других пользователей;
- мультиаккаунтинг или связь с ранее заблокированными аккаунтами;
- использование VPN, прокси или иных средств сокрытия местоположения;

- отказ от предоставления информации;
- противоречивость данных;
- PEP-статус;
- санкционные совпадения;
- adverse media и иные репутационные факторы;
- требования партнёров и компетентных органов.

4.3. Категории риска

Компания может присваивать пользователям, операциям, адресам или сделкам внутренние категории риска, например низкий, средний, высокий или неприемлемый риск.

Категория риска может влиять на:

- доступные функции;
- лимиты;
- необходимость KYC;
- необходимость EDD;
- скорость обработки операций;
- возможность вывода;
- доступ к P2P;
- необходимость ручной проверки;
- вероятность заморозки или отказа в обслуживании.

Компания не обязана раскрывать пользователю внутреннюю категорию риска, методику расчёта, точные критерии или результаты скоринга.

5. KYC/CDD: проверка пользователей

5.1. Общий подход

Компания не требует полной KYC-верификации от всех пользователей по умолчанию, если иное не предусмотрено законом, интерфейсом, требованиями партнёров или конкретной функцией. Проверка применяется на риск-ориентированной основе.

5.2. Когда может потребоваться KYC

Компания может запросить KYC или дополнительные сведения в следующих случаях:

- достижение лимитов;
- крупная операция;
- необычная операция;
- подозрительная активность;
- открытие спора;
- запрос на вывод;
- AML-совпадение по адресу или транзакции;

- связь с высокорисковой юрисдикцией;
- использование фиатной функции вне P2P;
- требование платёжного партнёра, банка, обменного провайдера или AML/KYC-провайдера;
- запрос компетентного органа;
- восстановление доступа к аккаунту;
- подозрение на мультиаккаунтинг, мошенничество или использование чужих данных;
- иные обстоятельства, требующие проверки.

5.3. Какие данные могут запрашиваться

В зависимости от уровня риска Компания может запросить:

- имя, фамилию, отчество или иное полное имя;
- дату рождения;
- гражданство;
- страну проживания;
- адрес проживания;
- email;
- номер телефона;
- документ, удостоверяющий личность;
- фотографию, селфи, видео-проверку или liveness-проверку;
- подтверждение адреса;
- подтверждение источника средств;
- подтверждение источника благосостояния;
- подтверждение цели операции;
- выписку, чек, квитанцию или подтверждение платежа;
- документы по P2P-сделке;
- сведения о связи с PEP;
- иные документы или пояснения, необходимые для оценки риска.

5.4. Проверка данных

Компания может проверять предоставленные данные:

- вручную;
- с использованием автоматизированных систем;
- через внешних AML/KYC-провайдеров;
- через санкционные и PEP-списки;
- через открытые источники;
- через блокчейн-аналитику;
- через информацию, полученную от партнёров, пользователей, банков, платёжных провайдеров или компетентных органов.

5.5. Обязанность пользователя сотрудничать

Пользователь обязан своевременно, достоверно и полно предоставлять запрошенную информацию и документы.

Если пользователь отказывается предоставить данные, предоставляет ложные или противоречивые сведения, не отвечает на запросы или пытается обойти проверку, Компания вправе ограничить функции, приостановить операции, заморозить активы, отменить сделки, отказать в обслуживании или закрыть аккаунт.

5.6. Повторная проверка

Компания вправе повторно запросить документы или сведения, даже если пользователь ранее уже проходил проверку, если:

- изменились данные пользователя;
- истёк срок действия документа;
- изменилась активность пользователя;
- появились новые риски;
- пользователь достиг новых лимитов;
- открылась новая функция;
- изменились требования закона или партнёров;
- возник спор или подозрительная активность.

6. Усиленная проверка EDD

6.1. Когда применяется EDD

Компания может применить EDD, если пользователь, операция, адрес, P2P-сделка, юрисдикция или поведение имеет повышенный риск.

EDD может применяться, в частности, если:

- пользователь является PEP или связан с PEP;
- пользователь связан с высокорисковой юрисдикцией;
- операция является крупной, сложной, необычной или экономически необъяснимой;
- средства поступают с высокорискового блокчейн-адреса;
- операция связана с миксерами, даркнет-рынками, взломами, ransomware, скамом, санкционными адресами или иными красными флагами;
- пользователь часто открывает или проигрывает споры;
- есть признаки мультиаккаунтинга;
- есть признаки использования чужих реквизитов или чужого аккаунта;
- пользователь не может объяснить источник средств;
- пользователь противоречиво отвечает на вопросы;
- требуется подтверждение по запросу партнёра или компетентного органа.

6.2. Меры EDD

EDD может включать:

- запрос дополнительных документов;
- подтверждение источника средств;
- подтверждение источника благосостояния;
- подтверждение цели операции;
- проверку открытых источников;
- проверку adverse media;
- углублённый анализ блокчейн-истории;
- снижение лимитов;
- временную заморозку средств;
- ручное согласование операции;
- отказ в операции;
- прекращение обслуживания.

6.3. Результаты EDD

По результатам EDD Компания может:

- разрешить операцию;
- разрешить операцию с лимитами или условиями;
- запросить дополнительные сведения;
- отказать в операции;
- вернуть средства, если это допустимо и возможно;
- заморозить средства;
- ограничить аккаунт;
- закрыть аккаунт;
- передать информацию компетентным органам, если это требуется или допускается законом.

7. КУТ и мониторинг транзакций

7.1. Общий мониторинг

Компания может осуществлять постоянный или выборочный мониторинг операций пользователей, включая:

- пополнения цифровыми активами;
- выводы цифровых активов;
- внутренние переводы;
- P2P-сделки;
- фиатные операции вне P2P, если такие функции доступны;
- попытки операций;
- отменённые операции;

- операции, связанные со спорами или жалобами.

7.2. Блокчейн-аналитика

Компания может использовать блокчейн-аналитику для оценки риска адресов, транзакций, кластеров адресов, источников средств и связанных сущностей.

Проверка может учитывать связь с:

- санкционными адресами;
- даркнет-рынками;
- миксерами и сервисами обфускации;
- ransomware;
- взломами и украденными средствами;
- скам-проектами;
- мошенническими схемами;
- незаконными сервисами;
- высокорисковыми биржами или обменниками;
- иными источниками повышенного риска.

7.3. P2P-мониторинг

В P2P-сделках Компания может анализировать:

- частоту сделок;
- суммы сделок;
- поведение сторон;
- количество отмен;
- количество споров;
- жалобы;
- подтверждения оплаты;
- совпадения реквизитов;
- связь аккаунтов;
- признаки мультиаккаунтинга;
- несоответствие платёжных данных;
- попытки вывода сделки вне правил Платформы;
- использование чужих банковских счетов, карт или платёжных реквизитов.

7.4. Лимиты и задержки

Компания может устанавливать лимиты, задержки, ручные проверки или дополнительные требования для отдельных пользователей, операций, сделок, адресов, активов, платёжных методов или юрисдикций.

Операция может быть задержана или приостановлена до завершения проверки.

8. Red flags: признаки подозрительной активности

К red flags могут относиться, в частности:

- отказ пользователя предоставить данные или документы;
- предоставление поддельных, изменённых или противоречивых документов;
- использование чужих данных, чужих карт, чужих счетов или чужих кошельков;
- попытка использовать несколько аккаунтов;
- частые отмены P2P-сделок;
- частые споры по P2P-сделкам;
- поддельные чеки, квитанции или скриншоты оплаты;
- несоответствие имени плательщика и пользователя;
- быстрый ввод и вывод средств без очевидной экономической цели;
- структурирование операций на несколько мелких сумм;
- операции, не соответствующие обычному поведению пользователя;
- использование высокорисковых блокчейн-адресов;
- связь с миксерами, даркнет-рынками, взломами, ransomware, скамом или санкционными адресами;
- резкий рост оборота;
- попытки обойти лимиты;
- использование VPN, прокси или иных средств сокрытия местоположения для обхода ограничений;
- агрессивное давление на контрагента или поддержку;
- отказ объяснить источник средств;
- попытка вывести сделку за пределы Платформы;
- жалобы от других пользователей;
- негативная информация из открытых источников;
- совпадение с санкционными, PEP или adverse media-источниками.

Наличие одного red flag не всегда означает нарушение, но может стать основанием для дополнительной проверки, ограничения операции или иных мер.

9. Санкции и запрещённые отношения

Компания не устанавливает и не продолжает отношения с пользователями, если это запрещено законом, санкциями, требованиями партнёров или внутренними правилами управления рисками.

Компания может отказать в обслуживании, ограничить аккаунт, заморозить активы или прекратить отношения, если пользователь:

- находится в санкционном списке;
- связан с лицом из санкционного списка;
- находится в запрещённой юрисдикции;
- действует в интересах запрещённого лица;

- использует Платформу для обхода санкций;
- отказывается предоставить информацию, необходимую для санкционной проверки.

Компания может проводить санкционные проверки при регистрации, перед операцией, после операции, при изменении санкционных списков, при открытии спора, при выводе средств или в иных случаях.

10. Запрещённая деятельность

Пользователю запрещено использовать Платформу для:

- отмыwania доходов;
- финансирования терроризма;
- обхода санкций;
- мошенничества, скама, фишинга или социальной инженерии;
- торговли украденными средствами, аккаунтами, картами, документами или персональными данными;
- использования чужих банковских карт, счетов, кошельков или реквизитов без законного основания;
- незаконного оборота наркотиков, оружия, опасных веществ или иных запрещённых товаров;
- незаконных азартных игр;
- нелегальных финансовых услуг;
- даркнет-активности;
- финансирования экстремистской, террористической или иной запрещённой деятельности;
- нарушения прав третьих лиц;
- использования поддельных документов, чеков, квитанций или скриншотов;
- мультиаккаунтинга и обхода ограничений;
- иной деятельности, которую Компания считает незаконной, высокорисковой или неприемлемой.

11. Меры Компании при выявлении риска

Если Компания выявляет подозрительную активность, AML/KYC-риск, санкционный риск, нарушение настоящей Политики или отказ пользователя сотрудничать, Компания вправе:

- запросить дополнительные сведения;
- запросить KYC или EDD;
- снизить лимиты;
- задержать операцию;
- отказать в операции;
- отменить P2P-сделку;

- ограничить P2P-функции;
- заморозить или зарезервировать активы;
- ограничить вывод;
- временно заблокировать аккаунт;
- закрыть аккаунт;
- вернуть средства отправителю, если это возможно, допустимо и не запрещено законом;
- удержать применимые комиссии, сетевые расходы или расходы на возврат, если это предусмотрено правилами Платформы;
- передать информацию компетентным органам, если это требуется или допускается законом;
- предпринять иные разумные меры для защиты Платформы, пользователей, партнёров и Компании.

Компания не обязана заранее уведомлять пользователя о применении таких мер, если уведомление может нарушить закон, требования AML/KYC/CTF, санкционные правила, интересы расследования, безопасность Платформы или права третьих лиц.

12. Возврат средств при AML/KYC-отказе

Если операция отклонена или обслуживание ограничено по результатам AML/KYC-проверки, Компания может, если это возможно и допустимо, вернуть цифровые активы на исходный адрес отправителя или иной адрес, который Компания сочтёт допустимым с точки зрения риска и закона.

Возврат может быть невозможен или отложен, если:

- средства связаны с санкционным адресом;
- средства связаны с преступной активностью;
- получен запрос компетентного органа;
- возврат может нарушить закон;
- исходный адрес недоступен, высокорисковый или технически непригоден;
- требуется дополнительная проверка;
- средства уже зарезервированы, заморожены или связаны со спором.

С суммы возврата могут удерживаться сетевые комиссии, сервисные комиссии, расходы на обработку и иные применимые расходы, если они предусмотрены Пользовательским соглашением, страницей комиссий <https://kashbi.io/information/fees>, интерфейсом Платформы или отдельными правилами.

Конкретный размер комиссии или сбора за такой возврат не фиксируется в настоящей Политике и может определяться страницей комиссий <https://kashbi.io/information/fees>, интерфейсом Платформы или отдельными правилами, если такой сбор применяется.

13. Отчётность и взаимодействие с органами

Компания может взаимодействовать с компетентными органами, подразделениями финансовой разведки, правоохрательными органами, судами, регуляторами, банками, платёжными провайдерами и иными уполномоченными лицами, если это требуется или допускается законом.

Компания может передавать информацию о пользователе, аккаунте, транзакции, P2P-сделке, споре, адресе, платёжных данных или иных обстоятельствах, если:

- получен законный запрос;
- есть обязанность сообщить о подозрительной активности;
- требуется исполнить санкционные требования;
- необходимо защитить права Компании, пользователей или третьих лиц;
- требуется предотвращение мошенничества, отмывания доходов или финансирования терроризма.

Компания не обязана уведомлять пользователя о такой передаче, если уведомление запрещено законом, может помешать расследованию, раскрыть внутренние AML-процедуры или создать риск для безопасности.

14. Хранение данных и записей

Компания хранит данные и записи, связанные с AML/KYC, транзакциями, P2P-сделками, проверками, спорами, ограничениями и отчётностью, в течение срока, предусмотренного применимым законодательством, требованиями партнёров, внутренними правилами управления рисками и Политикой конфиденциальности.

К таким данным могут относиться:

- KYC-данные;
- документы пользователя;
- результаты проверок;
- санкционные и PEP-совпадения;
- риск-профиль;
- история операций;
- блокчейн-адреса;
- txid/hash транзакций;
- данные P2P-сделок;
- подтверждения оплаты;
- материалы споров;
- переписка с поддержкой;
- внутренние решения по ограничениям;
- записи о запросах компетентных органов.

Удаление аккаунта, отзыв согласия или прекращение использования Платформы не всегда означает немедленное удаление AML/KYC-данных, если их хранение

требуется или допускается законом, правилами AML/KYC/CTF, защитой прав Компании, разрешением споров или исполнением запросов компетентных органов.

15. Третьи лица и поставщики услуг

Компания может привлекать третьих лиц для выполнения AML/KYC-процедур, включая:

- поставщиков проверки документов;
- поставщиков liveness-проверки;
- поставщиков санкционного скрининга;
- поставщиков PEP/adverse media-проверки;
- поставщиков блокчейн-аналитики;
- платёжных партнёров;
- банков, процессинги и обменных провайдеров;
- юридических, комплаенс- и аудиторских консультантов;
- поставщиков инфраструктуры и безопасности.

Провайдеры могут быть указаны категориями без конкретных названий, если иное не требуется законом, договором с провайдером или отдельной политикой Компании.

Компания может проверять партнёров и поставщиков на предмет санкций, репутации, лицензий, разрешений, рисков и способности соблюдать требования безопасности и конфиденциальности.

16. Обязанности пользователя

Пользователь обязуется:

- не использовать Платформу для запрещённой деятельности;
- предоставлять достоверные сведения;
- своевременно отвечать на запросы Компании;
- предоставлять документы и пояснения, если они запрошены;
- использовать только законно принадлежащие ему средства;
- не использовать чужие банковские карты, счета, кошельки или реквизиты без законного основания;
- не предоставлять поддельные документы, чеки, скриншоты или квитанции;
- не обходить лимиты, проверки, санкционные ограничения или правила Платформы;
- не создавать несколько аккаунтов для обхода ограничений;
- соблюдать применимое законодательство;
- самостоятельно оценивать законность своих операций в стране проживания.

Отказ от сотрудничества, уклонение от проверки, предоставление ложных сведений или попытка обойти AML/KYC-контроль может привести к ограничению или прекращению обслуживания.

17. Конфиденциальность AML/KYC-процедур

Пользователь понимает, что Компания не раскрывает:

- точные критерии риска;
- внутренние red flags;
- пороги мониторинга;
- алгоритмы скоринга;
- источники AML-данных;
- детали расследования;
- причины подачи отчёта компетентным органам;
- детали внутренних решений;
- информацию, раскрытие которой может нарушить закон, безопасность или эффективность AML/KYC-контроля.

18. Изменение Политики

Компания вправе изменять настоящую Политику в любое время. Актуальная версия публикуется на сайте <https://kashbi.io> или в интерфейсе Платформы.

Продолжение использования Платформы после публикации обновлённой версии означает согласие пользователя с новой редакцией Политики, если иное не предусмотрено применимым законодательством.

19. Языковые версии

Настоящая Политика может быть опубликована на русском, казахском, английском и иных языках.

Если применимое законодательство требует приоритета определённой языковой версии, применяется такая версия. В остальных случаях при расхождениях между языковыми версиями приоритет имеет версия на русском языке.

20. Контакты

По вопросам настоящей Политики пользователь может обратиться:

- Компания: F-Tech
- Страна регистрации: Kazakhstan
- Сайт: <https://kashbi.io>
- Приложение: KashBi
- Email: legal@kashbi.io
- Telegram: [kashbi_support](https://t.me/kashbi_support)
- Юридический адрес: 44/1 Al-Farabi Avenue, Apartment 207