Королевский институт объединенных служб
по изучению вопросов обороны и безопасности

Руководящий документ 2022 года

Противодействие финансированию распространения оружия массового уничтожения для провайдеров услуг в сфере виртуальных активов.

Kayla Izenman

Противодействие финансированию распространения оружия массового уничтожения для провайдеров услуг в сфере виртуальных активов.

Kayla Izenman

Руководящий документ RUSI, Март 2022 г.

Королевский институт объединенных служб
по изучению вопросов обороны и безопасности

191 лет независимого мышления в области обороны и безопасности

Королевский институт объединенных служб по изучению вопросов обороны и безопасности (англ. RUSI) — это ведущий аналитический центр Великобритании по вопросам обороны и безопасности, являющийся старейшей в мире организацией подобного рода. Его миссия — информировать, влиять и активизировать общественные дебаты в целях построения более безопасного и стабильного мира.RUSI — это исследовательский институт, выполняющий независимый, практический и инновационный анализ для решения сложных задач сегодняшнего дня.

С момента своего основания в 1831 году RUSI поддерживается своими участниками. Благодаря доходам от исследований, публикаций и конференций, RUSI сохраняет политическую независимость на протяжении 191 лет.

Отказ от ответственности

Это руководство предназначено для провайдеров услуг в сфере виртуальных активов (ПУВА), желающих создать или продолжить разработку функции противодействия финансированию распространения оружия массового уничтожения (ПФРОМУ) в своей организации. Руководство направлено на создание основы для применения и адаптации ПУВА собственной практики в целях соблюдения требований в отношении финансовых преступлений при одновременном обеспечении соответствия с внутренними нормативными требованиями. Руководство не является юридическим или нормативным разъяснением и всегда должно рассматриваться в сочетании с соответствующим национальным законодательством, а также с международными стандартами и руководствами. По вопросам применения санкций, борьбы с финансовыми преступлениями и ПФРОМУ следует всегда обращаться за независимой юридической консультацией.

На момент написания статьи Кайла Айзенман занимала должность научного сотрудника Центра исследований финансовых преступлений и безопасности RUSI. Эта статья представляет ее личное мнение в тот период и не отражает ее сегодняшних взглядов, а также не имеет отношения к работе, которую она выполняет сейчас, или к ее нынешнему работодателю..

Мнения, выраженные в данной публикации, принадлежат автору и не отражают точку зрения RUSI или любого другого учреждения.

Эта версия была переведена с английского оригинала, который был опубликован в сентябре 2021 г.

Опубликовано в 2022 году Королевским институтом обороны и исследований по изучению вопросов обороны и безопасности.

уководство RUSI, Март 2022 г. ISSN 2397-0286 (онлайн).

Royal United Services Institute
for Defence and Security Studies
Whitehall
Лондон SW1A 2ET
Великобритания
+44 (0)20 7747 2600
www.rusi.org
RUSI является зарегистрированной благотворительной организацией (№ 210639)

Содержание

Благодарности

Данное исследование было проведено при щедрой поддержке Фонда Джона Д. и Кэтрин Т. Мак-Артуров. Благодарим Дэвида Карлайла и Малкольма Райта за полезные комментарии к предыдущей версии этого документа. Также благодарим всех тех, кто с 2017 года щедро предоставлял свое время для интервью в рамках исследования виртуальных активов RUSI, а также команду издательства RUSI за работу по редактированию руководства.

Аббревиатуры

ПОД – противодействие отмыванию денег

НПК – надлежащая проверка клиентов

ФТ – противодействие финансированию терроризма

ПФРОМУ – противодействие финансированию распространения оружия массового уничтожения

УПК – усиленная проверка клиента

ФАТФ – Группа разработки финансовых мер борьбы с отмыванием денег

KYC – знай своего клиента

ОД – отмывание доходов, полученных преступным путем

ФРОМУ – финансирование распространения оружия массового уничтожения

ФТ – финансирование терроризма

ВА – виртуальный актив

ПУВА – провайдер услуг в сфере виртуальных активов

I. Сфера применения и цели

ФИНАНСИРОВАНИЕ РАСПРОСТРАНЕНИЯ (ФР) ОМУ определяется Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ) как «акт предоставления средств или финансовых услуг, полностью или частично используемых для производства, приобретения, владения, разработки, экспорта, переправки, посредничества, транспортировки, передачи, накопления или применения ядерного, химического или биологического оружия».[1] Это рабочее определение ФАТФ, но стоит отметить, что признанного на международном уровне определения ФРОМУ не существует, и некоторые выступают за более широкое понимание, которое может включать, например, деятельность, приносящую доход.[2]

Лица, распространяющие ОМУ, такие как Северная Корея и Иран, продолжают уклоняться от адресных финансовых санкций. Виртуальные активы[3] (ВА) все чаще становятся средством для сбора и перемещения средств, связанных с распространением ОМУ. Однако высокий уровень осведомленности распространителей ОМУ, находящихся под санкциями, в сфере отмывания денег и сбора средств пока не находит должного отклика в соблюдении требований, регулировании и действиях правоохранительных органов. За последние несколько лет пространство ВА выросло и усовершенствовалось с точки зрения практики соблюдения требований, но некоторые преступные субъекты по-прежнему находятся на шаг впереди.

Санкции, направленные против программы ядерных вооружений Северной Кореи, действуют на уровне ООН с 2006 года и постоянно расширяются, включая целевые финансовые санкции против определенных физических и юридических лиц, санкции на основе деятельности, ограничивающие доступ Северной Кореи к международной финансовой системе, а также секторальные санкции, направленные на определенные отрасли или экспорт из Северной Кореи. ООН также сохраняет действие санкций против некоторых иранских физических и юридических лиц и ограничивает деятельность, связанную с разработкой баллистических ракет.[4]

---

1. Financial Action Task Force (FATF), 'Combating Proliferation Financing: A Status Report on Policy Development and Consultation', FATF Report, Августа 2010 г., p. 5.
2. Более развернутое определение финансирования распространения ОМУ (ФРОМУ) представлено здесь: Anagha Joshi, Emil Dall and Darya Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', RUSI, Май 2019 г., p. 5.
3. В данном руководстве под «виртуальными активами» подразумеваются цифровые платежные токены, такие как биткойн. Полное определение см. в разделе «Терминология».
4. Актуальную информацию о требованиях ООН в отношении санкций, связанных с распространением, см. здесь: UN, 'Subsidiary Organs of the United Nations Security Council', 2021. Односторонние санкции,

Начиная с 2014 года Северная Корея углубляет свой опыт и демонстрирует интерес к киберпреступности, в последнее время также включая ВА в данное понятие.[5] В течение 2020 и 2021 годов Министерство юстиции США предъявило обвинения.[6] Тем не менее, хотя большинство северокорейских ВА связаны с крупномасштабными взломами, такими как взлом Upbit[7] в 2019 году на сумму 49 млн долларов или 275 млн долларов, похищенных у криптовалютной биржи KuCoin в 2020 году,[8] режим также проявил интерес к атакам программ-вымогателей и майнингу ВА.[9] В целом, Северная Корея весьма продвинута в сфере киберпреступности и, похоже, все больше заинтересована в применении этих навыков в криптовалютной сфере. Хотя это и не является основной темой данного руководства, есть также сведения, что Иран начал использовать майнинг ВА для обхода санкций и экспорта нефти, причем огромная доля мирового майнинга ВА приходится на эту страну.[10] В условиях отказа от соблюдения законодательства и отсутствия регулирования

например, введенные США, ЕС или Великобританией, могут предъявлять дополнительные требования к санкциям ООН.

5. Одним из самых ранних примеров северокорейской киберпреступной деятельности был печально известный взлом Sony Pictures, который ФБР внесло в свой отчет в декабре 2014 года. См. FBI, 'Update on Sony Investigation', 19 декабря 2014 г., <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>, адата обращения: от 24 августа 2021 г.
6. Министерство юстиции США 17 февраля 2021 г.: «Трем северокорейским военным-хакерам предъявлено обвинение в широкомасштабной схеме совершения кибератак и финансовых преступлений по всему миру»; Министерство юстиции США 27 августа 2020 г.: «Соединенные Штаты подали жалобу на конфискацию 280 криптовалютных счетов, связанных со взломами двух бирж северокорейскими хакерами»; Министерство юстиции США 2 марта 2020 г.: «Два гражданина Китая обвиняются в отмывании более 100 миллионов долларов в криптовалюте в результате взлома биржи», <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, дата обращения: 24 августа 2021 г.
7. Подробнее о взломе Upbit см. в Marie Huillet «Upbit Hack: Stolen ETH Worth Millions on the Move to Unknown Wallets', *Coin Telegraph*, 3 Декабрь 2019 г., <https://cointelegraph.com/news/upbit-hack-stolen-eth-worth-millions-on-the-move-to-unknown-wallets>, дата обращения: 25 августа 2021 г. В жалобе Министерства юстиции США против Тянь Иньинь от 2020 года взлом Upbit назван «вторжением и кражей в ноябре 2019 года» «Exchange 3». Министерство юстиции США: «Два гражданина Китая обвиняются в отмывании более 100 миллионов долларов в криптовалюте в результате взлома биржи».
8. Подробную информацию о взломе биржи KuCoin см. в Chainalysis, «The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds', 2 Октябрь 2020 г., <https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap>, дата обращения: 25 августа 2021 г. В Заключительном отчете Группы экспертов ООН за 2021 год говорится о продолжающемся расследовании «взлома криптовалютной биржи, произошедшего в сентябре 2020 года», в результате которого «с биржи были похищены криптовалютные активы на сумму около 281 миллион долларов». 1718 Sanctions Committee (DPRK), 'Final Report of the Panel of Experts Submitted Pursuant to Resolution 2515 (2020)', 4 Март 2021 г..
9. Yosuke Onchi, 'North Korea Ramps up Ransomware Attacks in Hunt for Cash', *Nikkei Asia*, 18 февраля 2021 г.
10. Tom Robinson, 'How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil', Elliptic, 21 Май 2021 г.

в глобальном масштабе во многих юрисдикциях провайдеры услуг в сфере виртуальных активов (ПУВА) могут представлять собой легкую мишень для этих субъектов.

Целью настоящего руководства является предоставление ПУВА рекомендаций по соблюдению передовой практики при работе с риском ФРОМУ. Оно также включает в себя рекомендованные публикации для специалистов по соблюдению законодательства, которые могут помочь в их работе (см. Приложение II). Документ будет особенно полезен тем ПУВА, которые ранее не рассматривали ФРОМУ или введение целевых финансовых санкций за распространение оружия массового уничтожения в качестве отдельного финансового преступления или риска, связанного с санкциями.

Хотя в данном руководстве используются примеры из практики распространения ОМП, в основном касающиеся Северной Кореи, большая его часть опирается на типологии, тревожные признаки и передовую практику, которые можно найти в других видах преступлений в связи с ВА, особенно когда незаконная деятельность осуществляется крупными преступными организациями, которые могут иметь опыт и финансирование, сопоставимые со страной, находящейся под санкциями.

Руководство организовано в соответствии с общей структурой цикла обеспечения соответствия: формулирование предварительных требований до взаимодействия с клиентом, за которым следует процесс адаптации новых клиентов и постоянный мониторинг на протяжении всего периода работы с клиентом. После обзора данного цикла в руководстве рассматриваются индикаторы высокого риска и тревожные признаки, которые повлекут за собой усиленную проверку клиента или отказу в обслуживании, и завершается требованиями к отчетности после любого отмеченного факта подозрительной деятельности.

Рекомендации ФАТФ по виртуальным активам и провайдерам услуг в сфере виртуальных активов

Понимание и выполнение Рекомендаций ФАТФ для ПУВА является ключевым условием соблюдения передовой практики, и данное руководство направлено на соответствие и поддержку Рекомендаций ФАТФ.

Хотя ФАТФ с 2014 года[11] признает связанные с ВА риски, первое принятие изменений в Рекомендациях, связанных с ВА, состоялось в октябре 2018 года, с уточнением, что Рекомендации применяются к финансовой деятельности, связанной с ВА. В июне 2019 года ФАТФ приняла Пояснительную записку к Рекомендации 15[12] которая дополнительно

11. FATF, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', Июнь 2014 г., <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, дата обращения: 25 августа 2021 г.
12. FATF, 'Public Statement on Virtual Assets and Related Providers', 21 Июнь 2019 г., <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html>, дата обращения: 24

разъяснила, как Рекомендации ФАТФ применяются к ВА и ПУВА. Сюда вошли рекомендации по надзору, мониторингу, лицензированию и регистрации, надлежащей проверке клиентов (НПК), отчетности о подозрительных операциях, мерам по проверке в санкционных списках и многое другое.

В июне 2019 года ФАТФ также приняла Руководство по применению риск-ориентированного подхода к виртуальным активам и провайдерам услуг в сфере виртуальных активов[13] цель которого — помочь национальным органам в разработке соответствующих режимов регулирования ВА и ПУВА, а также предоставить частному сектору информацию по вопросам соблюдения этих требований.

С момента публикации Руководства ФАТФ было проведено два пересмотра — в июле 2020 года и в июле 2021 года.[14] Руководство также регулярно обновляется с целью улучшения рекомендаций и поддержания их актуальности по отношению к темпам инноваций в индустрии ВА; с этой целью ФАТФ проводит публичные консультации по Руководству.[15]

Международные требования

Цель данного руководства — представить набор стандартов в соответствии с наиболее строгими международными рекомендациями и правилами по соблюдению законодательства в сфере ВА. Необходимо также отметить, что данное руководство не придерживается какого-либо конкретного национального регламента в сфере криптовалют. Перед применением любых рекомендаций, изложенных в настоящем документе, необходимо убедиться в полном понимании нормативных актов соответствующих юрисдикций для ПУВА. В дополнение к этому и (или) в случае отсутствия регулирования в соответствующей юрисдикции (юрисдикциях) следует также обеспечить полное понимание Рекомендаций ФАТФ. Более подробную информацию см. в Приложении I.

августа 2021 г.

13. FATF, ‘Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers’, Июнь 2019 г., <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>, дата обращения: 24 августа 2021 г.
14. FATF, ’12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers’, Июль 2020 г., <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html>, дата обращения: 24 августа 2021 г.; FATF, ‘Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers’, Июль 2021 г., <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>, дата обращения: 24 Август 2021 г.
15. FATF, ‘Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’, Март 2021 г., <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html>, дата обращения: 24 августа 2021 г.

II. Терминология

В НАСТОЯЩЕМ РУКОВОДЯЩЕМ ДОКУМЕНТЕ используется терминология, принятая ФАТФ. Поэтому во всем тексте используются термины «виртуальный актив» (ВА) и «провайдер услуг в сфере виртуальных активов» (ПУВА).

Обратите внимание, что несмотря на использование термина «ПУВА», его сфера применения значительно уже, чем определение ФАТФ. Хотя определение ФАТФ включает в себя любой бизнес, занимающийся обменом виртуальных активов на фиатные средства, обменом виртуальных активов на ВА, или передачей, хранением или управлением ВА, а также любой бизнес, предоставляющий финансовые услуги, связанные с ВА[16] , в данном руководстве ПДУ определяется как **централизованная биржа виртуальных активов**, предлагающая услуги обмена ВА на фиатную валюту или ВА на ВА

Аналогичным образом, термин ВА применим только к **платежным токенам**, таким как биткойн, и не относится к стейблкоинам или цифровым валютам центрального банка. В настоящем документе термин ВА эквивалентен терминам «криптовалюта», «виртуальная валюта» или «криптоактив».

ВА-«кошельки» бывают разных форм, и в данной работе автор не делает различия между горячими (онлайн) кошельками и холодными (офлайн) кошельками. Кошельки обеспечивают безопасность и доступ к закрытым ключам пользователя и предлагаются многими провайдерами, включая централизованные биржи.

Методика

Настоящее руководство было подготовлено в рамках текущего проекта RUSI по ПФРОМУ. Команда RUSI анализирует деятельность ФРОМУ с 2015 года,[17] i включая продолжающееся исследование роли ВА и других новых платежных систем в уклонении от санкций, в основном рассматривая Северную Корею.[18] Данное руководство основано на опыте команды RUSI в этой области, глубоких исследованиях и неформальных беседах, проведенных за последние три года с заинтересованными сторонами в соответствующих

16. FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations’, с изменениями от июня 2021 года, стр. 130.
17. Другие публикации RUSI в отношении ФРОМУ см. в RUSI, ‘Proliferation Financing’, <https://rusi.org/explore-our-research/topics/proliferation-financing>, дата обращения: 24 августа 2021 г.
18. Более подробную информацию о деятельности северокорейских ВА читайте в статье Дэвида Карлайла и Кайлы Айзенман: David Carlisle and Kayla Izenman, ‘Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia’, *RUSI Occasional Papers* (апреля 2019 г.).

отраслях, включая ПУВА, регуляторов, правоохранительные органы, традиционные банки, альтернативные банки и научные круги.

III. Предварительные требования

ЭТОТ РАЗДЕЛ ПОСВЯЩЕН всем аспектам системы контроля над соблюдением законодательства, которая должна быть создана до работы с клиентами. С истема включает в себя создание эффективной и компетентной команды по соблюдению нормативных требований, первоначальную оценку рисков, глубокое понимание всех соответствующих национальных и международных требований, надлежащее обучение и протоколы по кибербезопасности, а также специальную политику относительно решений о добавлении криптовалют в списки.

Команда по соблюдению нормативных требований

Для того чтобы должным образом реализовать любой из перечисленных ниже принципов, ПУВА должны сначала убедиться, что у них имеется надлежащая структура управления и команда по соблюдению нормативных требований. Организационная структура ПУВА должна обеспечивать наличие у данной команды ресурсов, полномочий, информации и независимости, необходимых для оценки и управления рисками, связанными с финансовыми преступлениями.

Комплексная структура управления охватывает все уровни ведения бизнеса. Высшее руководство должно нести единоличную ответственность за надзор и эффективность программы по борьбе с финансовыми преступлениями.

Эффективная программа также требует наличия должностного лица, ответственного за соблюдение нормативных требований, которое обычно называется главным специалистом по соблюдению нормативных требований и который в конечном итоге отвечает за разработку и реализацию программы по соблюдению нормативных требований, а также за обеспечение полного соответствия нормативным и юридическим обязательствам. В крупных компаниях может быть назначен дополнительный сотрудник по соблюдению санкций для обеспечения надзора и соблюдения требований, связанных с санкционными списками.

Сотрудники среднего и младшего звена на всех уровнях организации также должны быть проинформированы о тревожных признаках транзакций, требованиях к проверке и отчетности, методах расследования и других соответствующих процедурах соблюдения нормативных требований, которые могут проявиться в других областях деятельности ПУВА. В некоторых регулируемых юрисдикциях требуются особые роли в команде специалистов по соблюдению нормативно-правового соответствия.

Руководство должно обеспечить учет этих факторов при формировании отдела по соблюдению нормативных требований. Все сотрудники группы по соблюдению нормативных требований должны регулярно проходить обучение, охватывающее новейшие тенденции в области ВА, инструменты соблюдения нормативно-правового соответствия, а также все соответствующие местные, национальные и международные нормы.

Оценка рисков

ПУВА должны регулярно проводить внутреннюю оценку рисков для выявления клиентов, секторов или типов операций, которые могут быть подвержены большему риску отмывания денег (ОД)/финансирования терроризма (Фт)/деятельности ФРОМУ, а также разрабатывать и внедрять механизмы контроля для снижения этих конкретных рисков. Финансовые учреждения регулярно проводят оценку рисков по аналогичным аспектам, и ПУВА также должны использовать этот подход.

Оценки рисков должны быть зафиксированы в письменном виде и доступны для проверки регулирующими органами. Оценка риска состоит из трех элементов: угроз, уязвимостей и последствий.

По заявлению ФАТФ, «угроза» в сфере ФРОМУ относится к любому физическому или юридическому лицу, которое ранее уклонялось, нарушало или использовало санкции в связи с ФРОМУ или склонно сделать это в будущем. «Уязвимости» — это все, что может быть использовано лицами, представляющими угрозу, например, пробелы в регулировании или слабые места в кибербезопасности. Сюда относится также географическая и отраслевая уязвимость. «Последствия» означают результат, при котором средства или активы становятся доступными для обозначенных угрожающих субъектов, не только в плане финансирования ОМУ, но и в отношении конечного воздействия на деловые операции и репутацию ПУВА.[19]

Граница между угрозами и уязвимостями может быть размыта, но важно понимать взаимодействие между ними, а также любые смягчающие факторы. Рассматривая угрозы и уязвимости, следует принимать во внимание следующие соображения:

- Известные субъекты угроз.
- Известные типологии преступлений в сфере финансирования.
- Размер и сложность ПУВА.
- Предлагаемые продукты и услуги.
- Метод предоставления продукции и услуг.
- Типы клиентов.
- Физическое местонахождение клиентов.
- Физическое расположение ПУВА и соответствующие нормативные акты.

19. Более подробную информацию об определениях этих трех элементов см. в руководстве ФАТФ: FATF, ‘Guidance on Proliferation Financing Risk Assessment and Mitigation’, Июнь 2021 г., p. 9.

- Смежные учреждения.

Результаты оценки рисков должны указать ПУВА, в каких областях типичные для него риски особенно высоки. Типичный риск обычно определяется как величина риска, существующая при отсутствии контроля; информация, которая станет более ясной после всесторонней оценки риска. Эти средства контроля должны рассматриваться как смягчающие факторы при оценке риска.

Потенциальные последствия ФРОМУ являются более серьезными, чем последствия ОД или ФТ. ПУВА должны оценивать физическое, социальное, экологическое, экономическое и структурное воздействие и вред.

Дополнительную информацию о проведении оценки рисков для ПУВА см. в Приложении I.

Кибербезопасность

В дополнение к процедурам по соблюдению нормативных требований, учитывая масштабы кибератак, которые используются для финансирования распространения ОМУ, необходимо уделять особое внимание кибербезопасности. Речь идет как об обучении сотрудников ПУВА всех уровней, так и о привлечении специалистов по кибербезопасности на платной основе для установки соответствующих средств защиты ПУВА.

Обучение персонала протоколам кибербезопасности необходимо для защиты от хакеров, действующих в интересах распространителей ОМУ. В частности, известно, что Северная Корея участвует в сложных фишинговых схемах для проникновения в ПУВА. Примером может служить атака на DragonEx в 2019 году.

Реальный пример 1: DragonEx (2019)

В марте 2019 года Северная Корея осуществила сложную фишинговую схему, в результате которой сотрудник ПУВА DragonEx неосознанно установил вредоносное программное обеспечение на компьютер, содержащий закрытые ключи кошелька ПУВА, что позволило Северной Корее украсть виртуальные активы на миллионы долларов. Исследователи установили, что ответственность за атаку несет северокорейская киберпреступная группировка Lazarus Group, чьи действия привели к потере более 7 миллионов долларов.

Lazarus зарегистрировала два интернет-домена, подделала программное обеспечение для торговли ВА, внедрила в него вредоносный код и спрятала дезинформацию в автоматизированной торговой платформе ВА, которая нормально работала в течение шести месяцев. Затем злоумышленники разослали программное обеспечение сотрудникам различных ПУВА под видом продвижения продукта. Сотрудники службы поддержки клиентов DragonEx открыли установочный пакет вредоносного программного обеспечения, с помощью которого хакеры смогли получить закрытый ключ для кошелька ПУВА и совершить кражу.

Источники: Lylian Teng, 'Alert! Lazarus Hacker Group Continues Targeting Crypto Using Faked Trading Software', 8BTC, 1 Апреля 2019 г., <https://news.8btc.com/alert-lazarus-hacker-group-continues-targeting-crypto-using-faked-trading-software>, дата обращения 24 Август 2021 г.; Chainalysis, 'As Exchanges Beef Up Security Measures, Hackers Get More Sophisticated', 21 январь 2020 г., <https://blog.chainalysis.com/reports/cryptocurrency-exchange-hacks-2019>, дата обращения 25 Август 2021 г..

Обучение сотрудников имеет ключевое значение, как и физическая защита ПУВА от подобных атак. Сотрудники должны проходить регулярное обучение в сфере кибербезопасности, уметь распознавать потенциально подозрительные электронные письма, вложения, ссылки и программы, а также знать, чего от них ожидать. Эти занятия должны проходить *все* сотрудники, а не только те, кто участвует в программе соблюдения нормативных требований. ПУВА также должны выделять отдельные инвестиционные средства на поддержание соответствующей инфраструктуры ИТ и кибербезопасности, чтобы злоумышленники не смогли проникнуть в систему извне.[20]

Требования к регистрации активов

Учитывая растущий интерес криминальных структур к анонимным криптовалютам, которые потенциально позволяют им перемещать ВА незамеченными, важно учитывать возможности блокчейна по отслеживанию любого актива, размещаемого на платформе ПУВА.

Существует множество вариантов, которые могут помочь снизить риски, связанные с анонимными криптовалютами. Один из вариантов — предлагать своим клиентам исключительно активы с прозрачными блокчейнами (другими словами, вообще не принимая никаких анонимных криптовалют). Если такое решение не подходит, а перечисление анонимных криптовалют является приемлемым риском и частью коммерческой стратегии ПУВА, следует рассмотреть следующие способы снижения риска:

- Листинг только избранных анонимных криптовалют, которые обладают хотя бы некоторой степенью прозрачности (например, Zcash) и для которых доступен анализ отслеживания блокчейна..
- Разрешение использования анонимных криптовалют *только* для транзакций ВА на ВА (другими словами, разрешение обмена анонимных криптовалют на другие ВА, но не на фиатные валюты) для ограничения обналичивания фиатных средств.
- Разрешение клиентам торговать анонимными криптовалютами только в том случае, если они проходят усиленную проверку (УПК) и если торговля анонимными криптовалютами регулируется строгими лимитами и пороговыми значениями.

20. олее подробную информацию о рекомендуемых мерах кибербезопасности см. здесь: Cloud Security Alliance, </727><728>'Crypto-Asset Exchange Security Guidelines', 13 Апреля 2021 г., <https://cloudsecurityalliance.org/artifacts/csa-crypto-asset-exchange-security-guidelines-abstract/>, дата обращения: 22 августа 2021 г.

IV. Санкции и проверка благонадежности ПЗЛ

Санкции применяются ко всем клиентам и сделкам, независимо от суммы. ПУВА должны строго соблюдать все применимые санкционные списки на международном и национальном уровнях, отказывая в открытии счетов обозначенным субъектам или любым лицам, принадлежащим, контролируемым, действующим от имени или под руководством указанных лиц. Проверка на присутствие в санкционных списках должна проводиться при первой проверке личности и далее регулярно на протяжении всего периода сотрудничества с клиентом,[21] при любых входящих и исходящих операциях или при внесении дополнений в санкционные списки.

Управление по контролю за иностранными активами США (OFAC) также ранее включало адреса ВА в свой санкционный список, помечая их флажками в дополнение к любым перечисленным именам.[22] OFAC также ввело санкции против многих лиц и групп за деятельность по уклонению от санкций, связанную с ВА. Рекомендуется рассматривать санкционные списки США в дополнение к любым международным спискам. OFAC специально включили в список адреса ВА, принадлежащие субъектам, занимающимся отмыванием денег от имени Северной Кореи, что свидетельствует о важности этих списков для устранения риска финансирования распространения ОМУ.

Реальный пример 2: Тянь Иньинь и Ли Цзядун (2020)

В марте 2020 года OFAC ввело санкции против Тянь Иньинь и Ли Цзядун, двух граждан Китая, отмывавших ВА от имени Северной Кореи. Эти субъекты были подвергнуты санкциям в рамках американских программ CYBER2 и DPRK3, а также отмечены как связанные с северокорейской хакерской группой Lazarus Group.

Список OFAC для каждого человека включает не только его личную информацию, но и все известные связанные с ним адреса биткойн-кошельков. Тянь, например, имеет восемь адресов биткойн-кошельков.

Списки также включают известные псевдонимы, в данном случае сетевые идентификаторы преступников.

21. Например, когда меняются данные клиента (директора, владельцы, идентификационные данные).
22. См. Министерство финансов США, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses', press release, 28 Ноябрь 2018 г., <https://home.treasury.gov/news/press-releases/sm556>, дата обращения: 24 августа 2021 года..

Источник: Более подробную информацию о списках OFAC см. здесь: Министерство финансов США, 'Treasury Sanctions Invididuals Laundering Cryptocurrency for Lazarus Group', 2 марта 2020 года, <https://home.treasury.gov/news/press-releases/sm924>, адата обращения: 24 августа 2021 г.; OFAC, <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=28263>,дата обращения: 24 августа 2021 г.

В дополнение к санкционным спискам любые субъекты или группы, упомянутые в докладах Группы экспертов ООН, должны проходить санкционный скрининг. Более подробную информацию об этих отчетах см. в Приложении I.

ПУВА также должны рассмотреть возможность проверки СМИ и консультаций с НПО и частным сектором, включая аналитические компании по блокчейну, а также фирмы, занимающиеся кибербезопасностью, по поводу типовых отчетов. Эти субъекты регулярно публикуют данные как о тревожных признаках использования ВА Северной Кореей, так и о связанных с Северной Кореей лицах и организациях. Аналогичным образом ПУВА должны не только проводить скрининг клиентов, но и осуществлять дальнейший мониторинг, в ходе которого ПУВА должны проверить, не являются ли они (или не взаимодействуют ли они с) политически значимыми лицами (ПЗЛ).[23] Если это так, то необходимо провести УПК. Дальнейшие указания по УПК см. ниже.

23. ФАТФ определяет политически значимое лицо (ПЗЛ) как «лицо, которому доверены или были доверены важные функции», и которое может занимать «должности, которые могут быть использованы в целях... отмывания [доходов, полученных незаконным путем]».' См. руководство ФАТФ: «FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)', Июнь 2013 г., <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf>, дата обращения: 22 августа 2021 г.

V. Интеграция новых клиентов

ИНТЕГРАЦИЯ НОВЫХ КЛИЕНТОВ — это следующий шаг в цикле обеспечения соответствия. ПУВА часто испытывают беспокойство по поводу уровня информации, требуемой от клиентов при первом контакте. Хотя предприятия могут работать по-разному, а юрисдикции будут предъявлять различные требования, существуют некоторые общие принципы и передовые методы работы, которые обеспечат максимальную вероятность обнаружения подозрительной активности.

Процедуры «Знай своего клиента»

Процедуры «Знай своего клиента» (ЗСК) являются стандартными банковскими процедурами и должны быть такими же стандартными в ПУВА. К сожалению, в отчете за 2020 год указано, что 56% глобальных ПУВА имеют слабые или уязвимые процессы ЗСК.[24] Для того чтобы ПУВА не попали в эту группу, можно предпринять простые первоначальные шаги.

Многие ПУВА разрешают создавать счета без проверки личности, но требуют дополнительную информацию для отправки или получения средств. Некоторые ПУВА даже требуют верификации перед созданием счета, в то время как другие требуют ЗСК только при использовании фиатной валюты.

Согласно передовой практике, процесс ЗСК должен проводиться *до* внесения или принятия средств клиента, будь то при создании счета или непосредственно перед началом первой транзакции.

В первую очередь, речь идет об идентификации клиента и проверке его личности. Хотя регулирующие органы могут потребовать дополнительную конкретную информацию, обязательному сбору подлежит следующий минимальный пакет данных:

- Имя, дата рождения и гражданство (проверяется с помощью официальных государственных документов, удостоверяющих личность).
- Адрес проверяется с помощью документа, подтверждающего адрес, например, банковской выписки, счета за коммунальные услуги, выданного правительством налогового письма, документа о страховании жилья или свидетельства о проживании, или с помощью цифровых средств, обеспечивающих разумную уверенность в физическом местонахождении клиента..

24. CipherTrace, 'CipherTrace 2020 Geographic Risk Report: VASP KYC by Jurisdiction', Октябрь 2020 г., p. 4, <https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/>, дата обращения: 24 августа 2021 г.

Кроме того, юридические лица должны предоставить как минимум следующую информацию:

- Название, регистрация, адрес и статус компании (проверяется по номеру компании или по соответствующим государственным регистрационным документам и реестрам).
- Идентифицирующая информация ключевого управленческого персонала, включая уполномоченных трейдеров, ведущих счет клиента..
- Структура собственности.

ЗСК (и постоянная НПК) должна проводиться не только в отношении самих клиентов, но и в отношении любых бенефициаров, а также любых лиц, действующих от имени клиента.

ПУВА также должны убедиться, что их процессы проверки информации являются комплексными. Это включает в себя запрос вышеуказанных официальных документов и обеспечение их легитимности, а также рассмотрение дополнительных механизмов ЗСК либо во время регистрации, либо во время подозрительной транзакции. Эти дополнительные требования могут включать:

- Селфи, сделанные в самом приложении, включая детектирование живого пользователя, чтобы доказать, что загруженное лицо принадлежит живому человеку, присутствовавшему в момент съемки.
- Видеозвонки.

Проверка личности и детектирование живого пользователя являются ключом к эффективному соблюдению требований, особенно когда речь идет о тактике, применяемой субъектами, участвующими в финансировании распространения ОМУ. В 2020 году лица, занимающиеся отмыванием денег и перевозящие средства от имени Северной Кореи, не смогли выполнить требования по соблюдению нормативных требований в отношении видеозвонков в одном ПУВА, что в идеале должно было предотвратить отмывание средств через платформу.

Реальный пример 3: 'VCE3' (2020)

В том же деле, описанном в примере 2, помимо санкций OFAC, Министерство юстиции США предъявило Тянь Иньинь и Ли Цзядуну обвинения в отмывании более 100 миллионов долларов в различных криптовалютах от имени Северной Кореи. Криптовалюта была получена в результате взломов ПУВА Северной Кореей, и Тянь и Ли попытались перевести средства через несколько ПУВА, немало в этом преуспев.

Для того чтобы предоставить ПУВА достаточно полную документацию в процессе регистрации, Тянь и Ли отредактировали фотографии людей, используя украденные персональные данные. Один из ПУВА (именуемый VCE3) не удовлетворился предоставленным изображением и запросил видеозвонок для личного общения с владельцем счета, в чем ему было отказано.

Несмотря на это, VCE3 принимал транзакции от Тяня и Ли, в результате чего на счет преступников были переведены похищенные средства в сумме почти 2 миллионов долларов. Это говорит о том, что если бы видеозвонок в реальном времени был обязательным требованием для всех задействованных ПУВА, возможно, средства вообще не отмывались бы через платформы.

Источник: US Department of Justice, 'Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack', 2 Март 2020 г., <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, дата обращения 24 Август 2021 г.

Характер и цель взаимоотношений

Не менее важным, чем идентификация клиента, является характер и цель отношений с клиентом. Единственный способ эффективного выявления признаков подозрительной активности конкретного клиента — это понимание того, на что похожа или должна быть похожа обычная активность этого клиента. Для того чтобы полностью понять характер и цель взаимоотношений во время знакомства с клиентом, необходимо запросить у него, как минимум, следующие оценочные данные:

- Ожидаемая частота транзакций.[25]
- Ожидаемый размер сделок.
- Ожидаемый объем сделок.

Источник и назначение средств

Все ПУВА должны понимать источник и назначение любых средств, перемещаемых через платформу. В частности, при необходимости проведения УПК ПУВА должны собирать информацию об источнике средств клиента и проверять его легитимность, прежде чем вести какие-либо дела от имени клиента. Дальнейшие указания по УПК см. в специальном разделе ниже в этом документе.

Аналогичным образом, если клиент получает средства или участвует в транзакциях, ПУВА должны попытаться собрать соответствующую информацию о другой стороне.26 Аналитические инструменты блокчейна могут обеспечить более глубокое понимание конечного источника и назначения средств и являются рекомендуемым шагом в достижении этой цели.

25. Понятие «транзакция» в данном случае относится к депозитам, снятию средств и сделкам..

VI. Текущий мониторинг и меры по надлежащей проверке клиентов

СЛЕДУЮЩИМ ЭТАПОМ ЯВЛЯЕТСЯ обеспечение непрерывной и эффективной НПК в отношении существующих клиентов. Это означает мониторинг транзакций с целью выявления любой необычной активности, например, отклонения от ожидаемой или предполагаемой активности транзакций, а также понимание причин и целей любых отклонений, обнаруженных на платформе. Необычная или подозрительная деятельность, которую клиент не может объяснить, может указывать на связи с ОД/ФТ/ФРОМУ. Необходимо постоянно проверять деятельность клиента на протяжении всего периода отношений, чтобы убедиться, что эта деятельность соответствует процедуре ЗСК, проведенной во время регистрации, и что характер и цель бизнеса соответствуют информации, предоставленной клиентом в рамках процесса регистрации и ЗСК. Любые значительные изменения должны быть задокументированы и поставлены под сомнение. Информацию ЗСК также следует периодически проверять на основании рисков или событий, вызывающих риск, таких как смена адреса.

Любые клиенты, которые считаются клиентами с повышенным риском на этапе интеграции или на любом этапе процесса НПК, должны подвергаться более частому и тщательному мониторингу.

ПУВА также должны убедиться, что все документы и информация, предоставленные во время регистрации, поддерживаются в актуальном состоянии на протяжении всего периода обслуживания клиента.

В тех случаях, когда в отношении клиента необходимо провести УПК, источники и места назначения средств, определенные во время регистрации, должны продолжать запрашиваться на протяжении всего периода обслуживания.

Ручной и автоматический мониторинг

Любая система мониторинга транзакций направлена на выявление подозрительных или необычных транзакций и (или) действий для дальнейшего изучения. Любая деятельность подобного рода должна незамедлительно рассматриваться людьми, имеющими соответствующую подготовку в этой области, которые затем предпринимают необходимые шаги в ответ на обнаруженные факты, например, сообщают в соответствующие регулирующие органы и (или) подают отчет о подозрительных операциях/деятельности (СПО/СПД). Это может происходить в ходе процедуры ЗСК, когда транзакция инициирована и отмечена флажком, или после проведения транзакции.

Хотя ручной мониторинг и отслеживание блокчейна являются возможными, *настоятельно* рекомендуется использовать автоматизированные сторонние решения для анализа блокчейна. Анализ блокчейна позволяет получить более полное представление о любых моделях поведения, а также выявить любые криминальные адреса и кошельки. Оценки риска для клиентов также значительно более детализированы при анализе с помощью блокчейна. Анализ блокчейна должен включать проверку кошельков до и после транзакции для определения источника и назначения средств. Анализ блокчейна и более глубокое понимание моделей транзакций, а также координация с правоохранительными органами позволяют ПУВА быстро реагировать на любые взломы или похищенные средства и замораживать их в случае необходимости — метод, который уже использовался ранее в борьбе с финансированием распространения через ВА.

Реальный пример 4: «Биржа 9» (2019)

В августе 2020 года Министерство юстиции США обнародовало иск о гражданской конфискации, в котором говорится о взломах ПУВА северокорейскими гражданами, которые отмывали средства через китайские внебиржевые рынки.

В иске говорится, что в декабре 2019 года один из преступников попытался конвертировать украденные эфириумы в биткойны через ПУВА (Биржа 9). Эфириумы были похищены путем взлома другого ПУВА (Биржа 2), факт чего был обнародован. В результате Биржа 9 заморозила средства, участвующие в транзакции, так как украденная с биржи 2 криптовалюта была отмечена флажком в их системе. Средства остаются замороженными на Бирже 9.

Источник: US Department of Justice, 'United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors', 27 Август 2020 г., <https://www.justice.gov/usao-dc/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two>, дата обращения: 24 августа 2021.

ПУВА должны инвестировать не только в аналитику блокчейна, но и в инструменты мониторинга для противодействия отмыванию доходов, полученных преступным путем (ПОД), которые исследуют классические для мониторинга транзакций модели поведения ОД/ФТ/ФРОМУ.

Усиленная проверка клиентов

Усиленная проверка клиентов (УПК) должна проводиться, если операция или счет отмечены как особо рискованные или потенциально подозрительные. Особые показатели высокого риска приведены в следующем разделе. УПК опирается на эффективный мониторинг и должен применяться на основе риск-ориентированной системы при подозрении на

деятельность, связанную с финансовыми преступлениями. Существует целый ряд причин, по которым может потребоваться УПК, включая (среди прочего) случаи, когда клиент:

- при оценке рисков идентифицируется как подверженный особо высокому риску совершения финансовых преступлений;
- Имеет неоправданно сложную или непрозрачную структуру бизнеса;
- осуществляет операции с физическими или юридическими лицами в юрисдикциях с высоким уровнем риска;
- предоставляет украденное или фальшивое удостоверение личности во время регистрации;
- участвует в сделках, которые не соответствуют характеру и цели сотрудничества;
- отправляет, получает или перемещает необычно крупные суммы виртуальных активов или фиатной валюты; является ПЗЛ;
- не может адекватно объяснить цель сделки.

Стоит отметить, что определение «крупных сумм» виртуальных активов является относительным и будет зависеть от масштаба ПУВА и характера отношений с клиентами.

В случае выявления одной или нескольких из этих проблем, следует начать УПК. Первым шагом является получение дополнительных идентификационных данных. Часть из них можно запросить у клиента, другую часть – выяснить отдельно через открытые источники. Например, в случае ПЗЛ необходимо указать должность и подробную информацию о занимаемой должности.

Для создания полного профиля следует также провести проверку неблагоприятной/негативной информации в СМИ. Подавляющее число отрицательных результатов этой проверки может указывать на клиента, с которым слишком рискованно продолжать сотрудничество.

Телефонные или видеоинтервью также могут быть необходимыми инструментами для понимания характера и цели сделок.

Многие ПУВА также регистрируют IP-адреса клиентов и местоположение банкоматов/банков/других ПУВА, участвующих в любом обмене, чтобы убедиться, что эти местоположения соответствуют ожидаемым отношениям.

Виртуальные частные сети (VPN) также могут быть индикатором риска, который при определенных обстоятельствах может привести к УПК. Несмотря на законное использование VPN для создания безопасной торговой среды, должна быть хотя бы одна точка соприкосновения, где сеть VPN не активна, например регистрация в ПУВА, чтобы ПУВА регистрировал подлинный IP-адрес.

VII. Индикаторы высокого риска и тревожные признаки

ЗДЕСЬ ПРИВЕДЕН РЯД индикаторов высокого риска и тревожных признаков, которые могут привести к проведению УПК, СПО/СПД или даже к замораживанию средств. ФАТФ, частный сектор и национальные регулирующие органы составили полный перечень выявленных тревожных признаков с соответствующими исследованиями практических примеров. Дополнительную информацию см.в Приложении I.

Использование миксеров или сервисов анонимизации

Миксеры, приватные кошельки и процедуры CoinJoin[26] — все они обеспечивают различные виды обфускации транзакций и повышают конфиденциальность пользователей. Каждый из них запутывает путь транзакции и делает отслеживание блокчейна все более сложным, а иногда и невозможным.[27]

Очень важно, чтобы ПУВА имели возможность идентифицировать операции с миксерами и приватными кошельками, и в большинстве случаев относились к операциям, связанным с миксерами, как к операциям с повышенным риском.

Такое управление рисками может включать:

- Создание утвержденного списка известных и (или) доверенных миксеров или сервисов CoinJoin, с которыми клиентам разрешено проводить транзакции.
- Авторизация отношений с доверенными миксерами только при определенных условиях (при определенном пороге стоимости).

Известно, что лица, занимающиеся отмыванием доходов, полученных преступным путем, и хакеры, работающие от имени распространителей ОМУ, все чаще используют миксеры.

---

26. CoinJoin — это стратегия анонимизации, которая сохраняет приватность криптовалютных транзакций. Стратегия использует смарт-контракты для смешивания криптовалют в новых транзакциях, при этом на выходе получается одинаковое количество криптовалюты, но из разных транзакций, что приводит к сокрытию источника и целевого назначения.
27. Подробнее о специфике этих технологий см. в статье Антона Моисеенко и Кайлы Айзенман “ From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency’, *RUSI Occasional Papers* (Сентябрь 2019 г.), pp. 19–24; Andrea O’Sullivan, ‘What are Mixers and “Privacy Coins”?’, Coin Center, 7 Июль 2020 г., <https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/>, дата обращения: 24 августа 2021 г.

Группа Lazarus Group, в частности, известна своей заинтересованностью и использованием услуг миксеров для запутывания следов транзакций.

Case Study 5: Lazarus Group (2018)

В своем отчете о криптопреступлениях за 2020 год американская компания Chainalysis, специализирующаяся на отслеживании блокчейна, рассказала о том, как Lazarus Group изменила свои методы в период с 2019 по 2020 год. Одной из областей, на которую обратили внимание, было более активное использование Lazarus миксеров и кошельков с технологией CoinJoin.

По данным Chainalysis, «48% средств, похищенных Lazarus, переместились на кошельки CoinJoin» в 2019 году. Например, в ходе взлома DragonEx (реальный пример 1) Lazarus перевел украденные альткоины, такие как эфириум и лайткойн, на платформу ПУВА, обменяв их на биткойны. Затем эти биткойны были переведены на ряд локальных кошельков, а далее – на кошелек Wasabi, который смешивает криптовалюту по протоколу CoinJoin.

Хотя в отчете о криптопреступности за 2021 год подробно описаны другие методы, используемые Lazarus, статистика Chainalysis также показывает, что в 2020 году использование группой Lazarus миксеров для отмывания украденных средств еще больше возросло.

Источник: Chainalysis, 'The 2020 State of Crypto Crime', январь 2020 г., <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>, дата обращения: 24 августа 2021 г; Chainalysis, 'The 2021 State of Crypto Crime', 16 Августа 2021 г., <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>, дата обращения: 2 сентября 2021 г.

VIII. Требования к отчетности

Требования к отчетности и подача СПО/СПД могут существенно различаться в разных юрисдикциях, а некоторые юрисдикции могут пока не требовать никакой отчетности от ПУВА.Однако ПУВА должны быть готовы работать по самым высоким стандартам — наряду с другими регулируемыми провайдерами финансовых услуг — и должны быть полностью осведомлены о требованиях своей юрисдикции. Сотрудники обязаны сообщать о подозрительных действиях. Кроме того, должен быть разработан четкий процесс, в рамках которого сотрудники сообщают об этом уполномоченному лицу, который инициирует соответствующее расследование и сообщает в соответствующие органы.

Этот процесс должен быть четко описан в должностных инструкциях сотрудников. Соответствующие термины должны быть стандартизированы и определены для упрощения понимания как соответствующим подразделением финансовой разведки, так и ПУВА. Примеры отчетности могут включать СПО/СПД, поданные в связи со следующими тревожными признаками («флажками»):

- Опасения по поводу источника средств, поступающих на кошелек пользователя.
- Структурированные сделки на небольшие суммы — чуть меньше пороговых значений отчетности.
- Немедленный перевод ВА на несколько ПУВА, работающих в других юрисдикциях, особенно в юрисдикциях со слабым регулированием ПУВА.
- Кошелек пользователя получает средства с адресов ВА, которые ранее были отмечены в связи с кражей средств или вымогательством.
- Поддельные или отредактированные документы или фотографии, используемые в целях идентификации.
- Неспособность ПУВА получить запрашиваемую информацию о клиенте или отказ клиента предоставить документы НПК или информацию об источнике средств.

Обратите внимание, что этот список не является исчерпывающим, и сообщать о подозрительной деятельности следует во всех случаях, когда внутренние процессы выявляют подозрительную деятельность.[28]

28. Валютное управление Каймановых островов опубликовало список дополнительных возможных тревожных признаков, которые могут привести к внедрению требований к отчетности для ПУВА в их юрисдикции. См. Cayman Islands Monetary Authority, 'Guidance Notes (Amendments) on the Prevention

and Detection of Money Laundering, Terrorist Financing, and Proliferation Financing in the Cayman Islands', Августа 2021 г., p. 13.

IX. Заключительные замечания

За ПОСЛЕДНИЕ НЕСКОЛЬКО лет повысилась степень контроля над соблюдением законодательства со стороны ПУВА, а нормативные рекомендации были усовершенствованы, но все еще предстоит добиться значительного прогресса. Крайне важно, чтобы ПУВА проводили оценку рисков и применяли скоординированный риск-ориентированный подход к деятельности по ОД/ФТ/ФРОМУ.

ФАТФ ожидает, что страны будут применять в отношении ПУВА меры пресечения, аналогичные тем, которые предусмотрены для традиционных финансовых учреждений, включая соответствующий надзор за сектором и требования по лицензированию или регистрации. Хотя Рекомендации ФАТФ направлены на страны-участницы, а не на сами ПУВА, выполнение странами Рекомендаций и Руководящих принципов все чаще требует от ПУВА их соблюдения, и ожидается, что этот показатель будет расти. У ПУВА имеется возможность понять, что требуется от сектора, и активно выполнять требования, если их юрисдикция еще не внедрила Рекомендации.

Также ведется много споров относительно Рекомендации 16 ФАТФ по электронным переводам, которая советует ПУВА рассматривать все транзакции ВА как трансграничные переводы, учитывая безграничный характер технологии.[29] Это потребует обмена информацией между ПУВА в степени, которую невозможно спрогнозировать, включая хранение и отправку информации об отправителе и бенефициаре другим ПУВА, участвующим в транзакции. В настоящее время существует ряд государственных и частных организаций, разрабатывающих технологические решения для Рекомендации 16.[30]

ПУВА должны стремиться к проактивному соблюдению требований и к риск-ориентированному подходу, чтобы эффективно противостоять угрозам, исходящим от стран-распространителей ОМУ, стремящихся использовать систему в своих корыстных целях.

Поскольку в требования ФАТФ по оценке рисков вносятся изменения, включающие ФРОМУ, ПУВА должны быть особенно бдительны в отношении таких субъектов. Судебная практика продолжает указывать на широкомасштабное использование ВА для уклонения от санкций, и в будущем, несомненно, будет обнародовано еще больше примеров. Для

29. ФАТФ «Международные стандарты по противодействию отмыванию денег, финансированию терроризма и распространения оружия массового уничтожения Рекомендации ФАТФ», стр. 77.
30. Например, см. Ian Allison, 'US Crypto Giants Build First Version of FATF-Compliant "Travel Rule" Tool', *CoinDesk*, 25 Июнь 2021 г., <https://www.coindesk.com/us-crypto-giants-build-first-version-of-fatf-compliant-travel-rule-tool>, дата обращения: 24 августа 2021 г.

снижения бизнес-рисков, а также международных и геополитических рисков, связанных с этими действиями, ПУВА должны применять наиболее полный уровень соблюдения нормативных требований, как показано в данном руководстве и связанных с ним рекомендательных материалах (см. Приложение II).

Приложение I: Контрольный список

Приведенный ниже контрольный список содержит краткое изложение этого руководящего документа. Для получения более подробной информации по любому из этапов просим обращаться к соответствующему разделу статьи.

Предварительные требования

- □ Провайдер услуг в сфере виртуальных активов (ПУВА) имеет надлежащую структуру управления и команду по соблюдению нормативных требований.
  - o Высшее руководство осуществляет надзор и несет ответственность за программу борьбы с финансовыми преступлениями.
  - o Назначается главный инспектор по контролю над соблюдением законодательства.
  - o Назначается сотрудник по контролю над соблюдением санкций (если применимо).
  - o Сотрудники среднего и младшего звена информируются обо всех соответствующих процедурах соблюдения нормативных требований, которые могут проявиться в других областях деятельности ПУВА.
  - o Сотрудники регулярно проходят обучение по тенденциям и типологиям ОД/ФТ/ФРОМУ.
- □ За последние два года ПУВА провел как минимум одну комплексную, документированную оценку рисков.
  - o На основании результатов оценки рисков ПУВА принял меры по выполнению ключевых требований контроля для устранения высоких областей риска.
- □ ПУВА имеет эффективные протоколы кибербезопасности.
  - o ПУВА имеет эффективные протоколы кибербезопасности.

- Существует подходящая и всеобъемлющая инфраструктура ИТ и кибербезопасности на местах.

- ПУВА имеет соответствующие требования к регистрации активов.

Осуществляется проверка на предмет санкций и принадлежности к политически значимым лицам (ВЗЛ)

- ПУВА проводит проверку всех клиентов на присутствие в санкционных списках.

- ПУВА использует все доступные материалы для всестороннего исследования.

  - ПУВА полностью придерживается международных и американских санкционных списков.

  - ПУВА проверяет субъектов, включенных в отчеты Группы экспертов ООН.

  - ПУВА обращается к типологическим отчетам НПО, а также производит анализ СМИ на предмет негативной информации.

- Санкции и проверка ПЗЛ носят непрерывный характер. ПУВА проверяет кошельки виртуальных активов (ВА) перед транзакцией и проводит постоянный мониторинг транзакций.

  - При первой проверке личности проводится скрининг.

  - Скрининг проводится на протяжении всего периода обслуживания клиента.

Интеграция новых клиентов

- В ПУВА действуют комплексные процессы, основанные на принципе «знай своего клиента» (ЗСК).

  - Процессы идентификации клиентов требуют сбора минимального пакета данных: полного имени клиента, даты рождения, гражданства и адреса.

  - Личная информация клиента проверяется с помощью официальных государственных документов, удостоверяющих личность. Адреса проверяются с помощью документа, подтверждающего адрес, или соответствующих цифровых средств.

  - Для идентификации юридического лица требуется, как минимум, название, регистрация, адрес, статус, идентификационные данные ключевого управленческого персонала и структура собственности.

  - Информация о юридическом лице проверяется по номеру компании, соответствующим документам государственной регистрации и реестрам.

  - ЗСК и постоянные процессы НПК проводятся в отношении любых бенефициаров или лиц, действующих от имени клиента.

  - Рассматриваются или внедряются дополнительные механизмы ЗСК, включая селфи, сделанные в приложении, и видеозвонки, подтвержденные детектированием живого пользователя.

- ПУВА полностью понимает характер и цель отношений с клиентом.

  - Клиент указывает ожидаемую частоту транзакций.

  - Клиент предоставляет ожидаемый размер транзакций.

  - Клиент предоставляет ожидаемый объем операций.

- ПУВА понимает, насколько это возможно, как источник, так и место назначения любых перемещенных средств.

Текущий мониторинг и НПК

- Все документы и информация, предоставленные ПУВА во время регистрации, поддерживаются в актуальном состоянии на протяжении всего периода отношений.

- ПУВА внедрил либо ручную, либо автоматизированную систему мониторинга транзакций.

  - У ПУВА используется система, позволяющая проводить комплексную проверку на присутствие в санкционных списках.

- ПУВА понимает ограничения существующей системы.

- □ ПУВА рассмотрел преимущества внедрения крупномасштабного анализа блокчейна.

- □ ПУВА проводит усиленную проверку клиента (УПК), если операция или счет отмечаются как характеризующиеся высоким уровнем риска.

  - ПУВА понимает, когда и как проводить УПК.

Индикаторы высокого риска и тревожные признаки

- □ ПУВА управляет отношениями с миксерами.

  - ПУВА создает утвержденный список известных и (или) доверенных миксеров и сервисов CoinJoin.

  - ПУВА разрешает отношения с доверенными миксерами только при определенных условиях.

Требования к отчетности

- □ ПУВА знает и понимает Рекомендации ФАТФ.

- □ ПУВА осведомлен, понимает и соблюдает все соответствующие нормы, установленные в конкретной юрисдикции.

- □ ПУВА осведомлен, понимает и соблюдает требования своей юрисдикции в отношении отчетности.

- □ Для сотрудников разработан четкий процесс уведомления о подозрительных операциях, поясняющий, что конкретно необходимо направлять назначенному сотруднику по внутренней отчетности.

- □ Назначенный сотрудник, ответственный за отчетность, четко знает процедуру передачи информации в соответствующие органы и вышестоящие инстанции.

- □ Соответствующие термины стандартизированы для служебного пользования и определены для облегчения понимания.

Приложение II: Рекомендуемая литература

Руководство ФАТФ по виртуальным активам и провайдерам услуг в сфере виртуальных активов

FATF, ‘Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers’, Июнь 2019 г., <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>.

FATF, ‘12-Month Review: Virtual Assets and VASPs’, Июль 2020 г., <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html>.

FATF, ‘Second 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs’, Июль 2021 г., <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>.

FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations’, updated Июнь 2021 г.

Руководство по применению рискориентированного подхода. Виртуальные активы и провайдеры услуг в сфере виртуальных активов

Anagha Joshi, Emil Dall and Darya Dolzikova, ‘Guide to Conducting a National Proliferation Financing Risk Assessment’, RUSI, Май 2019 г.

BitAML, ‘Cryptocompliance 101: Do You Need a Risk Assessment? In Crypto, the Answer Is Yes’, 28 январь 2019 г., <https://bitaml.com/2019/01/28/risk-assessment-crypto/>.

FATF, ‘Guidance on Proliferation Financing Risk Assessment and Mitigation’, Июнь 2021 г., <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf>.

Government of the Grand Duchy of Luxembourg Ministry of Justice, ‘ML/TF Vertical Risk Assessment: Virtual Asset Service Providers’, Декабрь 2020 г., <https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/ML-TF-vertical-risk-assessment-on-VASPs.pdf>.

New Zealand Government Department of Internal Affairs, 'Financial Institutions Sector Risk Assessment', Part 19: Sector Risks – Virtual Asset Service Providers, Декабрь 2019 г., <https://static1.squarespace.com/static/5a77b9d390bade7aa2cf8692/t/600e144cc42d5b31a3ccc997/1611535442275/Financial-Institutions-SRA-2019.pdf>.

Индикаторы высокого риска и тревожные признаки

Chainalysis, 'The Chainalysis 2021 Crypto Crime Report', Март 2021 г., <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>.

Elliptic, 'Sanctions Compliance in Cryptocurrencies: Using Blockchain Analysis to Navigate the Minefield', Май 2021 г., <https://www.elliptic.co/hubfs/downloads/Elliptic_Sanctions-Compliance-In_Crypto.pdf>.

FATF, 'Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing', Сентябрь 2020 г., <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>.

Government of Canada Financial Transactions and Reports Analysis Centre of Canada (FinTRAC), 'Money Laundering and Terrorist Financing Indicators – Virtual Currency Transactions', Декабрь 2020 г., <https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng>.

US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), 'Advisory on Illicit Activity Involving Convertible Virtual Currency', 9 Май 2019 г., <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>.

Additional Sources for Sanctions Screening

Australian Government Department of Foreign Affairs and Trade Sanctions, 'Australia and Sanctions', <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>.

EU External Action Service, 'Consolidated List of Sanctions', <https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions>.

Government of Canada, 'Consolidated Canadian Autonomous Sanctions List', <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng>.

Japan Ministry of Economy, Trade and Industry, 'Sanctions List', <https://www.meti.go.jp/english/>.

UK HM Treasury Office of Financial Sanctions Implementation, 'Consolidated Sanctions List', <https://sanctionssearch.ofsi.hmtreasury.gov.uk/>.

UN Security Council, 'Consolidated List', <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>.

UN Security Council, 'Panel of Experts 1718 Sanctions Committee (DPRK) Reports', <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports>.

US Office of Foreign Assets Control, 'Sanctions List Search', <https://sanctionssearch.ofac.treas.gov/>.