Структура нового формата AML (Compliance) рекомендации для клиентов компании Bestchange.

Глава 1. *Введение*

1. **Понятие AML и его роль в криптовалютной индустрии**

— Определение AML.

AML (Anti-Money Laundering, или борьба с отмыванием денег) процедуры, представляющие собой комплекс мер и действий, направленных на предотвращение и обнаружение незаконных финансовых операций, связанных с отмыванием денег и финансированием терроризма.

Данные процедуры вводятся внутри компании в соответствии с законодательством страны осуществления деятельности, законодательством стран, гражданами которых являются клиенты, а также в соответствии с общепринятыми нормами FATF, а также требованиями OFAC и иными контролирующими органами государственной власти разных стран. Наличие документации, закрепляющей данные нормы, а также их реальное практическое применение являются одним из обязательных аспектов используемым при соблюдении compliance.

— Специфика AML в контексте криптовалют.

Специфика AML в сфере криптовалют заключается в том, что первоначально криптовалютная сфера заявлялась как независимая от государственного влияния; сфера свободная от любых норм идентификации.

В итоге биржи, обменники и иные средства приема криптовалют на баланс не отражали информацию, касающуюся источника средств, владельца активов, перевода и иной информации в рамках осуществляемой сделки. Этот нюанс сделал AML крайне необходимой частью процесса в целях проверки транзакций и пополнений.

Иными словами, обещанное первоначально отсутствие регулирования привело к яркой необходимости в создании и применении вышеперечисленных норм. В иных сферах (например, банковской), эти нормы давно уже нашли свое место и применение в рамках внедрения процедур, выводящих транзакции на безопасный уровень для глобальной системы.

В итоге AML в криптовалютном контексте требует разработки и внедрения новых технологий, регулирующих стандартов и методов мониторинга. Эффективная борьба с отмыванием денег в сфере криптовалют должна сочетать в себе инновации в области аналитики данных, международное сотрудничество и развитие регуляторной базы, которая сможет справиться с быстро меняющимися технологиями и методами, используемыми преступниками. Ведь привычная децентрализация, анонимность, отсутствие регулирования и свободное международное движение теперь отходят на второй план, так как были изменены и помечены государством, как требующие регулирования.

— Методы предотвращения отмывания денег в криптоиндустрии.

Методы предотвращения отмывания денег (AML) в криптоиндустрии развиваются с учетом особенностей работы блокчейна и криптовалют. Ключевые подходы включают как технологические решения, так и организационные меры, направленные на соблюдение нормативных требований. Рассмотрим основные методы и подходы:

1) Процедуры KYC (Знай своего клиента)

Важным инструментом для предотвращения отмывания денег является внедрение политики **KYC (Know Your Customer)**, которая включает сбор и верификацию данных о клиентах криптовалютных платформ.

Основные этапы KYC:

- **Идентификация клиента**: Платформы требуют предоставления документов, удостоверяющих личность (паспорт, водительское удостоверение и иные).
- **Проверка адреса**: Зачастую требуется подтверждение места жительства клиента по методу предоставления счета за коммунальные услуги или другие документы.
- **Оценка риска**: Платформы могут использовать различные инструменты для оценки уровня риска, связанного с клиентом, включая проверку по международным спискам санкций и черным спискам.
- **Общая проверка клиента**. Такая проверка может включать в себя анализ общедоступных списков тех, кто может быть задействован в незаконной деятельности или деятельности связанный с политическим полем (PEP), проверка источника средств клиента, если объём его активов кажется подозрительным для его бэкграунда (например, слишком большой объём транзакции; потенциально незаконное происхождение средств; санкционные средства и иные варианты)).

Этот процесс позволяет криптовалютным компаниям отслеживать и идентифицировать пользователей, представляющих опасность, что снижает для компании риски, связанные с анонимностью транзакций, а также предоставляет платформам плацдарм действий в случае получения запросов от государственных органов, а также от иных субъектов, имеющих полномочия на уточнение информации, получаемой от клиентов и из иных источников, для снятия подозрений в сфере совершения осознанных противоправных действий.

2) Мониторинг и анализ транзакций

Для выявления подозрительных операций также важно отслеживать поведение пользователей на платформе и анализировать криптовалютные транзакции в реальном времени.

Основные инструменты и методы мониторинга:

- **Системы мониторинга транзакций (Transaction Monitoring Systems, TMS)**: Эти системы анализируют все транзакции в сети и выявляют те, которые могут быть связаны с отмыванием денег. Они помогают идентифицировать необычные паттерны, такие как частые переводы больших сумм в краткие сроки или стабильное взаимодействие с высокорисковыми странами.
    - **Программное обеспечение для аналитики блокчейн (например, Chainalysis, Crystal, Elliptic и иные)**: Эти инструменты позволяют отслеживать источники и конечные адреса криптовалютных транзакций, анализировать связи между адресами и выявлять подозрительные

    операции, такие как использование миксеров или анонимных криптовалют.

3) Соблюдение нормативных требований (комплаенс)

Комплаенс-службы (Compliance) криптовалютных компаний обязаны следить за соблюдением местных и международных норм и стандартов AML, которые включают в себя:

- Применение международных рекомендаций и стандартов, таких как требования **ФАТФ** (Финансовая группа борьбы с отмыванием денег) и внутригосударственных требований.
- Регистрация в качестве **представителей финансовых учреждений** в странах с жестким законодательством (например, в ЕС ил иных странах с официальным регулированием, где криптовалютные платформы обязаны соблюдать законы о борьбе с отмыванием денег, как и традиционные финансовые институты).
- Создание внутренних процедур для обработки подозрительных операций, включая обязательное уведомление компетентных органов

(например, **FinCEN** в США, **Нацбанк** в Грузии или **FATF** на международном уровне).

4) Механизмы блокировки подозрительных адресов

Многие криптовалютные платформы и кошельки используют механизмы блокировки транзакций с адресами, связанными с незаконной деятельностью, такими как адреса, которые были занесены в черные списки, используются для финансирования терроризма или провели большое количество транзакций с активами, которые обозначены в качестве высокорисковых.

Платформы выбирают методы регулировки и блокировки аккаунтов, которые были замечены в осуществлении деятельности, обозначенной выше на основании собственных убеждений, а также международного и локального законодательства, в зависимости от юрисдикции получения лицензии.

Адреса, который показались платформе подозрительными могут быть заблокированы либо со всеми их активами, либо частично (только в отношении активов, которые напрямую были связаны с незаконной деятельностью до момента обнаружения дополнительных фактов).

5) Использование «псевдонимных» криптовалют и миксеров

Использование анонимных или псевдонимных криптовалют (например, **Monero**, **Zcash**) и сервисов для "микширования" транзакций (например, **Bitcoin Mixers**) представляет собой серьезный вызов для AML-мер. Чтобы предотвратить такие практики:

- **Контроль за миксерами и анонимными криптовалютами**: В некоторых юрисдикциях криптовалютные биржи ограничивают или запрещают работу с такими активами. Также они могут применять специальные фильтры для выявления использования миксеров.

- **Аналитика блокчейна**: Некоторые системы мониторинга могут отслеживать даже анонимные транзакции, анализируя метаданные блокчейна и паттерны транзакций.

6) Обучение и повышение осведомленности

Криптовалютные компании и платформы активно обучают своих сотрудников и пользователей на тему важности соблюдения AML-законодательства. Это может включать:

- Внедрение обязательных обучающих программ для сотрудников по распознаванию подозрительных транзакций.
- Информирование пользователей о возможных рисках и важности соблюдения правил безопасности при совершении криптовалютных операций.

7) Внедрение системы "Reputation" (Репутации)

Некоторые платформы используют систему репутации для отслеживания пользователей и их транзакций. Это может включать:

- **Оценку репутации кошельков и адресов**, например, на основе частоты операций, связи с сомнительными адресами, географической принадлежности.
- Применение **AI (искусственного интеллекта)** для оценки поведения пользователей и предсказания, могут ли их транзакции быть связаны с отмыванием денег.

8) Периодические аудиты и проверки

Платформы могут проводить регулярные **внутренние аудиты** своих систем и операций для обеспечения соответствия стандартам AML. Аудит может включать проверку:

- Программного обеспечения для мониторинга транзакций.
- Работы с клиентами, их идентификацией и верификацией.
- Истории подозрительных операций.

2. Compliance: определение и важность

— Определение Compliance и его роль в бизнесе.

Compliance — это соблюдение и практическое осуществление установленных правил, норм, законов, стандартов и процедур, принятых в определённой организации или сфере деятельности. Комплаенс может касаться различных аспектов, таких как юридические требования, нормативные акты, стандарты безопасности, внутренние политики компании, процедуры и этические

нормы. В рамках криптовалютного бизнеса данные требования могут включать в себя процедуры KYC/KYB, проверку транзакций, заполнение отчетов для регуляторов, и иные требования, в зависимости от юрисдикции.

***Страны которые не выполняют требования FATF заносят в черный список[1], в последнюю неделю октября компания Crystal, отнесла обменник и биржи работающие в таких юрисдикциях как к санкционным и определила в сущности, как нелегальные.**

[1] https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

Важность комплаенса заключается в том, что каждая компания, физическое лицо занимающиеся криптовалютной деятельностью по сути является микро

или макро финансовой организацией в зависимости от количества клиентов, оборотов, пропускаемых в ходе своей деятельности. И как каждой организации в традиционном финансовом кластере, так и в хайтек финтехе, необходимо построение защитной модели бизнеса, руководителей и конечных бенефициаров, так как финансовые преступления в некоторых странах караются очень и очень строго. На наш взгляд примерная структура защиты должна начинаться от перехода на ваш сайт и в каком-то смысле даже никогда не заканчиваться:

1)Фронт защиты Сайт/приложение и иные формы взаимодействия с вашими клиентами, данные элементы должны быть качественно настроены с точки зрения compliance и проведены специальные технические мероприятия.
2)Онбординг в ваш сервис, платформу, - здесь вам необходимо настроить современные и эффективные заградительные меры чтобы не допустить к взаимодействию с вами подставных лиц или же преступников.
3)Так как мы говорим о криптовалютном кластере в вашей ситуации все входящие и исходящие транзакции должны подвергаться автоматизированному аудиту, а также, ручному, в особых установленных внутренними правилами и политиками случаях.
4)В операционные моменты должны быть строго внедрены и реализованы самые современные практики и процедур AML.
5)Важным фактором является хранение и сбор данных о всех ваших контактах с вашими клиентами (контактные данные, переписки и иная информация о клиентах), лучше, если данное хранение осуществляется бессрочно.

Данная структура, конечно, это не полная инструкция. Подробно мы ее декомпозируем в следующих главах.

— Взаимосвязь Compliance и AML, совместное значение для безопасности и соблюдения законодательства.

Compliance (комплаенс) и **AML** (Anti-Money Laundering — борьба с отмыванием денег) тесно взаимосвязаны и играют ключевую роль в обеспечении безопасности вашего бизнеса в предотвращении финансовых преступлений и соблюдения законодательства. Комплаенс является широким понятием, охватывающим все аспекты соблюдения нормативных требований и внутренних стандартов, в то время как AML — это одна из важнейших составляющих системы комплаенс, направленная исключительно на предотвращение осуществления отмывания денег и финансирования терроризма.

Взаимосвязь Compliance и AML

- **AML как часть общего комплаенс-режима**

AML является важной частью общей системы **compliance**, так как компании должны соблюдать не только общие правила законодательства (например, в области защиты данных, корпоративного управления), но и специальные требования, направленные на предотвращение финансовых преступлений, таких как отмывание денег и финансирование терроризма конкретно в их сфере деятельности.

Комплаенс-отдел или специалисты по комплаенсу (compliance officers) в большинстве организаций отвечают за внедрение и соблюдение политик **AML**, которая включает в себя процедуры, направленные на выявление, предотвращение и фиксирование информации о подозрительных операциях.

- **Общие цели для безопасности и соблюдения законодательства**

Одна из главных задач как **compliance**, так и **AML** — это минимизация рисков бизнеса, связанных с нарушением законодательства, а также защита от правовых и финансовых санкций, которые могут наступить в связи с работой с определенным перечнем физических и юридических лиц.

Введение данных норм во внутренние и внешние политики компании, помогают соблюдать не только национальные, но и международные стандарты, такие как рекомендации **ФАТФ (Financial Action Task Force)**, которые требуют внедрения эффективных систем AML и комплаенс-процедур.

AML-процедуры являются важной частью соблюдения **compliance**, направленной на защиту компании от вовлечения в незаконные финансовые операции, что помогает избежать штрафов, уголовных преследований и утраты репутации.

- **Комплаенс как интегратор в борьбе с отмыванием денег**

Комплаенс-отдел играет роль интегратора для внедрения процедур, которые позволяют компании соблюдать **AML**-регуляции. Он разрабатывает и внедряет стратегии для предотвращения отмывания денег, таких как:

Проводит **KYC (Know Your Customer)** — идентификацию и верификацию клиентов.

Обеспечивает **мониторинг транзакций** для выявления подозрительных действий.

Внедряет внутренние контрольные механизмы для обеспечения соблюдения **AML**.

Обучает сотрудников компании стандартам **AML** и регулярным обновлениям законодательства.

Важность совместного значения Compliance и AML для безопасности бизнеса

- **Предотвращение финансовых преступлений**

AML служит основой для выявления и предотвращения незаконных действий, таких как отмывание денег, финансирование терроризма и иных видов преступлений. В свою очередь, **compliance**-отдел встраивает **AML**-политику в более широкую систему соблюдения норм, что позволяет эффективно выявлять любые правонарушения.

Пример: Платформы для обмена криптовалют могут использовать средства **AML** для мониторинга и блокировки транзакций, которые могут быть связаны с преступной деятельностью, при этом соблюдая общие требования комплаенса, включая законы по защите персональных данных и правам клиентов.

- **Защита от юридических и финансовых рисков**

Нарушение стандартов **AML** может привести к значительным юридическим и финансовым последствиям для компании, включая огромные штрафы, уголовные преследования и потерю деловой репутации. Внедрение **compliance**-процессов, включая **AML**, помогает минимизировать такие риски и обеспечивает соблюдение всех требований законодательства.

.

- **Соответствие международным стандартам**

На международном уровне существует множество стандартов и рекомендаций, регулирующих вопросы **AML** (например, **ФАТФ**, **EU Directives on Anti-Money Laundering, MiCA (Markets in Crypto-Assets Regulation) и иные**), которые требуют от компаний внедрения механизмов комплаенса для борьбы с отмыванием денег и финансированием терроризма. Комплаенс-отделы ответственны за внедрение этих стандартов в повседневную практику и обеспечение их соответствия международным требованиям.

Пример: В Европе, в соответствии с **Директивой ЕС по борьбе с отмыванием денег**, криптовалютные платформы обязаны в определенном порядке соблюдать требования **AML** и **KYC**, что выдвигает высокие требования как к комплаенс-отделам, так и к специалистам по AML. Данные требования

включают в себя особый порядок работы AML специалистов внутри компаний, особый порядок проведения и анализа транзакций, выводя нормы комплаенса, а также AML.

- **Репутационная безопасность**

Соблюдение норм **AML** и общих принципов **compliance** помогает защищать репутацию компании. Нарушения могут повредить доверие клиентов и партнеров, что имеет долгосрочные последствия для бизнеса.

Пример: Если платформа для обмена криптовалютами не соблюдает требования **AML** и вовлекается в незаконные операции, она рискует потерять клиентов и доверие инвесторов. Её активы, выводимые с кошельков компании рискуют быть размечены как высокорисковые и санкционные, что отразиться на возможностях обмена, предоставляемых лицу. В то же время, демонстрация приверженности **AML** и **compliance** может укрепить репутацию компании, отражаемую в также ее готовности во взаимодействии с государственными органами стран.

- **Снижение операционных рисков**

Комплаенс и **AML** помогают компаниям управлять операционными рисками. Соблюдение этих стандартов позволяет выявлять аномальные транзакции, предотвращать несанкционированные переводы, выявлять слабые места в операционной деятельности и минимизировать потенциальные убытки.

Пример: Для криптовалютных обменников важно следить за соблюдением **AML**-процедур, чтобы предотвратить использование их платформ для отмывания денег, что также является частью общей стратегии управления операционными рисками.

3. FATF и международные стандарты

— Определение FATF и его роль в формировании AML-стандартов.

FATF – созданная по решению стран «большой семерки» в 1989 году межправительственная организация, которая занимается выработкой мировых стандартов в сфере противодействия отмыванию преступных доходов и финансированию терроризма. Также организация осуществляет оценки соответствия национальных систем этим стандартам.

Рекомендации FATF (Financial Action Task Force) играют ключевую роль в формировании международных стандартов для предотвращения отмывания денег (AML) и финансирования терроризма (CFT).

Одной из наиболее актуальных тем в последние годы является влияние этих стандартов на криптовалютные компании и их деятельность, особенно в контексте выполнения требований, связанных с **Travel Rule** (правило

путешествия). Рассмотрим, как рекомендации FATF касаются криптовалютных компаний и их взаимодействия с финансовыми учреждениями.

Рекомендации FATF и криптовалюты

FATF выпустила ряд рекомендаций, которые касаются криптовалютных компаний (включая биржи, кошельки и другие провайдеры криптовалютных услуг) и отражают важные положения о соблюдении стандартов AML/CFT. В последние годы FATF постоянно обновляет свои рекомендации, уточняя, на кого конкретно распространяются их требования, например, теперь их требования влияют не только на **криптовалютные компании**, но и на субъекты, осуществляющие финансовые операции.

Основные положения, влияющие на криптовалютные компании:

- **Регистрация и лицензирование криптовалютных компаний**: Криптовалютные сервисы должны быть зарегистрированы и/или лицензированы в соответствии с местным законодательством, которое соответствует стандартам FATF, включая соблюдение требований по предотвращению отмывания денег и финансирования терроризма. Это означает, что криптовалютные компании должны внедрять внутренние системы для анализа и отчетности о подозрительных операциях.
- **Проверка клиентов (KYC)**: Криптовалютные компании обязаны проводить процедуры **знания своего клиента (KYC)**, что включает в себя сбор и верификацию информации о пользователях. Это необходимо для предотвращения анонимных транзакций и для обеспечения того, чтобы компании могли отслеживать и идентифицировать потенциальные угрозы, такие как отмывание денег и финансирование терроризма.
- **Отчетность о подозрительных операциях**: Как и традиционные финансовые учреждения, криптовалютные компании обязаны сообщать о подозрительных операциях в соответствующие органы, если существует основание полагать, что транзакция может быть связана с преступной деятельностью.

Travel Rule

Одним из ключевых требований FATF, которое непосредственно влияет на криптовалютные компании, является **Travel Rule**. Это правило предполагает обязательство для финансовых учреждений передавать определенную информацию о клиентах в случае, если переводы средств превышают определенные суммы. В отношении криптовалют это правило было адаптировано к особенностям криптовалютных транзакций.

Суть Travel Rule для криптовалют: В соответствии с Travel Rule, криптовалютные компании, такие как биржи, кошельки и другие провайдеры

услуг, должны собирать и передавать информацию о контрагенте при совершении транзакций выше установленного порога (обычно это сумма в эквиваленте 1000–3000 USD или евро, в зависимости от юрисдикции). Эта информация должна передаваться от одной компании к другой, если

криптовалютные средства перемещаются между разными платформами. В частности, требования касаются следующих данных:

- Имя, адрес, дата рождения клиента или название юридического лица;
- Номер счета или идентификатор транзакции;
- Дополнительная информация, позволяющая идентифицировать отправителя и получателя.

Таким образом, **Travel Rule** требует, чтобы криптовалютные компании могли отслеживать и идентифицировать как отправителей, так и получателей криптовалютных транзакций, что в значительной степени уменьшает анонимность криптовалют и позволяет предотвратить использование криптовалют для незаконных целей.

Влияние на криптовалютные компании

- **Сложности в исполнении**: Криптовалютные транзакции часто бывают анонимными или псевдонимными, что затрудняет сбор и передачу требуемой информации о клиентах. Для того чтобы соответствовать стандартам FATF, криптовалютные компании вынуждены внедрять новые технические решения для сбора и передачи информации, например, через использование стандарта **VASP (Virtual Asset Service Provider)** и соответствующих протоколов передачи данных.
- **Технические вызовы**: В отличие от традиционных финансовых транзакций, криптовалютные переводы происходят напрямую между пользователями без посредников, что требует создания новой инфраструктуры для сбора и передачи данных, соответствующих требованиям Travel Rule. Одним из таких решений является **InterVASP Messaging Protocol**, который был предложен для упрощения передачи данных между провайдерами виртуальных активов.
- **Проблемы с конфиденциальностью**: Множество криптовалютных компаний опасаются, что полное соблюдение правил FATF, в том числе Travel Rule, может нарушать принципы конфиденциальности и анонимности, которые являются важными для многих пользователей криптовалют. Это может привести к негативным последствиям для криптовалютной индустрии, включая потерю клиентов, которые ценят анонимность своих транзакций.
- **Разница в подходах по регионам**: Не все страны следуют рекомендациям FATF одинаково. В некоторых странах требования могут быть мягче, в то время как в других криптовалютные компании могут столкнуться с жесткими ограничениями. Это создаёт фрагментацию на глобальном уровне и требует от компаний значительных усилий для соблюдения локальных нормативных актов.

- **Отчетность и взаимодействие с регуляторами**: FATF требует, чтобы криптовалютные компании обеспечивали механизмы отчетности и соблюдения требований AML/CFT. Это приводит к необходимости интеграции с правительственными органами и финансовыми учреждениями для обмена информацией, что создает дополнительные административные и юридические задачи.

Данные меры значительно отражаются на уровне доверия клиентов к платформам с двух сторон:

1. Уровень доверия повышается, так как деятельность компании становится понятной и прозрачной.
2. Уровень доверия понижается по вышеперечисленным причинам, так как общепринятая анонимность криптовалют до сих пор является один из основных факторов ее использования. Но соблюдение анонимности внутри крипторынков для крупных игроков снижается с каждым днем, потому что крипто сферу продолжают пытаться полноценно включить в «финансовый» сектор.

4. KYC и KYT — основные элементы программы AML

Процедура **KYC** была раскрыта ранее, теперь же мы обратим ваше внимание на **KYT**.

— Процедура **KYT** (Know Your Transaction) и ее значение для мониторинга транзакций.

KYT (Know Your Transaction) — это процесс мониторинга и анализа транзакций с целью выявления подозрительных или аномальных операций, которые могут быть связаны с отмыванием денег (AML), финансированием терроризма (CFT), мошенничеством или другими незаконными действиями. Эта процедура часто используется в сочетании с **KYC (Know Your Customer)**,

который сосредоточен на идентификации и верификации клиента. Вместе KYC (KYB) и KYT образуют полный комплекс мер по предотвращению финансовых преступлений, обеспечивая более глубокое понимание и контроль над поведением клиентов и их операций.

Определение и суть процедуры KYT

KYT фокусируется на **мониторинге транзакций**, анализе их паттернов и аномалий с целью идентификации операций, которые могут быть связаны с незаконной деятельностью. В отличие от **KYC**, который концентрируется на сборе и верификации данных клиента (отправителя/получателя), **KYT**

анализирует каждую финансовую операцию с точки зрения потенциальных рисков, таких как:

- Необычные суммы или частота транзакций.
- Операции с высокорисковыми странами или юрисдикциями.
- Использование анонимных сервисов или криптовалют.
- Многочисленные небольшие транзакции (так называемый **smurfing**).

Таким образом, **KYT** помогает выявить подозрительные действия на уровне транзакций, что является неотъемлемой частью общей политики **AML** и **CFT**.

Значение KYT для мониторинга транзакций:

- **Выявление аномалий в транзакциях**

KYT играет важную роль в обнаружении **аномальных транзакций**, которые могут указывать на отмывание денег или другие формы финансовых преступлений. Примером аномалии может быть внезапное увеличение объема операций клиента, частые переводы в короткие промежутки времени или операции с высокой стоимостью без видимой экономической обоснованности. Для этого используются **алгоритмы и автоматические системы мониторинга**, которые анализируют поведение транзакций в реальном времени, что позволяет быстро обнаруживать аномалии.

- **Идентификация схем отмывания денег**

Технология **KYT** помогает идентифицировать несколько типов схем отмывания денег, таких как **структурирование (smurfing)**, когда большие суммы разбиваются на небольшие транзакции, чтобы избежать пороговых значений для отчетности, или использование **мульти-каналов** для перемещения средств.

Например, если клиент выполняет несколько переводов на небольшие суммы, которые в совокупности представляют собой крупную сумму, это может вызвать подозрение.

- **Поддержка соблюдения нормативных требований**

Компании, работающие в финансовых и криптовалютных секторах, обязаны соблюдать международные стандарты **AML** и **CFT**. Процедуры **KYT** помогают соответствовать этим требованиям, отслеживая все транзакции и уведомляя органы о возможных подозрительных операциях.

ФАТФ (Financial Action Task Force) и другие международные организации требуют от финансовых учреждений внедрять системы мониторинга, способные выявлять такие риски.

- **Использование технологий для автоматизации мониторинга**

Современные **системы мониторинга транзакций** используют технологии искусственного интеллекта (AI), машинного обучения (ML) и аналитики больших данных (Big Data) для создания моделей поведения пользователей и

выявления подозрительных паттернов. Эти технологии могут автоматически отмечать транзакции, которые выходят за рамки привычного поведения клиентов.

Например, алгоритмы могут анализировать объем и частоту транзакций, географию перевода средств и другие параметры, чтобы определить высокорисковые операции.

- **Минимизация рисков и обеспечение репутации**

KYT помогает минимизировать риски для финансовых учреждений, в том числе **банков**, **криптовалютных платформ**, **страховых компаний** и **финансовых технологий (FinTech)**. Раннее выявление подозрительных транзакций позволяет не только предотвратить возможное участие в отмывании денег, но и защитить компанию от штрафов, судебных разбирательств и потери репутации.

Пример: криптовалютная биржа может использовать **KYT** для мониторинга операций, связанных с криптовалютами, чтобы предотвратить их использование для незаконных целей, таких как финансирование терроризма или торговля на черном рынке.

- **Противодействие финансированию терроризма (CFT)**

KYT играет ключевую роль в борьбе с финансированием терроризма, потому что она помогает отслеживать денежные потоки, которые могут быть использованы для финансирования террористических группировок или других незаконных операций. Например, если система мониторинга фиксирует переводы средств в высокорисковые регионы, это может быть сигналом для дальнейшего расследования.

Как работает KYT?

- **Мониторинг в реальном времени**

Система **KYT** мониторит транзакции в реальном времени, что позволяет мгновенно выявлять любые аномалии или подозрительные операции. Это особенно важно для финансовых организаций и криптовалютных платформ, где объем транзакций может быть очень большим.

Пример: платформа для обмена криптовалютами может настроить персональную систему для автоматического мониторинга всех транзакций и предупреждения о подозрительных переводах или использовании анонимных криптовалют.

- **Анализ транзакционных паттернов**

Использование алгоритмов для анализа **транзакционных паттернов** позволяет системе выявить неожиданные изменения в поведении клиента

или его операций. Это может включать необычные схемы переводов, частые переводы в различные страны или нетипичное поведение по сравнению с историей транзакций клиента.

- **Отчеты и уведомления**

В случае выявления подозрительных транзакций, системы **KYT** генерируют **отчеты** и **уведомления** для дальнейшего анализа. Эти отчеты могут быть отправлены внутреннему отделу комплаенса для более глубокого расследования или направлены в регуляторные органы, если того требует законодательство.

- **Интеграция с KYC и AML процессами**

В рамках общего процесса соблюдения требований **AML**, система **KYT** интегрируется с процедурами **KYC**, чтобы получить полную картину клиента и его финансовой деятельности. Например, если клиент уже проходит процедуру **KYC**, система может анализировать его транзакции в контексте ранее полученной информации о нем, чтобы определить, являются ли его действия аномальными или высокорисковыми.

Примеры применения KYT:

- **Криптовалютные платформы**: Биржи, такие как **Binance**, **Coinbase** и другие, используют **KYT** для мониторинга криптовалютных транзакций, чтобы предотвратить отмывание денег и финансирование терроризма. Они анализируют поток средств и следят за переводами на адреса, которые могут быть связаны с преступной деятельностью.
- **Банки и финансовые учреждения**: Банки применяют **KYT** для мониторинга ежедневных транзакций, выявления подозрительных операций, таких как структуры с несколькими мелкими переводами или транзакции с высокорисковыми странами.
- **FinTech компании**: Платежные системы и компании, работающие с цифровыми валютами или мобильными платежами, могут использовать **KYT** для мониторинга операций в реальном времени, чтобы предотвратить мошенничество и другие незаконные финансовые действия.

5. Зачем соблюдать AML-процедуры?

— Последствия несоблюдения: юридические, финансовые и репутационные риски.

На данный момент, продолжая ориентироваться на первые годы функционирования криптовалютного бизнеса, когда почти полностью отсутствовало законодательство данной сферы, а также государственное влияние на неё было минимальным, индивидуальные предприниматели,

компании, или частные лица, к сожалению, при его построении, продолжают пренебрегать простейшими нормами должной осмотрительности, которым необходимо следовать. Несоблюдение даже простейших мер (мы не говорим сейчас, конечно, о строгом регулировании) может приводить к серьезным последствиям, которые мы распишем далее.

Хочется также отметить, что в текущей обстановке, повышается необходимость не только базового соблюдения минимальных требований, но и полноценного погружения в уже более сложные международные стандарты «compliance», во избежание вышеупомянутых последствий. Ведь криптовалютная сфера, которую можно отнести к финтех-кластеру, в связи с продолжающимся повышением к ней интереса привлекает к себе всё больше внимания регуляторов.

Повышенное внимание регуляторов несёт в себе ужесточение законодательства, более детальное и подробное применение санкций, а также более активное противодействие правонарушениям внутри сферы.

В качестве первого примера приведем, всем уже давно известную, некачественную проверку поступавших активов, а также продавцов и покупателей, приводящую к как минимум постоянным блокировкам активов/аккаунтов и запросам от государственных органов, которые будут влиять на стабильность бизнеса и частных финансов, дополнительно хочется отметить объем заблокированного токена USDT прямо на блокчейне в обход каких либо централизованных ресурсов приближается к 1.8 млрд.$ и к 4 тысячам кошельков, что по истине не может оставлять в стороне любого профессионального участника рынка.

При этом, если ранее порядок снятия блокировки был понятен и относительно прост, то теперь он стал сложнее, а требования выше.

Например, участился порядок снятия блокировок не по личному решению и рассмотрению бирж, а через получение лицензии OFAC/FINCEN. Дополнительно формируется практика, при которой даже при снятии блокировки и ограничений внутри биржи, средства всё равно не подлежат выводу по иным причинам, обозначенным платформой, практически любой сервис или биржа защищают себя похожими по смыслу формулировками «заблокированы и удерживаются на срок который сервис посчитает нужным».

Также обратим внимание на учащение направления запросов от государственных органов разных стран и расширение такой практики по все большему количеству стран. Это связано с расширением законодательных норм, а также перечня юрисдикций, применяющих их. Увеличилось и

количество специалистов, базово разбирающихся в порядке работы данного сектора. Повышение количества запросов дают дополнительное давление на крипто бизнес и необходимость полноценного внедрения ими процедур **compliance**. Ведь при предоставлении всех запрошенных документов и информации, платформы смогут избежать негативных последствий, которые могут быть возложены на них, вместо, конечно, бенефициара нарушения. Также несоблюдение норм* и невозможность предоставления информации базово может наложить ограничения на предпринимателей и частные лица, так как несоблюдение норм, с каждым разом наказывается все строже, накладываемыми ограничениями, запретами и санкциями.

Конечно, мы не можем забывать и о таких санкциях как гигантские штрафы, большие сроки лишения свободы, испорченная репутация, - всё это может быть последствием несоблюдения элементарных норм, о которых мы писали выше.

В текущих реалиях криптовалютный сектор более не является «самоуправной» платформой, позволяющей участникам рынка действовать по «совести» и устанавливать свои требования безопасности и ведения бизнеса самостоятельно. Государственное влияние растет, деанонимизация продолжается, санкции ужесточаются.

Именно поэтому сейчас, как никогда, важно внимательно и четко соблюдать compliance и процедуры AML.

Далее в документе мы обсудим шаги, которые могут помочь нам избежать всех этих страшных, но вполне реальных и применяемых мер, от которых каждый месяц сотрясается наше коммьюнити.

— Основные выгоды: повышение доверия клиентов, устойчивость бизнеса и адаптивность к изменениям в законодательстве.

Соблюдение норм, описанных выше, не просто помогает избежать вышеперечисленных санкций, но и позволяет вашему бизнесу остаться «на плаву» при внесении изменений в текущее законодательство. Любая компания, обладающая лицензией и реально работающими нормами соблюдения комплаенса в глазах клиента является благонадежной, повышая уровень доверия и объём средств, направляемых внутрь структуры.

Помимо доверия клиентов, соблюдение норм также позволяет быстро и своевременно действовать при изменении структуры и законодательства, формирования новых требований и особенностей работы. Ведь компания, изначально заточенная на законное оформление и проведение деятельности, формирует впечатление благонадежного юридического лица, соблюдающего

и следящего за видоизменением норм. В связи с чем подстроение под них проходит быстро, эффективно и с минимальными материальными затратами.

— Влияние на долгосрочную стратегию компании.

Как уже было указано ранее, пластичность политик и юридической обвязки компании помогает ей быстро подстроиться под рынок, а также его требования. Остаться на плаву и не подвести уже существующих клиентов, привлекая новых. Именно резкие изменения, несущие в себе обязанность соблюдения норм, с наличием прямых санкций, не позволяет многим компаниям быстро и эффективно продолжать свою деятельность, поддерживая свои активы в положительном балансе на момент перестройки внутренних политик и процедур компании. Готовность компании соблюдать эти нормы сразу и их фактическое соблюдение – именно это позволяет ей лидировать на рынке, не теряя время не перестройку и проблемы с государственными органами, а также, не позволяя данный факторам влиять на бизнес-процессы и тем самым необоснованно ограничивать пользователей.

6. **Структура защиты компаний финтех-кластера**

— **Основные уровни защиты**: краткое описание иерархии и зон ответственности (например, AML-офицер, отдел Compliance).

В зависимости от выбранной юрисдикции будет отличаться перечень потенциальных сотрудников. Мы возьмем базовую иерархию. Без излишней строгости, но и вне полного отсутствия регулирования.

Внутри компании должны быть трудоустроены:

Директор/учредитель – они должны иметь финансовое образование, понимать потенциальные риски и методы их нивелирования, назначать и обучать персонал.

AML/комплаенс офицер – связующее звено между компанией и государственными органами. Следит за соблюдением норм внутри компании, вносит коррективы и комментарии, а также передает информацию о потенциально опасных транзакциях, а также о целенаправленных не соблюдениях законодательства компанией государственным органам.

Рядовые сотрудники – вручную осуществляющие работу по проверке используемых технических решений, их эффективности и применения.

Отдел приема обращений – немаловажные сотрудники, берущие на себя роль разрешающих конфликты и иные ситуации, связанные с работой с клиентами, раскрывающие содержание политик и причины вносимых

ограничений и изменений, работающие и активно коммуницирующие с клиентами, фиксирующими паттерны их поведения.

— **Порядок внедрения процессов**: описание ключевых этапов внедрения AML-процедур в компании (например, разработка политик и процедур, обучение персонала, регулярные аудиты).

Порядок работы прост и сложен одновременно. Он состоит из нескольких шагов и эффективность их внедрения будет зависеть исключительно от эффективности внедрения данных пошаговых действий в зарегистрированную и лицензированную в рамках законодательства компанию:

- определение сферы работы и перечня оказываемых услуг, включая юрисдикции и клиентскую базу;
- составление письменных политик и бизнес плана;
- практическое внедрение составленной документации вовнутрь компании в качестве реальных процессов;
- найм и обучение необходимого персонала.

— **Механизмы отчетности и контроля**: как компании проверяют соответствие установленным правилам, включая внутренние и внешние аудиты, отчеты и тестирование систем.

Данная информация доступна в рамках конкретной юрисдикции при получении лицензии. Данная работа ложится полностью на нанятого AML офицера/специалиста, именно поэтому важна его профессиональная квалификация и эксклюзивная работа с компанией.

В соблюдении установленных норм помогает изначально качественная подготовка юридической обвязки, которая формируется исключительно на базе законодательства и иных необходимых требованиях. Наличие качественной документации позволяет компании и её сотрудникам совместно и эффективно следовать её «прописным истинам», тем самым защищая компанию от потенциальных неосознанных нарушений.

Бухгалтерия в сфере криптовалют также имеет большую ценность. Например, некоторые юрисдикции на данный момент обладают нулевой налоговой ставкой для криптокомпаний, какие-то пытаются взыскивать налог с прибыли, некоторые, не имея возможность до конца проработать порядок работы крипто компаний, взымают налоги с дохода. Наличие четкой документации, фиксирующей расходы, доходы и прибыль компании – поможет

компании свободно и уверенно защищать свои права в случае возникновения вопросов или спорных ситуаций.

Отчетность финансистов, бухгалтеров и AML специалистов, хотя бы раз в квартал, также предоставит компаниям дополнительную уверенность в своем бизнесе и его процессах. Некоторые страны позволяют соблюдать свободную форму отчётности или вовсе не требуют её (но данный факт не исключает ее необходимость в целях безопасности вашего бизнеса).

Технические сотрудники внутри компании (или стабильный аутсорс, или официально трудоустроенные) также являются немаловажным фактором, способствующим безопасному ведению бизнеса. Стабильный специалист будет больше внимания уделять паттернам и особенностям работы, позволяя актуально видоизменять применяемые технические решения.

Глава 2. Подготовительная.

В этой главе будут раскрыты этапы первичных действий с описательной частью на момент возникновения идеи о создании криптовалютного бизнеса.

Мы рассмотрим порядок и его особенности с использованием фигуры, например, Ивана, которой было принято решение о создании бизнеса в криптовалютной сфере.

2.1 Введение в подготовительные этапы

— Переход от теории к практике: важность применения знаний AML и Compliance на этапе создания криптовалютного бизнеса.

— Пример создания криптобизнеса на основе бизнес-идеи Ивана: введение к подробному анализу этапов организации.

В первой главе мы обсудили, какие нормы AML и Комплаенса существуют, а также важность их применения на практике.

Данные аспекты важно понимать и осознавать перед созданием своего крипто бизнеса по следующим причинам:

- оценка готовности соблюдения данных норм
- оценка возможности соблюдения данных норм
- готовность отвечать за риски и последствия несоблюдения норм или их неосознанного нарушения
- затраты, связанные с применением данных норм внутри структуры
- подбор структуры, сотрудников и юрисдикции в соответствии с данными нормами
- подбор ПО, которое будет использоваться, и иных технических решений, которые необходимы, в соответствии с нормами Комплаенса

После изучения законодательных требований и особенностей бизнеса Иван должен поставить перед собой следующие вопросы:

Определение конечного продукта, потребителя и вида оказываемых услуг.

Какой именно вид бизнеса закроет поставленные цели и запросы?

Будет ли это криптовалютный процессинг, обменник в стране нерегулирующей криптовалютную сферу или полноценная биржа с возможностью работы с разными иностранными гражданами?

Предположим, Иван, хочет иметь возможность работать с большим количеством юрисдикций, с разными клиентами, иметь возможность официально регистрировать прибыль компании, платить налоги.

Также Иван не хочет предоставлять сложные технические решения, работать в качестве платёжного агента с использованием криптовалюты, предоставлять услуги процессинга или кастодиальные решения. Иван интересует только возможность предоставления услуги обмена криптовалют.

В связи с чем он принял решение остановиться на создании биржи[2] за рубежом, в более урегулированных юрисдикциях.

Следующий вопрос, который теперь встает перед ним, это как данная биржа будет работать?

Будет ли она принимать безналичный/наличный фиат или торговать только в связке крипта-крипта?

Здесь мы переходим ко второму этапу.

2.2 Выбор направления бизнеса

— Различия в методологиях регулирования: ФИАТ-Крипта и Крипта-Крипта.

— Ключевые аспекты выбора направления, влияние на структуру AML и Compliance.

Фиат – крипта и крипта- крипта.

Рассмотрим, чем эти два аспекта отличаются.

На первый взгляд, эти два варианта отличаются между собой всего парой шагов, но в них заложена огромная разница повышающая сложность создания бизнеса и выведения его в полноценно рабочую структуру.

Биржа, работающая по направлению крипта-крипта сокращает своё взаимодействие с финансовыми структурами, банками, снимает с себя обязательства дополнительных AML, KYC, KYB и DD процедур, запрашиваемых банками.

Порядок взаимодействия с биржами и банками также различается, в связи с чем такому бизнесу нет такой острой необходимости в разносторонних специалистах, которые смогут закрывать общение и

взаимодействие с обеими структурами, ведь коммуникация с банками при работе крипта-крипта минимальна.

[2] На иностранном рынке нет понятия обменника, которое более развито для стран СНГ. Компания, осуществляющая обмен крипта-крипта, на территории, например, Российской Федерации будет называться обменником, но для иностранного рынка такая компания будет сразу квалифицированна в качестве биржи. Внутри данного текста используется понятие, более применимое для иностранных рынков – биржа, но в ходе прочтения текста, можно учитывать, что, по сути, учитывая подмен понятий и их разное формирование в связи с особенностями перевода и развития рынка, биржа, иногда, равно обменник (биржа – exchange – обменник).

Риски блокировки счетов, заморозки средств и введения иных ограничений более ощутим в банковской сфере так как, например, открытие банковского счёта занимает больше времени и запрашивает больший объём информации о компании и ее бенефициарах, чем открытие аккаунта на бирже. Что усложняет процесс создания для себя подушки безопасности и альтернативных решений.

Помимо вышеперечисленных сложностей в работе компании, для такой биржи также возникают дополнительные требования в сфере Комплаенс и AML процедур. Внутри компании должны быть сформированы отдельные направления и наняты отдельные сотрудники, которые применяют внутри структуры AML нормы, которые общепризнаны в банковской сфере и которые отличаются от крипто AML норм. Расширенное KYC, вопрос хранения/использования банковской информации клиентов для осуществления переводов, риски утечки и безопасности. На данный момент санкции за несоблюдение любых из перечисленных норм на уровне банков выше, чем для крипто.

По сути, компания, принимающая решение работать с фиатом, принимает на себя обязательства по дополнительному соблюдению ещё одних законодательных норм в сфере AML по сложности, объему и количеству выше, чем AML нормы для крипто компаний, работающих крипта-крипта, в два раза увеличивая свою ответственность, обязательства и риски.

2.3 Оценка целевой аудитории (ЦА)

— Почему анализ целевой аудитории важен для запуска бизнеса.
— Примеры крупных игроков и их подходы к выбору целевой аудитории.
— Как целевая аудитория влияет на выбор юрисдикции и услуг.

Иван определил, что хочет работать с биржей крипт-крипта, в иностранной юрисдикции. Чтобы более точно сформулировать свой запрос и определить, интересующие его страны он хочет определить, кому конкретно он хотел бы продавать свои услуги, свою ЦА. Почему это важно?

Целевая аудитория играет важную роль в успешном продвижении бизнеса на криптобиржах. Чтобы эффективно привлекать пользователя и удерживать его, необходимо понимать, кто может быть потенциальным клиентом.

Потенциальными клиентами криптобиржи могут быть люди, заинтересованные в инвестировании и торговле криптовалютами. Они могут быть как новичками, так и опытными трейдерами, которые ищут новые возможности для торговли и получения прибыли. Кроме того, среди целевой

аудитории могут быть предприниматели и компании, которые хотят использовать криптовалюты для проведения бизнес-операций.

Так как Иван создаёт биржу, его интересуют только те, кто хотел бы торговать криптовалютой, осуществлять обмен и получать иные услуги в этой сфере. Иван не заинтересован в том, чтобы предоставлять услуги компаниям или физическим лицам, которые хотят использовать криптовалюту для своих бизнес целей, таких как оплата услуг/заработной платы или иных.

Теперь ему нужно понять, его клиент, какой он, какой у него портрет. Для каждой страны, портрет может быть свой. Возраст, пол, образование, уровень дохода – могут изменяться в зависимости от страны гражданства и проживания.

Какой дополнительный функционал внутри моей платформы может заинтересовать именно того клиента, к которому я стремлюсь?

Первоочередно нужно понять, какой рынок вам ближе?

Где вы сможете заработать наибольший объем, чтобы продолжать развитие вашей платформы?

Ответив на эти вопросы, и только после этого, можно запускать процесс получения лицензии.

Даже обращая внимание на работу крупных игроков, можно обратить внимание, что все они выходят на новые рынки постепенно, объявляют о запуске работы на территории той или иной страны шаг за шагом. Почему же? Потому что наличие криптолицензии в одной юрисдикции не гарантирует возможность работы по всему миру. Каждый рынок индивидуален, имеет свои особенности и свои опасности.

Например, вы можете начать с рынка стран СНГ, пока там не такие высокие требования к регистрируемому юридическому лицу, к Комплаенсу. Создать там почву для старта, разогнать объем и получаемую прибыль. Опять же, мы всё делаем с целью развития, для развития нужны средства, для заработка необходимых средств нужно трезво оценить вкладываемый ресурс и потенциально получаемую прибыль. На каждом этапе ваша ЦА аудитория может и будет меняться. Например, на рынке СНГ вы более спокойно относитесь к гражданам из

санкционных стран. Далее, заработав необходимый объём, вы двигаетесь дальше, в сторону международного рынка, например, в сторону ЕС. И создаете отдельное ответвление там.

Здесь вам более серьёзно придётся относиться к AML нормам в сфере санкционных стран и граждан, ограничить их участие на вашей платформе.

При регистрации вы можете отдать своё предпочтение Латвии или Литве, может быть Польше, если готовы к её налоговым ставкам. Когда компания настроена сразу выходить на высокие объёмы отдаётся предпочтение Эстонии – ведь именно там законодательство ЕС по MICA отражено в своей финальной форме. Надо учитывать, что вскоре, все страны ЕС выровняют своё криптозаконодательство и процедуры регистрации ощутимо усложняться в юрисдикциях, где ранее это было проще (ориентировочный срок финализации законодательства MiCA во всех ЕС странах – июль 2025 года).

Потом вы можете рассмотреть Азию — тогда вас заинтересует Гонконг или Сингапур.

При наличии идеально чистой истории и выверенной системы комплаенса можно рискнуть идти на Штаты и Канаду, тогда, конечно, нужно рассматривать получение лицензии в одной их стран.

Разделять рынки – стабильная практика, находящая отражение в самых крупных компаниях, в том числе Binance или Huobi. Например, рынок СНГ и иных стран этих территорий – регулируется, пока, спорно, также часто рассматривается как санкционный, в связи с чем его лучше выделять из основного бизнеса компании, выстраивая под него свою систему. Азиатский рынок предоставляет широкий объем технических решений в сфере криптовалюты позволяя погружать её во многие сферы вашего бизнеса.

Целевая аудитория, как мы писали ранее, также будет отличаться от рынка к рынку. Например, учитывая, что Азия предоставляет необычные технические решения в сфере криптовалют в связке с финансовыми институтами, то на этом рынке заработок вашего клиента должен быть выше среднего, также он должен быть заинтересован в использовании криптовалют внутри своей бизнес структуры, например, в качестве процессинга. В связи с чем, для обменника данный рынок, учитывая его дороговизну, на начальных этапах вовсе не имеет смысла.

Подсанкционная аудитория рынка СНГ и стабильные клиенты рынка ЕС также буду запрашивать разный маркетинг, функционал и затраты на реализацию проекта.

Поэтому важно оценить объём вкладываемых средств, желаемый заработок, уровень структуры, который ваш бизнес готов предоставить на начальных этапах, понять какую ЦА вы сможете привлечь под ваш ресурс и в зависимости от этого выбрать подходящую вам юрисдикцию.

2.4 Выбор юрисдикции и лицензирование

— Основные факторы, влияющие на выбор юрисдикции для криптобизнеса.
— Перечень документов для регистрации бизнеса: road map, AML-документация, сбор информации о бенефициарах, выбор AML специалиста.
— Юридическое оформление бизнеса: регистрация юридического лица и получение криптолицензии.
— Сравнение различных юрисдикций: Латвия, Литва, Польша, Эстония, Гонконг, Сингапур, США и Канада.

Основные факторы, влияющие на выбор юрисдикции для криптобизнеса – данного вопроса мы кратко коснулись в предыдущей части.

Что же ещё нужно понять после определения вида бизнеса, а также его целевой аудитории?

- Определение вводных данных: объем средств для начального этапа, бэкграунд бенефициаров и учредителей, цели на развитие и рост
- Определение примерных оборотов, объемов, целевые показатели на год/три
- Маркетинг, его направление, порядок и вид используемой рекламы, используемые для продвижения каналы
- Занимаемая на рынке ниша, сравнение с конкурентами и схожими бизнесами, потенциальные преимущества перед конкурентами на том или ином рынке

Предположим, Иван уже давно работает в сфере криптовалют и убедился, что хочет сразу вложить определенный объем средств на создание структуры на территории одной из стран ЕС, по направлению крипта-крипта. Какие документы ему пригодятся? Какие шаги ему нужно будет соблюсти?

- Подготовка road map, AML документации (политик, риск моделей и иных документов, в зависимости от юрисдикции), сбор информации о бенефициарах, подбор AML специалиста;
- Регистрация юридического лица;
- Получение криптолицензии;
-Практическое введение AML и иных норм в целях соблюдения Комплаенса;
- Регистрации на юридическое лицо биржевых аккаунтов, личных корпоративных кошельков;
- Запуск работы.

Постепенно пойдем по стадиям, начиная с подготовки road map, остальной документации и общей подготовке к регистрации.

Road map – ваш бизнес план. Как вы видите свою структуру, в ней отражается всё то, что мы обсуждали выше:

- Вид предоставляемых услуг, особенности порядка их предоставления;
- Целевая аудитория;
- Маркетинг;
- Пути и способы развития вашего бизнеса, ожидаемая прибыль через год, три , пять;
- Учредительный состав;
- Структура бизнеса;
- Его риск мониторинг, отношения к безопасности и способ её гарантирования.

С помощью этого документы вы раскрываете регулятору, кто вы есть, почему вы хотите выходить на рынок и как вы планируете на нём работать. Он изучает данный документ и принимает решение, стоит ли вам выдавать лицензию и выпускать на запрашиваемый вами рынок.

Параллельно вы разрабатываете политики для своей компании._ Данные документы создаются в соответствии с международными нормами, а что наиболее важно, локальными требованиями в юрисдикции, где получается лицензия. Политика AML, Политика о персональных данных, Пользовательское соглашение, Risk scoring, - эти документы должны быть у вас на руках на момент подачи заявления на лицензию. И мы говорим не только о внешних, но и о внутренних политиках (более подробно мы раскроем информацию о данных документах в следующей главе).

Также вместе с этими процессами собирается информация об учредителях и идёт подбор персонала. Учредители должны раскрыть о себе всё – образование, опыт внутри сфер, предыдущие места работы, банковские выписки, место проживания и иную информацию. Для некоторых юрисдикций данная информация должна соответствовать определённым требованиям, даже у учредителей. Параллельно идет подбор AML/Compliance офицера. У него должно быть определённое образование, опыт, ограниченное количество компаний в которые он уже трудоустроен, знание местного законодательства и внутренних порядков взаимодействия между компанией и государственными органами.

Далее можно переходить к регистрации юридического лица.

Регистрация юридического лица и получение криптолицензии – объединим данные этапы, ведь теперь все ранее подготовленные, составленные, собранные и переведённые документы, в том числе на учредителей, будут направлены в органы государственной власти на рассмотрение. Потенциально возможно внесение изменений и подготовка дополнительных документов в соответствии с требованиями вышестоящих органов, при ответе на которые в течение примерно 2-8 месяцев вас ожидает получение лицензии (срок зависит от выбранной юрисдикции и вида лицензии). Успех данного этапа примерно на 60% зависит от качества подготовительных этапов.

Поэтому к составлению документов и выбору сотрудников нужно подойти максимально внимательно.

	Латвия/Литва	Польша	Эстония	Сингапур	Гонконг	США	Канада
Лицензия	Вскоре лицензия будет идентична Эстонской (точных данных пока нет, но нет смысла делать компанию на полгода)	Вскоре лицензия будет идентична Эстонской	Крипто лицензия по нормам MiCA	MAS лицензия платежного учреждения	Лицензия оператора денежных услуг (бессрочная)	Необходимо быть зарегистрированным как Money Services Businesses	- Money Service Business registration (MSB), есть для местных и для иностранных компаний, делится на 5 видов.
Налоговая ставка	15% прибыль компаний	Облагается доход, не выгодно для обменников.	20% налог на нераспределенную прибыль, пока не распространяется на крипто компании	Прогрессивная ставка подоходного налога от 0 до 22%. В среднем крипто бизнес подпадает под ставку в 17%. Прирост капитала не	Нет налога на доход, полученный вне территории Гонконга и не от его граждан	Варьируется от штата к штату, где-то может отсутствовать/быть минимальной (н-р Невада, Делавер)	От 15 до 33 % на доход/прибыль

				облагается налогом.			
Срок регистрации	От 4 месяцев	От 4 месяцев	От 5 месяцев	От 6 месяцев	От 8 месяцев	От 8 месяцев, может разниться от штата к штату	От 8 месяцев
Примерная стоимость проекта*	От 40 000 EUR	От 25 000 EUR	От 80 000 EUR	От 250 000$	От 100 000$	От 50 000$ (но дорогие сопровождение, обслуживание и осуществление деятельности)	От 140 000$

Актуальную информацию о стоимости, порядке, ставкам и иную нужно запрашивать на момент регистрации.
*Включает в себя регистрацию компании, подготовку необходимых документов и внедрение внутренних норм AML Compliance, при необходимости также открытие счетов. Данная стоимость закладывает в себя не просто регистрацию компании, а подготовку готового к выходу на рынок продукта.

Выше представлена краткая сравнительная табличка юрисдикций, конечно, при регистрации, нужно учитывать большее количество факторов, но для вводной оценки расходов можно использовать данную информацию. Дополнительный комментарий:

- Скоро на территории всех стран ЕС будут идентичные требования и порядок регистрации крипто компаний, потенциально даже налог будет схож, именно поэтому уже сейчас многие выбирают Эстонию, чтобы в дальнейшем не сталкиваться с процедурами пересоставления и переподачи документации на свои компании при введении финальных норм на территории остальных стран
- Большинство финансовых решений и институтов, а также банков для крипто сферы созданы в Литве, это основная причина, по которой данная юрисдикция является привлекательной
- США, Канада имеют жёсткие требования AML и Compliance особенно к иностранным лицам. Дополнительно нужно учитывать дорогое обслуживание и сопровождение компании.
- Сингапур и Гонконг – закрытый рынок, на котором сложно работать иностранным лицам. Местные директора, сотрудники обязательное требование.

2.5 Действия после регистрации

- Основные этапы подготовки биржи: регистрация аккаунтов, создание кошельков.

После получения одобрения от регуляторов и получения на руки долгожданной лицензии мы переходим к следующим этапам:

Практическое внедрение AML и иных норм в целях соблюдения Комплаенса.

Данный шаг подразумевает в себе внедрение всех норм, описанных в выше обозначенных документах (политиках и тд) внутрь компании на практическом уровне при помощи внешних или внутренних специалистов, в отношении которых может осуществляться донайм. Данный шаг обязательно нужно пройти перед запуском работы для того, чтобы максимально обезопасить свой бизнес. Данный этап защищает вас не только от гонений со стороны государственных органов, но и от недобросовестных клиентов.

После этого компания может начать процесс открытия биржевых аккаунтов и банковских счетов, в зависимости от выбранного порядка работы фиат- фиат или крипта – фиат, и запуск работы.

Данные шаги ведут к финализации задуманного бизнеса и запуску его работы. Они будут отличаться в зависимости от выбранной юрисдикции и вида деятельности.

В общем, они подразумевают повторное прохождение процедуры Комплаенса вашим бизнесом в выбранных биржах/банках, предоставление уже составленных документов, а также дачу дополнительных комментариев и разъяснений с дополнительным подтверждением компанией реальности практической реализации норм, которые были описаны в бизнес- плане.

После открытия счетов, запуска сайта или иных платформ, а также иных элементов вашей структуры, вы можете начать объединение данного пазла, в рабочую бизнес-модель.

Только после этого ваш бизнес можно будет считать успешно зарегистрированным и запустившим работу.

2.6. Дополнительный комментарий

Несмотря на подробность данного документа, при принятии решения о регистрации вашего крипта бизнеса мы советуем вам обратиться за консультацией к юристам, которые работают в данной сфере и помогут вам дать оценку вашим целям, бизнесу и стремлениям.

Например, нет возможности дать чёткий ответ, в какой же стране стоит регистрировать компанию?

Возможность определения четкой страны регистрации будет возможна только после личного общения с юристами или иным специалистами в сфере, которые оценят ваши цели и найдут способы их достижения.

Также специалисты помогут вам дать ответы на следующие вопросы:

- Дешевле/дороже?
- Полное соблюдение норм/подстроение под них в ходе работы?
- Фиат – крипта/ крипта- крипта?
- Наличие/отсутствие кастодиальных решений?

Каждый элемент повлияет на то, какая юрисдикции будет выбрана, как наилучший вариант реализации и достижения поставленных задач.

Подводя итог к выше высказанной информации, включая как вторую, так и первую главы, можно определить следующие основные столпы мироздания при создании крипто бизнеса, каждый из которых мы раскрыли внутри 3 главы:

- Перечень и вид услуг
- Закладываемые затраты
- Интересующий рынок
- Готовность и возможность соблюдать AML требования при создании, до каких объемов
- Уровень внедряемых процедур по безопасности
- Финальные цели и задачи проекта

При определении данных пунктов перед запуском процесса регистрации компании у вас будет возможность создать успешный и прибыльный бизнес в рамках вашего запроса, поставленных задач и целей.

2.7 ВЫВОД. Какую компанию нужно создавать для работы в 2025 году?

Легальную. Это основной рецепт и основное предсказание на 2025 год. Сфера крипто бизнеса выходит из серой зоны, обрастает всё новыми законодательными нормами и требованиями, причём часто, законодательство формируется на основе практики, а не в её преддверии. А данная практика формируется на системе преступление – наказание, преступление может быть неизвестно компании, а наказании реализовываться в процессе разбора. Именно поэтому важно самостоятельно заботиться о безопасности себя и своей компании. Потенциальные материальные и репутационные риски становятся слишком велики, чтобы продолжать вести деятельность, не учитывая все необходимые нормы. Ранее это было выгодно, но более - нет.

Глава 3. Операционная работа.

Операционная работа компании закладываются в ее юридической обвязке и структуре практического применения отраженных в ней норм.

Внешняя политика AML отражает содержание, но не полноту его отражения. Внутренняя политика AML более подробно раскрывает порядок выполнения и соблюдения норм внутри компании и самими сотрудниками. Совместно внутренняя и внешняя политики отражают регуляторные нормы, правила компания с точки зрения рискованности ведения бизнеса. Обе политики AML являются составной, неотъемлемой частью операционной работы финансовых организаций, так как они коррелирует процессы финансовых потоков, предупреждают пользователей и напоминают сотрудникам компании как вести себя в той или иной ситуации.

Основная цель Пользовательского соглашения или Terms of Service (TOS) это установить права и обязанности сторон. Раскрыть, за какие нарушения, допущенные клиентами, компания имеет право реализовать свои права на ограничение предоставляемых клиенту сервисов и также его свободу распоряжения собственными активами. Это делается исключительно в целях защиты крипто компании и в допустимых законодательством рамках. Именно поэтому данный документ по сути является основным документом, к которому часто уже как приложение, может идти внешняя политика AML (зависит от вида компании), далее мы предоставим пример пользовательского соглашения:

Пользовательское соглашение.

Веб сайт разработан и управляется сервисом Имя сервиса.

Данное Пользовательское соглашение («Соглашение») распространяется на всех пользователей Сайта, Сервисов и их Услуг. Перед использованием Сайта, Сервисов и их Услуг, Пользователь должен внимательно прочитать это Соглашение, регулирующие использование им Сайта, Сервисов и их Услуг. В случае несогласия с каким-либо из пунктов настоящего Соглашения, просит Пользователя отказаться от использования данного Сайта и его сервисов и Услуг. Используя в дальнейшем Сайт, Сервисы и/или регистрируясь для использования Услуг, Пользователь подтверждает, что изучил, понимает, принимает и обязуется соблюдать данное Соглашение, регулирующее использование Пользователем Сайта, Сервисов и их Услуг.

Настоящее Соглашение находится в открытом доступе на сайте в актуальной редакции.

Сервис сохраняет за собой право вносить изменения в данное Соглашение. Любые изменения данного Соглашения будут вступать в силу с момента их публикации на Сайте.

Предупреждение

Никакие материалы или информация, полученные через Сайт, Сервисы и Услуги , не представляют собой и не могут быть истолкованы как рекомендация, одобрение, приглашение или предложение заключить какую-либо сделку с любым продуктом или приобрести его, или иным образом иметь дело с цифровой валютой или другими продуктами. Пользователь также понимает, что ни один из поставщиков информации, включая любых Сторонних Поставщиков, не консультирует его лично относительно характера, потенциала, стоимости или пригодности какой-либо конкретной цифровой валюты, портфеля, транзакции, инвестиционной стратегии или любого иного вопроса.

Предоставленная информация не адаптирована к инвестиционным потребностям какого-либо конкретного человека.

Пользователь понимает, что инвестиции в любую цифровую валюту подвержены ряду рисков, и что обсуждения любой цифровой валюты, опубликованные на сайте или иных Сервисах, могут не содержать списка или описания соответствующих факторов риска. Данное соглашение подразумевает, что Пользователь осознаёт, что рынки постоянно меняются, поэтому любая информация, контент, Контент Третьих лиц или другие материалы, предоставляемые на Сайте или иных Сервисах или через них, могут быть неполными или неактуальными или могут быть заменены более актуальной информацией, и Пользователь полагается на такую информацию на свой страх и риск.

Сервис не предназначен для предоставления налоговых, юридических, страховых или инвестиционных консультаций, и ничто не должно быть истолковано как таковое. Пользователь самостоятельно несет единоличную ответственность за определение того, являются ли какие-либо инвестиции или решения подходящими, исходя из инвестиционных целей и личного и финансового положения. При необходимости Пользователю следует проконсультироваться со специалистом в интересующей его сфере относительно конкретной ситуации.

1. Понятия и определения

Персональные данные (Информация) — любая информация, связанная с идентифицированным или идентифицируемым физическим лицом. Лицо является идентифицируемым, когда возможно его идентифицировать прямо или косвенно, в частности, по идентификационному номеру или характерным

физическим, физиологическим, психологическим, экономическим, культурным либо социальным признакам.

Пользователь — физическое лицо, посещающее Сайт или использующее Сервисы для получения Услуг Сайта и Сервисов и являющиеся Субъектом данных, а также Клиентом.

Субъект данных— любое физическое лицо, данные о котором обрабатываются Сайтом, Сервисами или Услугами .

Сайт— веб-сайт.

Учетная запись Пользователя— персональный профиль пользователя или личный кабинет, который создается после регистрации на Сайте, Сервисах или при пользовании Услугами.

Цифровая валюта— валюта, существующая и доступная исключительно в виртуальном виде.

Фиатные деньги— регулируемый государством вид платежных средств, доступных в физическом виде.

Сторонний поставщик Услуг— третье лицо, контрагент , который предоставляет дополнительные Услуги Пользователю или .

Услуги— продукты, предоставляемые Пользователю на сайте через Сервисы или Сайт.

Запрещенное поведение— любое незаконное поведение, которое включает мошенничество, коррупцию, отмывание денег, сговор, финансирование терроризма и любое другое преступное поведение.

Мошенничество— использование обмана с целью преследования личных интересов и нанесения ущерба интересам Пользователей и/или по способу хищения чужого имущества, либо приобретение на него права путем обмана.

Обман— в контексте данного договора — способ мошенничества для получения денег от пользователей интернета. Может включать в себя сокрытие информации или предоставление неверной информации с целью вымогательства у жертв денег, имущества и наследства.

Коррупция— предложение, предоставление, получение или ходатайство (прямо или косвенно) чего-либо ценного, что могло бы оказать ненадлежащее влияние на действия другой стороны.

Отмывание денег— схема финансовых транзакций, целью которой является сокрытие личности, источника и места назначения незаконно полученных денег или финансирование незаконной деятельности.

Противодействие отмыванию денег (AML)— комплекс мероприятий и процедур, направленных на выявление и/или предотвращение использования сайта, сервисов и/или Услуг, предоставляемых в целях отмывания денег.

Противодействие финансированию терроризма (CTF)— комплекс мероприятий и процедур, направленных на выявление и/или предотвращение использования Сайта, Сервисов и/или Услуг, предоставляемых в целях финансирования терроризма.

Санкции— коммерческие и финансовые санкции, применяемые одной или несколькими странами против целевых самоуправляющихся государств, групп или отдельных лиц.

Красные флаги— предупреждения или индикаторы, предполагающие наличие потенциальной проблемы или угрозы с операциями Пользователя, которые проходят через и/или Услугу/Сервис/Сайт .

Сговор— договоренность между двумя или более сторонами, направленная на достижение ненадлежащей цели, включая неправомерное влияние на действия другой стороны.

Финансирование терроризма— предоставление или сбор средств любыми способами (прямо или косвенно) с намерением их использования или при условии, что они будут использоваться полностью или частично для осуществления любого из преступлений, связанного с терроризмом.

Преступное поведение— преступление в любой части мира или то, что будет квалифицироваться как преступление в любой части мира, если оно произошло там.

Знай Своего Клиента (KYC)— комплекс мероприятий и процедур, направленных на получение информации о Пользователе и его деятельности с целью управления рисками Компании.

Надлежащая комплексная проверка клиентов (CDD)— проверка данных/информации о Пользователе и другие проверки, связанные с изучением Пользователя и его деятельности, с целью комплексной оценки риска Пользователя при принятии его на обслуживание и во время его обслуживания.

Политически значимое лицо (PEP)— физическое лицо, играющее выдающуюся общественную роль внутри той или иной страны, или на международном уровне.

Нормативные требования— любой применимый закон, статус, постановление, приказ, судебное решение, решение, рекомендация, правило, политика (в том числе, но не исключительно, Политика управления рисками) или руководство, принятые или изданные парламентом, правительством или любым компетентным судом или органом власти, или любой платежной системой (включая, помимо прочего, банковские платежные системы, карточные платежные системы, такие как Visa, MasterCard, или любую другую платежную, клиринговую

или расчетную систему, или аналогичное соглашение, которое используется для предоставления Сервисов/Услуг).

Политики(а)— Политики и положения, регулирующие порядок предоставления Сервисов и Услуг, в том числе, но не исключительно, Политики управления рисками, Политика конфиденциальности и иные.

2. Содержание Сайта

2.1. Сайт, включая любую информацию, графические изображения, эстетические, технические и другие эффекты, направлен на информирование Пользователей по поводу Сервисов и Услуг («Содержание»).

2.2. имеет все права для адаптирования и внесения изменений в Содержание Сайта по своему усмотрению без предварительного уведомления Пользователя.

2.3. обязан предпринимать разумные и достаточные усилия для постоянного обновления Содержания Сайта. Вместе с этим не вся информация может быть актуальной и полной не гарантирует точности Содержания и не несёт за неё ответственность.

Любые примеры в Содержании Сайта являются иллюстративными. Сервис обязуется делать все возможное для корректного отображения настоящих и будущих Услуг и Сервисов, в то же время они могут отличаться в реальности.

2.4. В случае обновления настоящего Соглашения, его новая редакция вступает в силу через 24 часа после размещения актуальной версии Соглашения на Сайте , или ранее, соответственно с требованиями применимого законодательства. Обязанность об отслеживании актуального Пользовательского соглашения возлагается на Пользователя. Использование Пользователем Сайта с обновленной версией Соглашения будет рассматриваться как понимание Пользователем Пользовательского Соглашения и согласие на использование обновленной версии Соглашения.

3. Содержание Сервиса:

3.1. Сервис, включая любую информацию, графические изображения, эстетические, технические и другие эффекты, направлен на предоставление Пользователю Услуг и предоставления информации о порядке предоставления данных Услуг, его перечня и ограничений (“Содержание”).

3.2. имеет все права для адаптирования и внесения изменений в Содержание Сервиса по своему усмотрению без предварительного уведомления Пользователя.

3.3. обязан предпринимать разумные и достаточные усилия для постоянного обновления Содержания Сервиса. Вместе с этим не вся информация может быть актуальной и полной. не гарантирует точности Содержания и не несёт за неё ответственность.

Любые примеры в Содержании Сервиса являются иллюстративными.

4. Использование Сайта, Сервисов и их Услуг. Учетная запись и ограничения
Использование сайта, Сервисов и их Услуг:

4.1. Сайт, Сервисы и их Услуги являются публичными и доступными для всех пользователей.

Пользователь соглашается использовать Сайт, Сервисы и их Услуги исключительно в законных целях. Сайт, Сервисы и их Услуги предназначены для личного использования Пользователем и в некоммерческих целях.

4.2. Использование Сайта, Сервисов и Услуг осуществляется согласно данному Соглашению и положениям Политик, выложенных в свободном доступе на Сайте.

4.3. С целью обеспечения безопасности пользования Сайта, Сервисам и их Услугами запрещается использование методов сокрытия месторасположения пользователей. В случае возникновения сомнений по поводу безопасности использования Сайта, Сервисов и их Услуг, имеет право запросить у пользователя информацию о его точном местонахождении.

4.4. Пользователь соглашается получать рекламные и/или информационные сообщения от на адрес электронной почты, предоставленный Пользователем в Учетной записи.

Такие электронные письма будут отменены по запросу Пользователя с использованием опции «отписаться», предоставленной в уведомлении, когда это применимо.

4.5. Доступность Сайта, Сервисов и их Услуг не гарантирует возможность доступа к ним в любое время. Пользователь признает, что оставляет за собой право в любой момент задержать, отказать или сделать недоступным в любое время и по своему усмотрению все или часть Услуг, а также сами Сервисы и/или Сайт. Сервис не несет ответственности в случае недоступности какой-либо Услуги, независимо от причин (намеренные действия согласно требованиям настоящего Соглашения и Политик, форс-мажорные обстоятельства и прочее).

4.6. Безопасность и вирусы. Пользователь не может сознательно или неосознанно использовать, или внедрять любое вредоносное программное обеспечение или файлы с целью получения доступа к Сайту, Сервисам и их Услугам, искажения их Содержания или разрушения. Пользователь обязуется предпринимать разумные меры

предосторожности во избежание подобных процессов. Пользователь не может искажать, модифицировать или манипулировать Сайтом, Сервисами и Услугами и их Содержанием любыми способами. Сервис рекомендует предпринимать разумные меры безопасности для предотвращения ущерба оборудованию Пользователей любыми вредоносными программами, а также при получении и прочтении сообщений, уведомлений, писем от , в связи с возможностью причинения вреда их оборудованию. Рекомендуется вход в Учетную запись исключительно с использованием Сайта или официального Сервиса.

Учетная запись и ограничения:

4.7. Создавая учетную запись для пользования Услугами («Учетная запись»),

Пользователь гарантирует, что:

- Пользователь принял это Пользовательское соглашение, положения Политики управления рисками, Политика конфиденциальности и прочих положений использования Сайта, Сервисов и их Услуг;
- Пользователь достиг совершеннолетия в стране проживания, но в любом случае не является лицом моложе 18 лет;
- Пользователь ранее не был заблокирован или ограничен в использовании Сервисов и Услуг ;
- В настоящее время у Пользователя нет учетной записи;
- Пользователь не является пользователем/гражданином/ резидентом из США или стран, которые определены в Приложении 1 и Приложении 2 данной Политики управления рисками;
- Пользователь также не действует от имени и/или в интересах пользователя из США или стран, которые определены в Приложении 1 данной Политики управления рисками;
- Пользователь обладает полной дееспособностью для заключения сделок с использованием Услуг и Сервисов и несет ответственность за свои действия в рамках использования Сайта, Сервисов и их Услуг;
- Пользователь обязуется придерживаться общепринятых норм при общении с сотрудниками и не допускать неприемлемого поведения (хамство, ложь, использование ненормативной лексики, угрозы и запугивание и т.д.) при общении со службой поддержки;
- Пользователь гарантирует, что не будет использовать Сайт, Сервис и его Услуги для незаконных целей или подозрительных операций, в том числе, но не исключительно, для операций

прямо или косвенно связанных с финансирования терроризма, мошенничеством, обманом, коррупцией, обходом санкционных ограничений, DarkNet и иными;

- Информация и данные предоставляемые Пользователем с целью регистрации, а в дальнейшем для пользования Услугами и Сервисами , являются легитимными, актуальными, полными и не вводят в заблуждение;
- Пользователь признаёт и понимает, что является налоговым резидентом и субъектом налогообложения в своей юрисдикции и самостоятельно несет полную ответственность за соблюдение налогового и иного законодательства в своей юрисдикции.

4.8. Допускается использование исключительно одной Учетной записи одним Пользователем. Несанкционированный доступ к Учетной записи другого Пользователя, а также помощь в несанкционированном доступе к Учетным записям других Пользователей строго запрещены.

4.9. Намеренное создание Учетной записи с целью нелегитимного использования/злоупотребления , в том числе с целью осуществления противозаконных операций, как следствие может привести к приостановлению

любых действий, связанных с такой Учетной записью, либо закрытие Учетной записи, включая уведомление компетентных органов и другие действия, согласно требованиям законодательства.

4.10. Пользователь обязуется немедленно уведомить о любом несанкционированном доступе к его Учетной записи, использовании третьим лицом его Учетной записи или пароля, предполагаемой краже его регистрационной информации или любом другом нарушении безопасности в службу поддержки по электронному адресу: info@

4.11. Сервис обязуется уведомлять пользователей о нарушении безопасности пользования Сайтом, Сервисами и их Услугами, включая попытки несанкционированного доступа к Учетной записи, путем отправления сообщений на предоставленный адрес электронной почты и/или номер телефона. В случае изменения электронного адреса и/или номера телефона, Пользователь обязуется уведомить о соответствующих изменениях. Сервис не несет ответственности за причиненный Пользователю ущерб, в случае нарушения пользователем настоящего Соглашения и Политик, в том числе компрометации учетных данных для доступа к Учетной записи, а также бездействия и/или некорректных действий, в случае получения уведомлений о нарушении безопасности.

4.12. Приостановка, прекращение и аннулирование Учетной записи. С целью предотвращения и/или прекращения противозаконных действий имеет право по своему усмотрению приостановить действие Учетной записи и ограничить доступ к Сайту, Сервисам и Услугам; закрыть/заблокировать Учетную запись и средства, которые числятся за ней; приостановить или отменить транзакцию независимо от списания средств с аккаунта у сторонних поставщиков финансовых Услуг, счетах или электронных кошельках.

4.13 имеет право ограничить доступ к Сайту, Сервисам и Услугам помимо прочего, в случае:

- Нарушения настоящего Соглашения, в том числе нарушения обязательств по оплате транзакций, попытке несанкционированного доступа к Сайту или Учетной записи третьего лица, использования нескольких Учетных записей и злоупотребления преимуществами рекламных акций;
- У сервиса есть основания полагать, что целью транзакции является незаконная деятельность (прямо или опосредованно), в том числе, но не исключительно, финансирование терроризма, отмывание денег, мошенничество, коррупция, обман, обход санкционных ограничений и прочее;
- Решения суда или постановления другого компетентного органа, относительно Пользователя или его операций, требующих соответствующих действий со стороны в рамках применимого действующего законодательства;
- Отказа любого стороннего поставщика в предоставлении Пользователю Услуг;

- Форс-мажорных обстоятельств, в том числе эксплуатационных и технических ошибок;
- Если пользователь не осуществлял транзакции в отношении Услуг в течение двенадцати и более месяцев подряд;
- Есть основания полагать, что предоставление Пользователю Услуг будет иметь следствием отрицательное влияние на деловую репутацию ;
- Сервис обоснованно полагает, что ваша Учетная запись связана с любой другой Учетной записью, которая была приостановлена или прекращена за нарушением Соглашения, Политик, или приостановлена по любой другой причине, которая может иметь негативные последствия для Сервиса;
- Пользователь не предоставил информацию по запросу или предоставленная информация не соответствует требованиям ;
- Считает, что Учётная запись Пользователя и/или транзакция не соответствуют допустимым рискам или Политикам .

4.14. В случае приостановки или отмены доступа к Учетной записи, Сайту, Сервисам и их Услугам, в связи с обстоятельствами, предусмотренными настоящим Соглашением или Политиками , имеет право:

(i) отменить невыполненные и/или отложенные ордера на покупку Цифровой валюты;

(ii) удержать любые Фиатные деньги, которые Пользователь заплатил за приобретение Цифровой валюты, но которую Пользователь не получил. Ответственность за последствия в виде удержания средств возлагается исключительно на Пользователя;

(iii) заблокировать все средства, которые находятся на Учетной записи Пользователя;

(iiii) заблокировать, приостановить или прекратить действие Учетной записи Пользователя;

(iiiii) изъять средства, хранящиеся на Учетной записи пользователя, поступившие на нее, а также средства, внесенные им на баланс Учетной записи для проведения транзакции.

4.15. В случае приостановления или прекращения действия Учетной записи Пользователя, а также отмены невыполненных и/или отложенных ордеров, удержании, блокировки или изъятия средств, может предоставить Пользователю уведомление о таком действии.

Сервис не обязан раскрывать информацию, полученную в результате проведения процедур, соответствующим требованиям безопасности , управления рисками и выполнения требования Политик.

4.16. Пользователь может закрыть свою Учетную запись в любое время, отправив запрос на удаление своей Учетной записи на электронный адрес . Плата за удаление Учетной записи не взимается, за исключением выполнения денежных обязательств перед, существующих на дату удаления Учетной записи

Пользователя. Сервис оставляет за собой право приостановить любые незавершенные транзакции в момент отмены. Права Пользователя:

4.17. При утрате доступа к утраченной учетной записи Пользователя (в том числе перенос балансов на новую учетную запись), сервис готов рассмотреть возможность восстановления доступа к такой учетной записи Пользователя (в том числе перенос балансов на новую учетную запись), исключительно при условии предоставления достаточного объема информации и/или подтверждающих документов (объем запрашиваемых документов в каждом случае определяется индивидуально и не является исчерпывающим) о личности Пользователя, истории его транзакций и т.д.

4.18. Пользователь вправе рассчитывать, что будет гарантировать и приложит все возможные усилия и меры, чтобы выполнять такие гарантии на регулярной основе, обеспечение максимального уровня защиты учетной записи, информации о пользователе и его транзакциях со стороны . Выполнение данного пункта со стороны Компании возможно только при надлежащем отношении Пользователя к обеспечению с его стороны сохранности и ограниченного доступа к паролям/учетной записи/транзакциям/документам по транзакциям, при этом потеря доступа через действия/ бездействие Пользователя не является ответственностью Компании и Компания не будет нести любую ответственность по таким событиям. Под “Бездействием” понимается в том числе, но не исключительно, отсутствие установленного пользователем 2FA, что может существенно повышать риск компрометирования логина и пароля и т.д.

4.19. Пользователь имеет право на предоставление качественного Сервиса со стороны и ее представителей при использовании Сайта, Сервисов и их Услуг.

4.20. Пользователь имеет право на квалифицированное и непредвзятое рассмотрения спорных ситуаций со стороны Компании. Для оформления обращения пользователь предоставляет всю необходимую информацию и подтверждающие документы (при наличии) в службу поддержки Компании по электронному адресу: _____

5. Предоставление Услуг

5.1. Сервис Предоставляет Услуги, направленные на приобретение любой доступной Цифровой валюты с помощью Сервисов, а также продажу доступной цифровой валюты, включая цифровую валюту («Цифровая валюта»).

5.2 Также предоставляет Услуги по проведению AML проверок криптовалюты с использованием автоматизированной системы проверки «Выберите Вашего провайдера». Результаты проверки никак не выражают собой отношение к проводимой сделке, а также не являются консультацией, советом, рекомендацией или предложением к заключению или отказу от заключения определенной сделки. Пользователь понимает и подтверждает, что финальное

решение принимается им самостоятельно, вне зависимости от полученных результатов проверки.

5.3. Приобретение Цифровой валюты. Такой вид Услуги позволяет Пользователю покупать Цифровую валюту, доступную на Сайте и через Сервис в момент заключения сделки по приобретению Цифровой валюты.

5.4. Продажа цифровой валюты. Используя Сервисы, Пользователь вправе совершать сделки по продаже Цифровой валюты.

5.5. После успешного создания Учетной записи Пользователя, ему предоставляется возможность совершать сделки по приобретению и продаже Цифровой валюты. Приобретение цифровой валюты осуществляется в обмен на активы, устанавливаемые (доллар США, либо другие валюты) («Фиатные деньги») на основании каждой транзакции.

5.6. Способы оплаты. Пользователь может отправлять и/или получать Фиатные деньги из, посредством оплаты кредитной картой MasterCard/VISA/ или воспользовавшись Сервисами стороннего поставщика платежных решений.

5.7. Гарантии способов оплаты.

Сервис не может гарантировать, что все действующие на данный момент способы оплаты будут всегда доступны для Пользователей. Доступность каждого способа оплаты зависит от нескольких факторов, включая, помимо прочего, местоположение Пользователя, информацию для идентификации, которую он предоставил , и ограничения, налагаемые сторонними платежными системами, если таковые имеются.

5.8. Предоставление цифровой валюты. приложит разумные усилия для

предоставления Пользователю приобретенной Цифровой валюты в кратчайшие разумные сроки, в соответствии с этим Соглашением. Пользователь признаёт, что предоставление ему приобретенной Цифровой валюты может быть выполнено через некоторое время после завершения процесса оплаты, в связи с необходимостью операционной обработки перевода Цифровой валюты. Пользователь также признаёт, что в случаях, предусмотренных настоящим Соглашением, Компания может быть не в состоянии выполнить заказ Пользователя на приобретение или предоставление Пользователю Цифровой валюты.

5.9. Пользователь признаёт, что не несет ответственности за некорректную информацию адреса кошелька Пользователя.

5.10. Нет гарантии стоимости или ликвидности. Пользователь принимает риски, связанные с приобретением и продажей Цифровой валюты, включая тот факт, что не может гарантировать, что любая Цифровая валюта будет иметь в любое время в будущем определенную стоимость (если таковая имеется) или рыночную ликвидность. Сервис не предоставляет гарантии, что Пользователь сможет продать Цифровую валюту третьему лицу через определенное время, и ни при каких условиях не обязуется приобретать у Пользователя любую Цифровую валюту, независимо от того, куплена ли она у или нет.

5.11. В случае совершения ошибочного перевода Цифровых валют на кошельки, принадлежащие иным пользователям, последняя не осуществляет возврат ошибочно отправленных средств. По усмотрению в исключительных случаях возможно рассмотрение вопроса возврата только после обращения в службу поддержки по электронному адресу:

После детального изучения предоставленной информации будет определена возможность или невозможность восстановления/возврата средств пользователю, потерянных/переведенных вследствие ошибочных действий, с последующим уведомлением пользователя по электронной почте.

Комиссия за восстановление и возврат назначается в каждом случае индивидуально. Данное правило также распространяется на Цифровые валюты, которые напрямую не поддерживаются.

6. Цена Цифровой валюты и исполнение транзакции Пользователя

6.1. Цена. Курс, определяющий стоимость продажи и покупки Цифровой валюты, зависит от обстоятельств и обозначается в соответствии с ценой, указанной на Сайте, в Сервисах или в их Услугах. ("Цена").

6.2. Несмотря на вышесказанное, Пользователь соглашается с тем, что любая Цена, отображаемая на Сайте и в Сервисах, на которых Компания продает или покупает Цифровую валюту, является точной только на данный момент, и Цена, которая появляется на Сайте, в Сервисе во время покупки или продажи Цифровой валюты может не быть окончательной ценой или курсом вашей транзакции. Это связано с крайне нестабильным характером стоимости Цифровой валюты и периодом времени, который может потребоваться для завершения транзакции.

6.3. Конечная цена транзакции Пользователя («Конечная цена») будет той ценой, которая указана на Сайте или в Сервисе после завершения операции и доступна для просмотра в личном кабинете.

6.4. Пользователь соглашается с тем, что Конечная цена может быть выше или ниже любого курса или цены, которые ранее были доступны на Сайте и/или в Сервисах, в соответствии с возможными колебаниями стоимости, и что это может измениться либо в пользу Пользователя, или в пользу , и не имеет никакого контроля над такими изменениями.

6.5. Как только это будет практически осуществимо и при условии успешного завершения процесса KYC, выполнит заказ Пользователя по Конечной цене («Исполнение»). До исполнения любой заказ Пользователя будет считаться отложенным и не завершенным и не будет иметь для обязательной силы.

6.6. Предоставление Цифровой валюты. Как только это станет возможным после выполнения заказа Пользователя:

- В случае приобретения Цифровой валюты у сервиса, соответствующая Цифровая валюта будет предоставлена на адрес кошелька Пользователя, с учетом завершения процесса операционной обработки;

- В случае продажи Цифровой валюты, она предоставит Фиатные деньги путём пополнения кредитной карты или другим сторонним платежным процессингом, или другим способом оговоренным при заключение сделки, учитывая данные которые были указаны при оформление заявки в личном кабинете;
- Сервис предоставит Пользователю либо на Сайте, либо в Сервисах по электронной почте или иным образом подтверждение транзакции с указанием Конечной цены и других сведений о приобретении и выполнении транзакции («Подтверждение транзакции»).

6.7. Стоимость Услуги пополнения/вывода с баланса Учетной записи доступна по ссылке.

6.8. Политика отмены. Пользователь признаёт, что выполненные транзакции не подлежат отмене, и Пользователь не может изменить или отменить любую транзакцию — независимо от того, была ли она завершена или находится в состоянии ожидания. Несмотря на вышесказанное, сервис , по своему собственному усмотрению, без каких-либо обязательств может попытаться выполнить запрос Пользователя на отмену транзакции на аккаунте Пользователя.

6.9. Неудачные платежи. Если способ оплаты Пользователя отклонен, будь то из-за недостатка средств, или признан неудачным по какой-либо другой причине, Пользователь соглашается с тем, что по своему собственному усмотрению может:

- Отменить любую применимую транзакцию;
- Выполнить часть этой сделки;
- Дебетовать альтернативные способы оплаты, предоставленные Пользователем, в сумме необходимой для завершения ожидающей транзакции. В случае прекращения любой транзакции, приложит разумные усилия, чтобы уведомить Пользователя о таком прекращении.

6.10. Право собственности на адрес кошелька Пользователя.

В целях выполнения любой транзакции, Пользователь гарантирует использование и предоставление адреса электронного

кошелька, принадлежащего исключительно Пользователю, и который находится под исключительным и полным контролем Пользователя, с которого будет переведена Цифровая валюта.

6.11. Сервис оставляет за собой право отказать в обработке или отменить любую незавершенную транзакцию, если:

- Транзакция является незаконной или в отношении лица, совершающего транзакцию, принято решение суда или другого компетентного органа, обязывающее предпринять соответствующие действия по отмене транзакции;
- Имеет основания предполагать, что транзакция нарушает какое-либо положение настоящего Соглашения;

- Транзакция превышает лимит, который может применяться к количеству или объему транзакций в данный период в соответствии с политикой, в которую

время от времени могут вноситься изменения в соответствии с положениями действующего законодательства;

- Такая транзакция совершается лицом, которое может причинить вред, в том числе деловой репутации Компании.

6.12. Сервис может предпринять любые дополнительные действия, доступные для нее в соответствии с настоящим Соглашением, Политиками или положениями применимого законодательства в отношении такой транзакции.

7. Платежные операции, сторонние процессинги и возвраты платежей

7.1. Пользователь несёт полную ответственность за выплату всех сумм (Фиатные деньги и/или Цифровая валюта), причитающихся сервису. Сервис оставляет за собой право удерживать любой платеж, который должен быть сделан в пользу Пользователя, до тех пор, пока не сможет надлежащим образом идентифицировать и подтвердить подлинность личности Пользователя и/или платежных реквизитов (в зависимости от обстоятельств) согласно Политикам и настоящему Соглашению.

7.2. Сторонние процессинговые Сервисы. Пользователь признаёт, что может, по собственному усмотрению, использовать сторонних поставщиков Услуг для обработки любого платежа между Пользователем и сервисом, включая, помимо прочего, платежи, связанные с использованием Пользователем Услуг и любой выполненной транзакцией. В таких случаях Пользователь подтверждает, что может предоставить личную информацию и/или документацию о Пользователе, в том числе в отношении транзакций, выполненных Пользователем, по мере необходимости для завершения транзакции или, в соответствии с

требованиями, по любому запросу в случае обнаружения мошенничества или подозрения на мошенничество, либо других противозаконных действий.

8. Взаимодействие со службой поддержки

8.1. Сервис готов к конструктивной критике и понимает важность человеческого фактора в обслуживании Пользователей и стремиться предоставить качественный Сервис своим Пользователям. Сервис готов обеспечить беспристрастное рассмотрение обращений и жалоб по спорным ситуациям, но важным элементом такого рассмотрения является взаимное уважение. Сервис обеспечивает безопасность транзакций не только наших Пользователей, но и безопасность и надлежащие условия работы службы поддержки.

8.2. В процессе обслуживания Пользователей могут возникнуть ситуации, которые требуют более детального изучения структуры расчетов в порядке, предусмотренном применимым законодательством и/или Политиками . Сервис понимает, что задержка в проведении операции может вызвать негативные

эмоции у Пользователей, но обязана убедиться в легитимности каждой транзакции. Несоответствие оперативности работы службы поддержки или сроков рассмотрения деталей транзакции службой комплаенс ожиданиям

Пользователя не является основанием для угроз, негатива и агрессии в адрес сотрудника службы поддержки.

8.3. При проявлении агрессии в отношении сотрудника , оставляет за собой право временной блокировки Пользователя и/или его учетной записи на не определенный период времени. Срок блокировки определяет по своему усмотрению и зависит от каждой ситуации отдельно. В течение этого времени заблокированный Пользователь не может общаться со службой поддержки и получить доступ к своей учетной записи.

8.4. Мы следим за тем, чтобы Пользователи не блокировались без веской причины. Если Пользователь считает, что ему предоставлена неквалифицированная Услуга поддержки, Сервис рекомендует Пользователю прекратить текущий чат и направить соответствующее уведомление посредством электронной почты в адрес службы поддержки (электронный адрес:) с указанием в теме сообщения ID учетной записи, а в теле сообщения указать жалобу на действия сотрудника, в которой изложить свою версию событий. рассматривает все жалобы и предоставляет обратную связь на такие обращения.

9. Интеллектуальная собственность Компании

9.1. Тексты, графические изображения, цветовое наполнение и прочие элементы, которые используются на Сайте и в Сервисах, защищаются авторским правом. Содержание Сайта и Сервисов является интеллектуальной собственностью и защищается действующим законодательством.

9.2. Использование объектов интеллектуальной собственности возможно только при условии личного и некоммерческого использования, с указанием источника () и по предварительному письменному согласию .

9.3. Любые незаконные действия в отношении прав интеллектуальной собственности приведут к привлечению виновных лиц к ответственности, согласно действующему законодательству. Сервис оставляет за собой право проводить расследование с целью уведомления компетентных органов о лицах и действиях, нарушающих требования законодательства, согласно действующего законодательства.

10. **Соответствие использования Сайта, Сервисов и их Услуг требованиям законодательства**

10.1. Пользователь является лицом, которое несет исключительную юридическую ответственность за использование Сайта, Сервисов и их Услуг в случае, если согласно применимому к Пользователю законодательству, использование Сайта, Сервисов и их Услуг является противозаконным.

10.2. В случае, если у Сервиса есть основания полагать, что использование Пользователем Сайта, Сервисов и их Услуг противоречит требованиям

применимого законодательства, в том числе это может быть связано с запрещенными видами деятельности, может приостановить или отказать в предоставлении Пользователю Услуг без уведомления о причинах отказа.

10.3. Применимые налоги. Пользователь несет исключительную ответственность за оплату налогов и сборов, применимых к его транзакциям на Сайте, согласно применимому к нему законодательству. Сервисе не предоставляет юридических разъяснений или консультаций в связи с взиманием налогов и сборов.

10.4. В своей деятельности придерживается применимого законодательства и лучших международных стандартов и практик, и ожидает от Пользователя выполнения данных Условий и Политик. Внутренние документы по управлению рисками AML/CTF и процедурам KYC/CDD разрабатываются дополнительно и являются внутренними документами с ограниченным доступом. Такие документы соответствуют данному Соглашению и Политикам.

11. Недействительность отдельных положений Соглашения

11.1. В случае недействительности любых отдельных положений настоящего Соглашения по любым причинам, остальные положения Соглашения остаются действительными и имеют юридическую силу.

12. Ограничение ответственности

12.1. Насколько это позволено действующим законодательством, ни Сервис , ни ее аффилированные лица не несут ответственности за любой ущерб в связи с использованием Пользователем Сайта и Сервисов.

12.2. Использование любой информации, полученной с Сайта или посредством использования Сайта и Сервисов, осуществляется исключительно под ответственность Пользователя. Сервис насколько это позволено действующим законодательством, отказывается от любой ответственности относительно решений, принимаемых Пользователем на основании информации, полученной с Сайта или посредством использования Сайта и Сервисов.

12.3.Сервис не гарантирует операционную и функциональную поддержку Сайта и Сервисов. Насколько это допустимо действующим законодательством, отказывается от ответственности в случае любого дефекта или недоступности Сайта, Сервисов и их Услуг и/или их Содержания, или в случае другого прямого или непрямого ущерба, возникшего в связи с доступом к Сайту, Сервисом или их использованием. не несет ответственности за причинение любого ущерба, обусловленного перерывами в работе Сервисов, техническими ошибками, вредоносными программами или файлами, а также другими факторами вне контроля .

12.4. Сервис не несет ответственность за неполучение Пользователем приобретенной Цифровой валюты, Фиатных денег в случае предоставления Пользователем некорректной информации относительно виртуального

кошелька, публичного ключа, платежных реквизитов или отказа проводить операцию третьими лицами (банками/провайдерами и т.д.) и прочее.

13. Правопреемники/передача информации третьим лицам

13.1 В случае слияния или разделения, Сервис имеет право передавать или переуступать информацию, предоставленную Пользователями в рамках действующего законодательства. имеет право передавать информацию, предоставленную Пользователями, третьим лицам исключительно в случаях, предусмотренных действующим законодательством, а также для предоставления Пользователям Услуг и Сервисов, предлагаемых в пределах, регулируемых Соглашением, Политиками и действующим законодательством.

14. Применимое законодательство и юрисдикция

14.1. Используя Сайт и Сервис, Пользователь соглашается с настоящим Соглашением.

14.2. Любые споры, возникающие между и Пользователями, должны решаться путем переговоров с соблюдением досудебного порядка решения споров. В случае невозможности достижения согласия путем переговоров, спор передается в компетентный суд, расположенный место юридической регистрации сервиса. Стороны обязуются сохранять конфиденциальность всех вопросов относительно судебных тяжб.

15. Форс-мажорные обстоятельства

15.1. Сервис не несет ответственности за задержки, сбои в работе или прерывание обслуживания, которые прямо или косвенно связаны с любой причиной или условием, находящимся за пределами разумного контроля , включая, помимо прочего, любую задержку или отказ в

результате какого-либо стихийного бедствия, катастроф, террористических актов, гражданских беспорядков, войн, забастовок, пожаров, решений уполномоченных государственных органов, перерывов в телекоммуникациях или Услугах сетевых провайдеров, отказа оборудования и/или программного обеспечения, или других событий, выходящих за рамки разумного контроля и влияющих на работу Сайта, Сервисов и предоставление Услуг.

16. Связаться с Компанией

16.1. Если у Пользователя есть любые вопросы, комментарии, отзывы, жалобы относительно настоящего Соглашения, Пользователь может связаться со через службу поддержки по электронному адресу.

Приложение №1
К Пользовательскому соглашению
Политика AML

Сервис предостерегает Клиентов от попыток использования сервиса в целях легализации денежных средств, полученных преступным путем, покупки запрещённых товаров и услуг, финансирования терроризма, мошенничества и любых других незаконных действий. Также сервис предостерегает Клиентов от попыток сокрытия информации, связывающей их с физическими и юридическими лицами, организациями или странами, включенными в санкционные списки РФ.

Документ политики управления рисками (далее по тексту «Политика» или «Политика AML») устанавливает системы контроля и механизмов для предотвращения вовлечения компании, услуг и сервисов в отмывание денег, деятельность по финансированию терроризма и ситуации нарушения установленных санкционных ограничений. Политика также определяет правила для сохранения и поддержания репутации сервиса при взаимодействии с Клиентами, контрагентами и представителями уполномоченных органов.

Согласно Политике, слова «сайт сервиса», «мы», «нам» или «наш» относятся к сервису, включая всех сотрудников и других относящихся к ней лиц. В зависимости от контекста, «сервис» может также относиться к услугам, товарам, веб-сайту, контенту или другим предоставляемым сервисом материалам. Политика является неотъемлемой частью Условий Пользования. Принимая Условия Пользования, Клиент автоматически соглашается с данной Политикой.

Перед использованием сайта или любого иного сервиса или услуги, предлагаемых на сайте сервиса, Клиент должен внимательно прочитать

эту Политику. В случае несогласия с каким-либо из пунктов настоящей Политики, сервис просит Пользователя отказаться от использования данного сайта и его сервисов и услуг.

1. Понятия и определения

Все термины, указанные в настоящей Политике AML заглавными буквами и не имеющие иных определений, имеют те же значения, что и в Условиях Пользования.

Определения

Термины, прописанные заглавными буквами в настоящей Политике, имеют значения, указанные в данном параграфе.

клиринговые или расчетные системы, либо аналогичные соглашения, которые используются для предоставления Сервиса/Услуг.

Внутренние контрольные механизмы и политики - Создание надежных внутренних контрольных механизмов и политик для обеспечения соответствия требованиям AML/CFT.

Знай Своего Клиента (KYC) - комплекс мероприятий и процедур, направленных на получение информации о Пользователе и его деятельности с целью управления рисками компании.

Запрещенное поведение — мошенничество, коррупция, отмывание денег, сговор, финансирование терроризма и любое другое преступное и незаконное поведение.

Коррупция — прямое или косвенное предложение, ходатайство, предоставление или получение чего-либо ценного с целью оказать ненадлежащее влияние на действия другой стороны.

Клиент (Пользователь) — физическое лицо, посещающее сайт сервиса и/или использующее его услуги для получения доступа к функционалу, являющееся субъектом данных и/или Клиентом.

Красные флаги - предупреждения или индикаторы, предполагающие наличие потенциальной проблемы или угрозы с операциями Пользователя, которые проходят через сервис и/или Услугу, Сайт или сервис.

Легализация средств, полученных преступным путем — сокрытие незаконного источника денежных средств путем перевода их в законно выглядящие денежные средства или инвестиции.

Мошенничество — обман с целью преследования личных интересов и нанесения ущерба интересам Пользователей и/или сервиса путем хищения чужого имущества либо приобретения на него права обманным путем.

Мониторинг транзакций - это применение комплексных систем для отслеживания транзакций с целью выявления необычной или подозрительной активности. Транзакции, выделяющиеся своими значительными суммами и отклоняющиеся от обычного поведения клиента, могут стать объектом дополнительного расследования.

Надлежащая комплексная проверка Клиентов (CDD) - проверка данных/информации о Пользователе и другие проверки, связанные с изучением Пользователя и его деятельности. Проводятся с целью комплексной оценки риска Пользователя при принятии и/или во время его обслуживания.

Нормативные требования - любой применимый закон, статут, постановление, приказ, судебное решение, решение, рекомендацию, правило, политику (в том числе, но не исключительно Политику AML) или руководство. Должны быть приняты или изданы парламентом, правительством, любым компетентным судом, органом власти, любой платежной системой. Это включает в себя банковские платежные системы, карточные платежные системы или любые другие платежные, клиринговые или расчетные системы, либо аналогичные соглашения, которые используются для предоставления Сервиса/Услуг.

Обман — в контексте данного договора способ мошенничества для получения денег от пользователей интернета. Может включать в себя сокрытие информации

или предоставление неверной информации с целью вымогательства у жертв денег, имущества и наследства.

Отмывание денег — схема финансовых транзакций, целью которой является сокрытие личности, источника и места назначения незаконно полученных денег или финансирование незаконной деятельности.

Оценка риска - периодическое проведение и актуализация анализа рисков с целью выявления и снижения возможных рисков в области противодействия отмыванию денег и финансированию терроризма, связанных с клиентами и географическими областями.

Обучение по предотвращению отмывания денег (ПОД) - представляет собой образовательную программу, предоставляемую сотрудникам с целью улучшения их осведомленности о политиках и процедурах в области предотвращения отмывания денег. Кроме того, данная программа направлена на повышение понимания сотрудниками важности соблюдения требований, направленных на предотвращение отмывания денег и финансовых преступлений.

Периодический мониторинг - это процесс обновления данных о клиентах и проведение систематических обзоров их профилей.

Противодействие отмыванию денег (AML) - комплекс мероприятий и процедур, направленных на выявление и/или предотвращение использования сайта, сервисов и/или услуг, предоставляемых сервисом, в целях отмывания денег.

Противодействие финансированию терроризма (CTF) - комплекс мероприятий и процедур, направленных на выявление и/или предотвращение использования сайта, сервисов и/или услуг, предоставляемых сервисом, в целях финансирования терроризма.

Противодействие отмыванию денег (ПОД) - включает в себя систему мероприятий, законодательных актов и нормативов, направленных на предотвращение и выявление незаконных действий, связанных с трансформацией незаконно нажитых средств с целью придания им легального облика.

Процедура "Знай своего клиента" (Know Your Customer/Client, KYC) - представляет собой систему, которую компания внедряет с целью проверки и идентификации своих клиентов. Процесс направлен на обеспечение наличия достаточной информации для полного понимания характера деятельности клиента и снижения риска отмывания денег.

Политически значимое лицо (PEP) - физическое лицо, играющее выдающуюся общественную роль на международном уровне или внутри страны.

Сайт - Веб-сайт, предоставляемый сервисом.

Сговор - договоренность между двумя или более сторонами, направленная на достижение ненадлежащей цели, включая неправомерное влияние на действия другой стороны.

Санкции (экономические санкции) - коммерческие и финансовые санкции, применяемые одной или несколькими странами против целевых самоуправляющихся государств, групп или отдельных лиц.

Скрининг санкций - это процедура, при которой физические лица, юридические структуры или финансовые операции анализируются на соответствие перечням санкций или спискам ограниченных лиц, предоставленным правительствами. Этот процесс направлен на обеспечение соответствия международным санкциям.

Усиленная проверка клиента (EDD) - представляет собой применение более строгих мер для клиентов или операций, связанных с высоким риском. Этот процесс включает более подробный анализ финансовой истории клиента, происхождения его состояния, а также непрерывный мониторинг его транзакций.

Финансирование терроризма - предоставление или сбор средств любыми способами, прямо или косвенно, с намерением их использования или при условии, что они будут использоваться полностью или частично для осуществления любого из преступлений, связанных с терроризмом.

2. Общие Положения

Деятельность сервиса, а также порядок взаимодействия сервиса и его клиентов регулируются Политиками, их положениями, соглашениями, в том числе, но не исключительно, Политикой управления рисками, Политикой конфиденциальности и тому подобные документы.

2.1. Для предоставления надлежащего и своевременного уровня услуг и сервиса Клиентам, сервис и его Клиенты обязаны соблюдать требования, содержащиеся во внутренних и международных законах о предотвращении отмывания денег и финансирования терроризма. А также требования других законов и нормативных актов в той степени, в которой они связаны с деятельностью сервиса.

2.2. Для выполнения процедур, предусмотренных данной Политикой, сервис разрабатывает и внедряет внутреннюю систему оценки уровня рисков Клиента и их операций. Также он определяет минимально необходимый набор требований, процедур, механизмов, отчетов, систем и мер контроля для управления рисками сервиса. Для Клиентов и операций с высоким риском применяются более жесткие процедуры.

2.3. Сервис может вносить изменения и дополнения в Политику по своему усмотрению в одностороннем порядке по мере выявления и идентификации новых рисков, внедрению новых продуктов/услуг/сервисов и их изменений в

применимом законодательстве. А также осуществлять контроль за соблюдением ее положений и требований.

3. Процедуры KYC

3.1. Сервис проводит процедуру проверки KYC, чтобы избежать риска привлечения к ответственности за нарушение применимого законодательства. А также, чтобы защитить себя от попыток использовать сервис и/или его услуги для осуществления незаконных действий.

3.2.В рамках процедур KYC сервис:

3.2.1. Устанавливает личность Клиента — изучает Клиента при установлении отношений и уточняет информацию о нем во время обслуживания.

Сервис выполняет процедуры идентификации, относящиеся к Клиенту:

а) при установлении отношений;

б) ежегодно для Клиентов с высоким риском, раз в два года для Клиентов со средним риском, раз в три года для Клиентов с низким риском;

3.2.2. Изучает характер деятельности Клиента — транзакции Клиента, чтобы оценить риски отмывания денег, связанные с этим Клиентом. Основная цель — убедиться, что источник средств является законным;

3.2.3. Собирает и хранит информацию о Клиентах, результатах их изучения, а также о существенных фактах, касающихся существующих и потенциальных Клиентов и их транзакций.

3.3. В целях идентификации Клиентов сервис может запрашивать следующие документы:

Контактную информацию:

- Никнейм в мессенджере (Telegram);
- Номер телефона;
- Адрес электронной почты.

Документы, удостоверяющие личность:

- Внутренний и/или заграничный паспорт;
- Удостоверение личности, ID карта;
- Водительское удостоверение.

Документы, подтверждающие адрес проживания/регистрации:

- Копия счета за коммунальные услуги;
- Копия счета за телефон;
- Копия счета за электричество;
- Выписка из банка.

Другие документы при необходимости.

3.4. Надлежащая комплексная проверка Клиентов.

В процессе изучения Клиентов сервис может выполнять три уровня проверки:

Упрощенная надлежащая комплексная проверка («SDD»): ситуации, когда риск отмывания денег или финансирования терроризма низок и полная проверка не требуется.

Пример: аккаунты с низкими оборотами и суммами транзакций.

Базовая надлежащая комплексная проверка Клиентов («CDD»): информация, полученная от всех Клиентов для проверки личности Клиента и оценки рисков, связанных с этим Клиентом.

Расширенная надлежащая комплексная проверка («EDD»): дополнительная информация, собираемая о Клиентах с более высоким уровнем риска для более глубокого понимания деятельности таких Клиентов и для снижения связанных с ними рисков.

3.5. Установление отношений с PEP происходит только по согласованию с Менеджментом сервиса. Таким Клиентам устанавливается высокий риск и применяется процедура EDD.

3.6. После проведения процедур идентификации, относящихся к Клиенту, сервис сохраняет информацию, полученную в файле этого Клиента.

4. Выявление и обнаружение подозрительных действий

4.1. Любая финансовая операция, которая может быть связана с отмыванием денег, финансированием терроризма, нарушением санкционных ограничений, обманом считается подозрительной.

4.2. Сервис самостоятельно разрабатывает и внедряет механизм выявления таких операций, систему и критерии определения Red flags, а также критерии оценки рисков. Основанием для определения того, что конкретная транзакция является подозрительной, могут быть личные наблюдения и опыт сотрудников сервиса, информация, полученная во время процедур KYC, информация, полученная с применением специализированных аналитических программ и/или систем, и другие источники.

4.3. Сервис на регулярной основе отслеживает транзакционную деятельность своих Клиентов. Он обновляет системы и критерии Red flags, используемые для обнаружения подозрительных действий, и внедряет лучшие международные практики для выявления таких операций.

4.4.В соответствии с применимыми действующими законами и требованиями компетентных международных организаций, сервис может уведомлять регулирующие и/или правоохранительные органы о любых подозрительных операциях, а также предоставлять необходимую информацию в ответ на запросы таких организаций. Сервис может действовать там, где это уместно, и без обязательства получения одобрения или уведомления Клиента.

4.5. При проведении изучения Клиентов и анализа их операций сервис использует следующие списки:

Санкционных лиц, известных террористов и/или террористических организаций, а также лиц, подозреваемых в террористической деятельности.

Списки должны быть опубликованы местными властями и международными организациями: OFAC (Office of Foreign Assets Control), ЕС, ООН и т.д.;

Юрисдикций, которые не обеспечивают достаточный уровень процедур по борьбе с отмыванием денег.

Это определяется в соответствии с политиками FATF, а также странами, на которые распространяются санкции OFAC, ЕС, ООН и других международных организаций;

Стран с высоким уровнем риска, указанных в Приложении 1. Это необходимо для определения того, включен ли Клиент сервиса или потенциальный Клиент и/или его страны или юрисдикции в вышеуказанные списки, сотрудничество с которыми запрещено или нежелательно.

4.6. Сервис постоянно проводит проверку своих Клиентов и проверяет их транзакции, чтобы обеспечить совместимость этих транзакций с данными сервиса о своих Клиентах, их бизнесе и, при необходимости, их источнике доходов.

4.7.Сервис не устанавливает отношения с Клиентами, которые внесены в санкционные списки, зарегистрированы/расположены на территориях/юрисдикциях, указанных в п. 4.5., или находятся под контролем таких лиц.

4.8.При установлении у Клиента статуса неприемлемо высокого риска сервис может отказать такому Клиенту в дальнейшем обслуживании.

4.9.Сервис также сохраняет за собой право запрашивать у Клиента дополнительные документы, приостанавливать или прекращать действие аккаунта Клиента, приостанавливать оборот или замораживать активы Клиента при обнаружении подозрительных операций. Приостановка длится до выяснения обстоятельств и иных действий, соизмеримых с выявленными рисками.

5. Третьи стороны

5.1. Для выполнения некоторых функций сервис может привлекать сторонних поставщиков услуг или взаимодействовать с контрагентами. Сервис прикладывает всевозможные усилия, чтобы изучить такого поставщика услуг/контрагента и его деятельность, а также определить, насколько это возможно, его репутацию (например, наличие инициированных расследований и исков против таких сторонних поставщиков услуг). Сервис также определяет, получил ли сторонний поставщик все необходимые лицензии, разрешения и одобрения, прежде чем устанавливать деловые отношения.

5.2. Сервис не устанавливает отношения с поставщиком услуг и/или контрагентом, который внесен в санкционные списки или

зарегистрирован/расположен на территориях/юрисдикциях, указанных в п. 4.5., или который находится под контролем таких лиц.

6. Обучение сотрудников и представителей

6.1. Сервис предпринимает все возможные меры по обучению сотрудников, чтобы не допустить вовлечения сервиса в действия, направленные на использование его услуг в целях отмывания средств, финансирования терроризма, мошенничества или нарушения установленных санкционных ограничений.

6.2. Касательно собственного персонала, сервис предпринимает все возможные меры для тщательного анализа всех кандидатов на работу с целью определить, подпадает ли деятельность и/или репутация нового сотрудника в категорию, которая подвержена или несет риски отмывания денег.

7. Отчетность о подозрительных транзакциях и рисковых Клиентах

Сервис разрабатывает и внедряет внутреннюю отчетность, которая позволяет получать своевременную информацию о рисках и их управлении. Если сотруднику сервиса стало известно о деятельности, которая попадает под ограничения, указанные в Политике, сотрудник должен незамедлительно уведомить о событии и предоставить всю необходимую имеющуюся информацию своему руководителю и/или уполномоченному подразделению (комплаенс) и/или высшему руководству сервиса.

8. Пользовательское соглашение

8.1. Используя услуги сервиса, Клиент гарантирует, что не собирается совершать какие-либо запрещенные действия, описанные в данном документе. Кроме того, Клиент соглашается на любые проверки, связанные с проведением расследования в соответствии с данной Политикой, и соглашается полностью и оперативно сотрудничать с уполномоченными представителями сервиса в рамках такого расследования. Отказ от сотрудничества или непредставление необходимых сведений/документов может послужить основанием для приостановления или отказа от обслуживания Клиента.

9. Ответственный за соблюдение Политики

Ответственный за соблюдение Политики сотрудник должен проводить следующие процедуры:

- Сбор идентификационной информации Пользователей и передача ее ответственному агенту по обработке персональных данных;
- Создание и регулярное обновление внутренних политик и процедур, требуемых в соответствии с существующими законами и правилами;
- Мониторинг транзакций и анализ любых существенных отклонений от нормальной деятельности Пользователей;

- При необходимости, инициирование взаимодействия с государственными и правоохранительными органами в сфере противодействия легализации денежных средств, отмывания денег, финансирования терроризма и мошенничества.

10. Заключительные положения

10.1. Настоящая программа утверждена в порядке, предусмотренном сервисом, и одобрена его Менеджментом.

10.2. Настоящая Политика вступает в силу с момента утверждения и/или опубликования на сайте сервиса.

10.3. Настоящая Политика находится в открытом доступе на сайте в актуальной редакции. Сервис сохраняет за собой право вносить изменения в данную Политику в одностороннем порядке.

Приложение 2
к Пользовательскому соглашению
Перечень стран

Перечень стран/юрисдикций и территорий, сотрудничество с которыми запрещено в связи с высоким уровнем риска или по иным причинам:

1. American Samoa
2. Afghanistan
3. Bahamas
4. Botswana
5. Burma
6. Ethiopia
7. Crimea
8. Cuba
9. Canada
10. Republic of Ghana
11. Island Guam
12. Iran
13. Iraq
14. Yemen
15. Libya
16. Malaysia
17. Nigeria
18. Republic of Nicaragua
19. Singapore
20. North Korea
21. Pakistan
22. Panama
23. Puerto Rico
24. Sri Lanka
25. Somali
26. Saudi Arabia
27. United States of America
28. Republic of South Sudan
29. Republic of Sudan
30. Syria
31. Republic of Trinidad and Tobago
32. Transnistria, Pridnestrovian Moldavian Republic (PMR)
33. Tunisia Virgin Islands
34. Bolivarian Republic of Venezuela
35. Republic of Artsakh

В операционную работу обменного бизнеса входит организация, распределение, конвертация денежного или имущественного потока, выраженного в криптовалюте — это операционная часть бизнеса, следовательно внутренняя политика AML должна контролировать, упреждать, и подтверждать её.

Пример содержания такой политики:

1. Цели и задачи политики

- Предотвращение использования платформы для отмывания денег и финансирования терроризма.
- Обеспечение соответствия местному и международному законодательству.
- Защита репутации компании и повышение доверия клиентов.

2. Программа "Знай своего клиента" (KYC)

- Обязательная идентификация клиентов:
  - Сбор личных данных, включая имя, дату рождения, адрес, контактную информацию.
  - Проверка документов (паспорт, водительское удостоверение, ID-карта).
  - Верификация адреса проживания (счет за коммунальные услуги, выписка из банка).
- Риск-профилирование клиентов:
  - Оценка риска клиента на основании происхождения средств, юрисдикции, истории транзакций.
  - Отнесение клиентов к категориям: низкий, средний или высокий риск.

3. Анализ и мониторинг транзакций (KYT - "Знай свою транзакцию")

- Использование автоматизированных инструментов анализа блокчейна для отслеживания движения средств.
- Проверка транзакций на соответствие нормам и выявление подозрительных операций:
  - Операции с крупными суммами.
  - Раздробленные транзакции (structuring/smurfing).
  - Переводы на адреса, связанные с "черными списками" (санкции, даркнет, взломы).

4. Подозрительные операции

- Признаки подозрительных операций:
  - Частые переводы на одни и те же адреса.

- Операции через офшорные счета.
- Отказ клиента предоставлять информацию.

● Процедура реагирования:

- Временная блокировка аккаунта.
- Направление отчета о подозрительных операциях (STR) в компетентные органы.

5. Обучение сотрудников

● Регулярные тренинги по AML/KYC и текущим методам отмывания денег.
● Ознакомление с современными инструментами анализа криптовалют.
● Постоянное обновление знаний в соответствии с новыми законодательными требованиями.

6. Хранение данных

● Срок хранения данных о клиентах и транзакциях — минимум 5 лет.
● Защита данных от утечек и несанкционированного доступа.

7. Взаимодействие с органами власти

● Сотрудничество с регуляторами, правоохранительными органами и финансовыми разведками (например, FINTRAC, FATF, Росфинмониторинг).
● Предоставление запрашиваемой информации в рамках расследований.

Пример инструментов для реализации:

1) Chainalysis или Elliptic для анализа блокчейна.
2) Sumsub или Onfido для верификации пользователей.
3) Автоматические системы мониторинга транзакций (например, AMLBot).

Так как для каждой компании внутренняя политика AML является разной, отдельным текстом также будут включены далее дополнительные аспекты, которые должны/могут быть отражены внутри документа.

Внутренняя AML политика должна быть адаптирована к конкретной юрисдикции и законодательным требованиям, чтобы она был эффективным и юридически обоснованной. (Каждая страна создаёт собственные нормы в ключе, например, взаимодействия платформы и государственных органов.)

Для внутреннего пользования должны быть отражены ответственные лица и порядок практического применения используемых норм. Например, на территории страны регистрации стоит требования к определённой форме отчётности, в её отражении нет необходимости для клиента, но есть для внутреннего пользования. Или принцип разумной оценки рисков и рискованных транзакций. Этого достаточно для клиента, но внутри компании

будут раскрыты рамки, которые фиксируются компанией в качестве разумных мер и подходов к оценке рисков и рискованных транзакций.

Должна быть отражена структура компании, ответственные сотрудники, принципы их работы и их контакты. Фиксируется иерархия подчинения и порядка взаимодействия сотрудников, их подходы к работе, определяемые внешними (законодательными) требованиями и компанией.

Фиксируются обязательства управляющих лиц. Например, комплаенс офицер, его полномочия и порядок взаимодействия с обращениями клиентов.

Внутри структуры документа также необходимо отразить то, как компания видит и применяет требования KYC/KYB, а также порядок проведения проверок Due Diligence (DD). Что компания расценивает как транзакции/клиенты, к которым требуются повышенные или дополнительные меры DD (Enhanced DD, Additional DD и иные). Какие идентификационные данные собирает компания, а также порядок их хранения компанией и опции их отзыва клиентами платформы или видоизменения.

Для внутреннего пользования документ должен включать реальные процедуры и технические решения, которые осуществляют все меры, перечисленные выше.

Также необходим отдельный раздел исключительно для внутреннего пользования раскрывающий порядок обучения персонала, найма и работы внутренней системы сотрудников компании.

Обозначенные условия – являются основными для любой, даже самой простой AML политики.

Глава 4. Техническо-операционная работа по AML.

Здесь будут описаны, шаги, методы, инструменты, необходимые для выполнения норм AML/KYC.

Технические настройки it-ландшафта с точки зрения норм AML и практики.

Учитывая высказанную ранее информацию нам необходимо довести уровень технического обеспечения защитного AML-барьера до высоких стандартов, заданных теорией нашей рекомендации, разберем необходимые аспекты, с примерами применяемых программ, модулей, решений, разделим описания на части:

1. Выбор хостинга.
2. Организация работы сайта/программного обеспечения +внедрения модуля автоматизированной проверки персональных данных ваших клиентов.
3. Внедрения модуля автоматизированной проверки входящих транзакций, построение “риск-аппетита”.
4. Последующая операционная работа.

4.1 Выбор хостинга.

При выборе хостинга необходимо учитывать несколько ключевых аспектов, а именно обеспечение конфиденциальности данных, надежность инфраструктуры и соответствие требованиям регуляторов, а также геопозиционирования своего продукта или бизнеса.

4.1.1 Регулирование и юрисдикция

Выбор страны, в которой будет размещен хостинг, имеет важное значение для соблюдения требований законодательства о защите данных и финансовом мониторинге.

- **ЕС (GDPR/MiCA)**: Если ваши клиенты находятся в Европе или ваши бизнес-решения связаны с финансовыми учреждениями в ЕС, выбирайте хостинг-провайдеров, соответствующих **GDPR, MiCA,**
- **США**: Если вы ориентированы на рынок США, важно, чтобы хостинг соответствовал **FATF** и **SEC** требованиям, а также местным правилам хранения персональных данных ваших пользователей.
- **Россия**: Если вы работаете с российскими клиентами или организациями, хостинг должен соответствовать требованиям **ФЗ-115**, **152-ФЗ (о персональных данных)** и требованиям(будущим требованиям) ЦБ РФ.

4.1.2 Рекомендуемые хостинг провайдеры:

- Германия (Hetzner, IONOS)
- США (AWS, DigitalOcean, Vultr)
- Россия (Selectel, VK Cloud, Yandex Cloud)

4.1.3 Важный аспект по серверу.

Стоит отметить более подробно, что, используя хостинг той или иной страны по правовой логике некоторых государств это равносильно осуществлению работы на территории той юрисдикции, где у вас расположен хостинг, а следовательно, возникает дополнительная ответственность перед властями той или иной страны.

То есть при аренде хостинга на территории США, вы обязаны выполнять американский финансовый compliance, и в случае совершения преступления вы также будете отвечать перед их законом, даже если вы находитесь в другой юрисдикции, ваша компания не является американской, а сами вы не резидент США и не работаете с гражданами США, отсюда следует что подход к выбору хостинга (сервера) необходимо осуществлять максимально продуманно.

4.1.4 Безопасность

Для хостинга обрабатывающего финансовую и персональную информацию критически важно обеспечить высокий уровень безопасности, обычно это одно из требований регулятора, но и так же обусловлено тем, что преступники нацелены на крипто-проекты так как, хакерская атака против подобного бизнеса практически всегда обеспечивает быстрый доступ к финансам, в новостях то и дело всплывают сообщения о взломе и потере миллионов долларов в криптовалюте.

Стандартные требования к безопасности хостинг провайдера:

- SSL-сертификаты (для шифрования соединений)
- DDoS-защита (чтобы избежать атак)
- Файрволы и антивирусные решения
- Поддержка VPN, SSH, и двухфакторной аутентификации
- ISO 27001:2022 сертификация хостинга

Поддержка резервного копирования и отказоустойчивость. Обычно самые именитые и дорогие хостинги предлагают данные функции по умолчанию, но все же лучше уточнять заранее используется ли подобный или аналогичный

набор мер для защиты ваших данных. После выбора хостинга мы можем перейти к следующему пункту.

4.2 Организация работы сайта/программного обеспечения

Как правильно организовать работу по данному блоку, соблюдая все требования, после выбора хостинга мы поняли, что вам необходимо будет соответствовать локальному финансовому праву, требованиям вашего регулятора, дополнительным нормам должной осмотрительности, ваши сервисы по умолчанию должны собирать согласие на обработку персональных данных, согласие с вашими правилами работы, а также с АМЛ политикой. В унифицированный модели ваш бизнес проект должен собирать и надежно хранить следующие данные:

1.KYC (персональные данные, документы, биометрию, данные связанные с интернет идентификацией, почта, номер телефона.
2.IP address.
3.User Agent, cookies.
4.Геолокацию, часовой пояс.
5.Действия, осуществляемые пользователем при использование вашего проекта.
6. Историю производимых операций, связанные адреса кошельков, ордера сделок, обсуждение деталей сделок.
7. AML-оценку транзакций.

4.2.1 Уровни KYC. Остановимся и распишем важные пункты KYC — как мы знаем проведение процедуры является обязательным в рамках исполнений требования регуляторов, а также исполнения правила должной осмотрительности. KYC можно градировать по уровням защиты:

Уровень 0 — нет защиты, самый рисковый уровень - вы не собираете никакие персональные данные, не проводите никаких верификаций, коллекционируете указанный пользователем почтовый ящик не валидируя его, произведенную операцию пользователем, аккаунт в мессенджере, из ценных данных собираете исключительно ip адрес, подобная работа осуществляется исключительно на свой страх и риск и по мнению законодательств многих юрисдикцией данный тип работы является преступным.

Уровень 1 — есть некая защита, рисковый уровень - вы собираете данные с уровня 0, а также обязуете пользователя создавать аккаунт, который связывается с данными интернет-идентификации, почта, номер телефона, а также проводите

их валидацию отправкой кода проверки, подобная работа осуществляется исключительно на свой страх и риск и по мнению законодательств многих юрисдикцией является преступной.

Уровень 2 — есть допустимая защита, средне рисковый уровень - вы собираете данные с уровня 0-1, а также собираете документы пользователя, проводите сбор биометрии и надлежащим образом это сохраняете.

Уровень 3 — есть приемлемая защита, минимально рисковый уровень - вы собираете данные с уровня 0-1-2, дополнительно проводите процедуру KYC в режиме реального времени валидируя документы, собираете актуальный источник проживания, градируете пользователей по риск-категориям, устанавливаете лимиты ограничивающие деятельность физ аккаунтов при наступление которых, предлагаете проходить KYB или запрашиваете источник происхождения средств, обновляете KYC, в некий установленный период.

Уровень 4 — есть максимальная защита минимально рисковый уровень - вы собираете данные и проводите мероприятия соответствующие уровню 0-1-2-3, а также проводите расширенные мероприятия по идентификации ваших клиентов с применением OSINT и других источников информации для выявления рисковых паттернов в его поведение вне вашей платформы.

Данные уровни не являются исчерпывающими или обязательными к исполнению, бизнесмен должен руководствоваться здравым смыслом, требованием регулятора, а также анализом современных угроз, и не забывать про мнение своего АМЛ офицера.

Помимо сбора и хранения данных на выбранном защищенном хостинге, часть данных, а именно связанных с персональными данными и данными идентификации в сети интернет, должны валидироваться, если почта и телефон валидируются проверочным кодом, то документы и биометрия клиентов могут быть валидированы программами проверки, а именно https://sumsub.com/, или в ручном режиме используя ряд различных инструментов, в том числе гос базы, мы конечно рекомендуем подключение автоматизированной проверки, так как это забирает лишние хлопоты, связанные с качественной проверкой, хранением данных ваших пользователей.

Допустим в программе sumsub, можно автоматически запретить возможность прохождения KYC гражданам из юрисдикций, находящимся в черном списке FATF.

4.2.2. IP address.

IP-адрес (internet protocol address) — **уникальный адрес компьютера, смартфона, планшета в интернете или локальной сети**. Помимо сбора и хранения этого важнейшего параметра, вам необходимо также настраивать работу, запрещающую доступ к вашему сервису с ip-адресов, запрещенных юрисдикций работа с которыми невозможна, по требованию регулятора, здравому смыслу или не возможности обеспечения должного уровня комплаенс при работе с резидентами тех стран, допустим установить запрет на доступ пользователей из стран, находящимся в черном списке FATF является обязательным защитным механизмом. Также рекомендуется запрещать к доступу анонимные сети, такие как TOR.

4.2.3 Пункты 3 и 4

User agent — идентификационная строка клиентского приложения; обычно используется для приложений, осуществляющих доступ к веб-сайтам — браузеров, поисковых роботов и «пауков», мобильных телефонов и других устройств со встроенным доступом к веб-ресурсам.

Ку́ки (англ. *cookie*, дословно — «печенье») — небольшой набор данных, отправляемый веб-сервером и хранимый на компьютере пользователя без изменений и какой-либо обработки. Веб-клиент (обычно веб-браузер) всякий раз при обращении к соответствующему сайту пересылает эти данные веб-серверу в составе HTTP-запроса. Обычно куки применяют для[1]:

- аутентификации пользователя;
- хранения персональных предпочтений и настроек пользователя;
- отслеживания состояния сеанса доступа пользователя;
- хранения сведений статистики о пользователе.

Данные переменные помогают в идентификации пользователя в сложных расследованиях, проводимых государственными органами, это обязательные параметры для сбора и хранения.

Геолокация, часовой пояс - сбор данных этого типа помогает дополнительно отслеживать и вовремя реагировать на реальное местоположение пользователя, как пример человек прошел KYC на документы, полученные в Казахстане, а сам находится на территории США, зная этот нюанс, вы сможете правильно построить будущую работу с данным пользователем.

4.2.4 Пункты 6 и 7

Пункт 6 является необходимым к сбору так как, кошельки в обозревателях блокчейн не имеют идентифицирующей привязки к пользователю, поэтому ваш

сервис должен надлежащим образом хранить подобные данные с привязкой к вашему пользователю, чтобы в случае наступления негативных событий вы смогли предоставить точные данные кому и когда данный адрес принадлежал с целью переадресации требований со стороны госорганов к вашему сервису.

Пункт 7 является необходимым в обеспечение должной осмотрительности и противодействию отмывания денежных средств, так как является ключевым в криптовалютном AML, потому что обладает максимальной информативностью о том или ином кошельке, транзакции, кластере, а также у вас появляется возможность сохранять историю проверок и ретроспективно возвращаться к финансовой истории пользователя, остановимся здесь подробнее:

Подобные AML-проверки можно автоматизировать или проводить в ручном режиме используя программное обеспечение, выбирать ПО стоит из ваших бизнес задач, количества проверок, региона присутствия.

4.2.5 Автоматизированная проверка входящих транзакций. Автоматизированная проверка входящих транзакций на соответствие AML (Anti-Money Laundering) требованиям для криптовалютных операций — это ключевой элемент для обеспечения соответствия регуляциям MiCA, FATF, другим регуляторным законам и правилам, а также нормам AML с точки зрения должной осмотрительности.

Так как в рамках операционной деятельности среднего и крупного проекта нет физической возможности проверять каждую транзакцию в ручном режиме, необходимо налаживать автоматизацию, для бизнеса с редкими транзакциями есть возможность использовать ручные решения, более простые. Ваша система должна иметь следующие модули:

1. Проверка источников и адресов отправителей.
2. Скрининг транзакций на наличие признаков отмывания денег.
3. Мониторинг подозрительной активности в реальном времени.
4. Риск скоринговая оценка транзакций.
5. Отчеты и аудит для регуляторов.

Этапы автоматизации проверки входящих транзакций

4.2.6 Проверка адресов на санкции и черные списки

Первый этап — проверка адресов отправителей на соответствие спискам подозрительных адресов (например, связанных с террористами, хакерскими группами, или адресов, находящихся под санкциями).

Инструменты для проверки адресов:

- **Chainalysis** — Платформа для анализа блокчейн-данных.
- **Crystal** — Платформа для анализа блокчейн-данных.
- **AML bot** — Платформа для анализа блокчейн-данных подходит под малый бизнес.

Данные решения имеют возможность API-интеграции и позволяют автоматически проверять адреса отправителей и выявлять подозрительные кошельки на основе данных из санкционных списков, черных списков и других источников, а также данные программы, способные решать все задачи, описанные нами выше.

4.2.7 Скрининг транзакций на признаки подозрительной активности

Криптовалютные транзакции могут быть использованы для отмывания денег (AML-риски). Поэтому важно выявить незаконные действия заранее, это поможет избежать проблем с законом. Это важно как для криптобирж, так и для любого бизнеса, работающего с цифровыми активами.

Ниже представим основные паттерны на что стоит обращать внимание:

Много мелких переводов	Получение большого количества небольших транзакций с разных адресов.
Обфускация через миксеры и мосты	Использование сервисов миксинга (Tornado Cash и др.) или мостов (Ava bridge или другие) для скрытия следов.
Аномальные суммы	Переводы необычно больших сумм по сравнению с предыдущей активностью.

Частые переводы	Короткие промежутки между транзакциями или многократные переводы за сутки.

Санкционные адреса	Взаимодействие с адресами из санкционных списков (OFAC, EU и т.д.).

Новые кошельки	Использование недавно созданных кошельков для крупных переводов.

Высокая географическая рискованность	Транзакции из стран с высоким уровнем коррупции, риском финансирования терроризма, или строгим финансовым законодательством по отношению к своим резидентам.

Данные паттерны хорошо автоматизируются в программах описанных выше, при ручной проверке будет уходить много времени, рекомендуем конечно использовать автоматизированные решения.

4.2.8 Мониторинг транзакций в реальном времени

Необходимо чтобы ваша система быть способна в режиме реального времени отслеживать входящие транзакции и проверять их по нескольким параметрам:

1. Проверка на аномалии раскрытые в главе 2.
2. Мониторинг транзакций в цепочке (чтобы отследить происхождение средств обычно делается AML- офицером по высокорисковым транзакциям).
3. Фильтрация транзакций из стран с высоким уровнем риска (страны с неблагоприятной юрисдикцией для вас)
4. Также необходимым является наличие модуля блокировки в реальном времени, который будет срабатывать автоматически при наступлении тех или иных событий.
5. Хорошим инструментом является обозреватель криптовалютных связей, который позволяет в режиме реального времени изучить историю движения тех или иных активов, продается по лицензии Crystal, Chainanalyses, программа AML-бот не обладает подобным модулем.

6. Установить срок спустя которого система будет перепроверять транзакции, это осуществляется затем чтобы всегда актуализировать оценку транзакции в ретроспективе, вызвано это особенностью разметки криптовалютных кластеров.
7. Необходимо также проверять исходящие адреса взаимодействия на наличие описанных выше паттернов.

4.2.9 Риск скоринговая оценка транзакций.

После проверки адреса, система должна оценить уровень риска транзакции сравнить его с настроенным вами приемлемым уровнем и принять решение пустить транзакцию или отправить ее на дополнительную проверку или блокировку. Это делается на основе анализа следующих факторов:

- История адреса (связь с преступными кластерами).
- Объем транзакции.

- Частота транзакций.
- Исходящая сущность.

Используя указанные выше данные, происходит автоматический расчет Risk Score:

- High Risk — Адрес или транзакция связаны с подозрительной активностью, работать не рекомендуется.
- Medium Risk — Требуется дополнительная проверка.
- Low Risk — Транзакция считается малорисковой.

В разных программах оценки и их наименование могут отличаться.

Обращаю ваше внимание что все эти оценки являются субъективным мнением той или иной компании и могут не отражать истинный источник происхождения активов, то есть преступные активы могут долгое время пребывать в низкорисковом кластере, чтобы уберечь себя от финансовых потерь рекомендуется проводить качественный КУС и соблюдать другие процедуры должной осмотрительности.

Создадим примерные, скоринговые модели, отмечу все уровни для реального бизнеса создаются на основание индивидуального подхода, данный модуль очень трудно унифицировать. *Первая модель будет максимально безопасная.*

Общий уровень оценки не выходит за 62% по модели программы Crystal. Уровень сигналов не превышает значения см.таблицу.

Category	**Max %**
Child Exploitation	0%
Darknet arketplace	0%
Darknet service	0%
Enforcement ction	0%
Fraudulent xchange	0%
Illegal Service	0%
Mixing Service	0%
Ransom	0%
Sanctions	0%
Scam	0%
Stolen Coins	0%
Terrorism nancing	0%
Gambling	50%
ATM	50%
Exchange nlicensed	50% с исключениями: крайне рисковые обменные сущности не допускаются к работе.
P2P Exchange nlicenced	50%
Liquidity Pools	100%
Exchange Licenced	100%
Miner	100%
Online marketplace	100%
Online Wallet	100%
Other	100%
P2P Exchange cenced	100%
Payment Processor	100%
Seized Assets	100%

Вторая модель средне безопасная. Общий уровень оценки не выходит за 70% по модели программы Crystal. Уровень сигналов не превышает значения см.таблицу

Category	Max %
Child Exploitation	0%
Darknet Marketplace	3%
Darknet service	3%
Enforcement Action	3%
Fraudulent Exchange	3%
Illegal Service	1%
Mixing Service	3%
Ransom	0%
Sanctions	3%
Scam	3%
Stolen Coins	3%
Terrorism Financing	0%
Gambling	100%
ATM	100%
Exchange Unlicensed	100%
P2P Exchange Unlicenced	100%
Liquidity Pools	100%
Exchange Licenced	100%
Miner	100%
Online marketplace	100%
Online Wallet	100%
Other	100%
P2P Exchange Licenced	100%
Payment Processor	100%
Seized Assets	100%

Высокорисковая модель. Общий уровень оценки не выходит за 75% по модели программы Crystal. Уровень сигналов не превышает значения см.таблицу

Category	Max %
Child Exploitation	0%
Darknet Marketplace	5%
Darknet service	5%
Enforcement Action	5%
Fraudulent Exchange	5%
Illegal Service	3%
Mixing Service	5%
Ransom	0%

Sanctions	5%
Scam	5%
Stolen Coins	5%
Terrorism Financing	0%
Gambling	100%
ATM	100%
Exchange Unlicensed	100%
P2P Exchange Unlicenced	100%
Liquidity Pools	100%
Exchange Licenced	100%
Miner	100%
Online marketplace	100%
Online Wallet	100%
Other	100%
P2P Exchange Licenced	100%
Payment Processor	100%
Seized Assets	100%

Хочу отметить, что это все примерные уровни сигналов, подобные скоринг-модели строятся индивидуально на основание многих факторов вашего бизнеса, ваших клиентов, средней суммы транзакции, для создания максимально эффективного модуля требуется проведение консультаций с вашим AML офицером.

4. 3. Отчеты и уведомления

После анализа транзакций система должна:

1. Генерировать отчеты для аудита (например, для предоставления регуляторам).
2. Отправлять уведомления о подозрительных транзакциях вашему комплаенс-отделу.
3. Надежным образом хранить данные для возможности возврата к проверке в любой момент времени.

Изучив вопрос операционного амл с точки зрения технологических мероприятий можно сделать следующие выводы:

В криптовалютном бизнесе не обойтись без ПО, которое заберет на себя необходимость проверки криптовалюных транзакций и проведения процедуры KYC. Очень многие настройки зависят от вашего геопозиционирования и

требований регулятора. За неисполнение или частичное исполнение норм существует уголовная ответственность в некоторых юрисдикциях.

Оценка транзакций, кошельков программами по проверки нередко носит субъективный характер и требует ручной проверки AML офицером. Построение автоматизированного модуля AML защиты потребует много ресурсов вашего AML офицера и системного администратора.

Глава 5. Выводы и итоговые рекомендации

Чтобы объединить обозначенную выше информацию, в данной главе мы кратко представим основные выводы и содержание каждой из Глав. Отразим основные рекомендации, на которые стоит обратить внимание и далее держать в голове. Это также поможет вам ориентироваться внутри документа при поиске необходимой конкретно вам информации.

Глава 1.

Акцент на изменениях в криптовалютной сфере, методов и подходов к ведению бизнеса внутри неё, сближение с классическими требованиями международных финансовых систем с добавлением требований, специфичных конкретно для криптовалют. Определения основных понятий, раскрытие их значимости – AML, Compliance и связанные с ними.

Международные требования и нормы, влияющие на работу в сфере криптовалют. Раскрытие их особенностей и важности.

Основные рекомендации на основании 1 главы:

Необходимость ознакомления с основной теоретической базой – первоочередный шаг при начале построения крипто бизнеса или погружения в эту сферу.

Глава 2.

Особенности формирования криптобизнеса в текущих реалиях, порядок шагов и особенности каждого из них. Разделение на подготовительные, основные и дополнительные этапы, их значение в построении успешного бизнеса. Разные направления и виды криптобизнеса, их особенности и основания для выбора конкретной модели. Ориентировочные затраты. Дальнейшее сопровождение и ведение бизнеса, мониторинг и контроль. Перечень внутренних и внешних документов необходимых юридическому лицу, осуществляющему деятельность в крипто сфере. Глава 3 раскрывает содержание данных документов.

Основные рекомендации на основании 2 главы:

1. **Обратить внимание на легализацию бизнеса и ужесточения его регулирования, а также санкций за несоблюдение необходимых мер безопасности.**
2. **Использовать основательный подход к формированию/созданию/модификации вашего криптобизнеса, использовать поэтапные шаги, а также не забывать о работе со специалистами (техническими, юридическими и иными).**

3. Оценить затраты, а также длительность регистрации криптокомпании перед запуском. Учитывать важность дальнейшего сопровождения и поддержания бизнеса, соблюдения норм, прописанных в документах компании.

4. Качественно подойти к созданию внутренней и внешней документации, оценить реализуемость прописанных там шагов на практике.

Глава 4.

Расширенный комментарий по технической части ведения крипто бизнеса после его регистрации, особенности юрисдикций и используемых процедур. Основные элементы для соблюдения безопасности вас и ваших клиентов. Подробно раскрыты рабочие элементы, подверженные проверкам и контролю.

Основные рекомендации на основании 4 главы:

1. Внимание к каждому используемому техническому решению: серверам, хостингам, Программному обеспечению и иным. Каждый элемент является вашей защитой от рисков и при неправильном введении в эксплуатацию может стать не спасением от рисков, а его источником.

2. Не только механизированные, но и ручные проверки специалистами транзакций, особенно при введении и стабилизации систем.

3. Поэтапность и структуризация. То, как заложена структура технически операционной работы в самом начале отражает эффективность применяемых внутри системы инструментов.

Для успешного создания прибыльного крипто бизнеса, который сможет закрывать интересы вас и ваших клиентов с минимальными рисками данные рекомендации являются основными и помогут последовательно структурировать вашу идею в реальную единицу бизнеса.