



Евразийская группа по противодействию легализации
преступных доходов
и финансированию терроризма

Eurasian Group on Combating Money Laundering
and Financing of Terrorism

ТИПОЛОГИЧЕСКИЙ ПРОЕКТ

МОНИТОРИНГ РИСКОВ ИСПОЛЬЗОВАНИЯ ВИРТУАЛЬНЫХ АКТИВОВ В ПРЕСТУПНЫХ ЦЕЛЯХ

2024

Мониторинг рисков использования виртуальных активов в преступных целях

Оглавление

Введение	2
Оценка уровня развития индустрии виртуальных активов	4
Угрозы, связанные с использованием виртуальных активов	18
Уязвимости в части развития рынка виртуальных активов.....	20
Риски использования виртуальных активов в преступных целях	31
Инструменты противодействия преступной деятельности, связанной с использованием виртуальных активов.....	32
Минимизация рисков и угроз, связанных с виртуальными активами	38
Приложение 1. Примеры противоправного применения виртуальных активов	73
Приложение 2. Свод рекомендаций	78

Введение

Внедрение новых финансовых технологий, продуктов и услуг может повлечь значительные возможности для развития экономики (в том числе на макроуровне). Вместе с тем, возрастают риски¹ использования платежных инструментов в преступных целях, в том числе в схемах ОД/ФТ.

Актуальная повестка дня в сфере расширения мировых криптовалютных рынков становится все более ориентированной на проблему выявления и минимизации рисков и угроз их использования в преступных целях. Это объясняется вовлечением все большего числа лиц в деятельность преступных группировок, функционирующих на рынках платежных инструментов. Несмотря на значительный рост использования виртуальных активов в незаконных целях, во многих странах отсутствует гармонизация нормативно-правового регулирования криптовалютного рынка.

Согласно «Целевому обновлению информации об имплементации стандартов ФАТФ по виртуальным активам и провайдерам услуг виртуальных активов» (ФАТФ, 2024 г.), виртуальные активы применяются в целях финансирования терроризма и оружия массового уничтожения, мошенничества и других преступлений. Значительную частоту имеют взлом кошельков, хищение виртуальных активов, применение схем отмывания преступных доходов. Применение виртуальных активов для финансирования террористической деятельности отмечается в Азии и на Ближнем Востоке, в частности, в Сирии.

Кроме того, возрастает частота использования стейблкоинов для целей отмывания преступных доходов, финансирования терроризма, распространения оружия массового уничтожения. ФАТФ приводит информацию об участившихся случаях взлома механизмов децентрализованных финансов (DeFi).

Отдельно отмечается недостаточный уровень внедрения Рекомендаций ФАТФ в части законодательного регулирования выпуска и (или) оборота виртуальных активов, в том числе для минимизации рисков их противоправного применения.

Это способствует широкому применению указанных инструментов преступными группами для совершения деяний, имеющих широкий общественный резонанс. Среди них – незаконный оборот наркотиков, сбор и перемещение средств на финансирование террористических и экстремистских группировок (в том числе действующих в зонах повышенной

¹ Указанная проблематика отмечается в резолюции Совета Безопасности ООН 2462 (2019)

террористической активности), материальная подпитка деструктивной деятельности и др.

С целью сокрытия истинных целей и источников средств, преступниками применяются различные схемы:

- веерное распыление, в том числе с использованием большого количества криптовалютных кошельков, заведенных подставными лицами;
- использование миксеров и обменных платформ;
- вывод средств на анонимные кошельки и криптовалютные площадки;
- применение максимально анонимных виртуальных валют (Monero, ZCash и другие).

В преступных схемах (в том числе в рамках финансирования терроризма²) отмечается также рост случаев использования криптовалют с повышенной анонимностью (privacy coins).

В ходе реализации проекта достигнуты следующие цели, определенные в концептуальной записке:

1. Классифицированы риски, предикатные преступления, связанные с использованием виртуальных активов для ОД/ФТ, уязвимости и угрозы интенсивного развития отрасли виртуальных валют в государствах-членах и заинтересованных государствах-наблюдателях ЕАГ, включая вопросы региональных тенденций и типологий.
2. Проведен анализ практик государств-членов и наблюдателей ЕАГ в части минимизации рисков использования виртуальных активов в противоправной деятельности.
3. Установлены информационные источники, позволяющие улучшить результативность при проведении финансовых расследований в рамках мониторинга виртуальных активов.
4. Оценены возможности и направления межведомственного взаимодействия, включая роли компетентных органов и представителей частного сектора в сфере предотвращения использования виртуальных активов в преступных целях.
5. Определены направления минимизации выявленных рисков с учетом национального законодательства государств-членов и наблюдателей ЕАГ.

² По данным тридцать четвертого доклада Группы по аналитической поддержке и санкциям «Аль-Каиды» Совета Безопасности ООН, отмечается рост использования криптовалют с повышенной анонимностью ИГИЛ и ее филиалами

В типологическом исследовании приняли участие Азербайджанская Республика³, Республика Армения, Республика Беларусь, Республика Индия, Республика Казахстан, Кыргызская Республика, Монголия, Российская Федерация, Республика Сербия, Республика Таджикистан, Туркменистан, Республика Узбекистан, АТЦ СНГ.

Оценка уровня развития индустрии виртуальных активов

Государства-участники типологического проекта выделяют технологические и финансово-экономические критерии развития рынка виртуальных активов.

Технологические критерии:

- готовность инфраструктуры для развития блокчейн технологий;
- использование цифровых идентификаторов в повседневной деятельности;
- доступность финансовых услуг, оказываемых в цифровом пространстве в сети Интернет.

Финансово-экономические критерии, по которым оценивается уровень развития рынка виртуальных активов в Республиках Казахстан, Беларусь, Узбекистан, Сербия, Кыргызской Республике и Монголии:

- степень вовлеченности граждан и юридических лиц в оборот и объем виртуальных активов;
- объем финансовых операций, связанных с виртуальными активами;
- количество поставщиков услуг виртуальных активов, в том числе лицензированных;
- количество эмитентов виртуальных активов;
- объем инвестиций в сектор виртуальных активов;
- наличие профессиональных игроков рынка криптовалют;
- использование виртуальных активов в качестве платежного средства;
- количество лицензий, выданных для криптовалютных бирж;
- количество виртуальных активов, активно используемых/торгуемых в отрасли;
- число провайдеров услуг виртуальных активов, предоставляющих услуги на международном и национальном уровнях;

³ По линии работы с АТЦ СНГ

- разнообразие и развитие проектов и услуг, использующих виртуальные активы.

Нормативно-правовое регулирование рынка виртуальных активов

Республика Беларусь

В Республике Беларусь действует Декрет Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики». Декретом установлен перечень разрешенных финансовых операций с цифровыми знаками (токенами) и условия их совершения.

Действуют специальные нормативно-правовые акты в сфере развития цифровой экономики и деятельности резидентов Парка высоких технологий:

- Декрет Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики».
- Декрет Президента Республики Беларусь от 22.09.2005 № 12 «О Парке высоких технологий».

Вопросы регулирования сферы виртуальных активов содержатся также в следующих общих законодательных актах, регулирующих операции на финансовом рынке, деятельность платежных систем, а также лиц, осуществляющих финансовые операции:

- Постановление Правления Национального банка Республики Беларусь от 16.09.2022 № 350 «Об утверждении правил осуществления операций с электронными деньгами».
- Закон Республики Беларусь от 19.04.2022 № 164-З «О платежных системах и платежных услугах».
- Указ Президента Республики Беларусь от 06.07.2021 № 260 «О лицах, осуществляющих финансовые операции».
- Закон Республики Беларусь от 30 июня 2014 г. № 165-З «О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения».
- Приказ Министерства связи и информатизации Республики Беларусь от 18.11.2021 № 293 «О критериях оценки степени риска в целях отбора операторов электросвязи и операторов почтовой связи для проведения выборочной проверки».
- Налоговый кодекс Республики Беларусь (Общая часть, Особенная

часть).

- Банковский кодекс Республики Беларусь.
- Закон Республики Беларусь от 24.10.2016 № 439-З «Об исполнительном производстве».
- Декрет Президента Республики Беларусь от 28.12.2014 № 6 «О неотложных мерах по противодействию незаконному обороту наркотиков».
- Указ Президента Республики Беларусь от 16.01.2009 № 40 «О Фонде социальной защиты населения Министерства труда и социальной защиты».
- Указ Президента Республики Беларусь от 29.04.2020 № 150 «О расходных операциях».
- Указ Президента Республики Беларусь от 07.08.2018 № 305 «О совершенствовании правового регулирования игорного бизнеса».
- Указ Президента Республики Беларусь от 16.10.2018 № 414 «О совершенствовании безналичных расчетов».
- Постановление Совета Министров Республики Беларусь, Национального банка Республики Беларусь от 28.06.2019 № 432/11 «Об автоматизированной информационной системе исполнения денежных обязательств» (вместе с «Положением о порядке осуществления безналичных расчетов посредством автоматизированной информационной системы исполнения денежных обязательств и ее функционирования»).
- Постановление Совета Министров Республики Беларусь, Национального банка Республики Беларусь от 06.07.2011 № 924/16 «Об использовании кассового и иного оборудования при приеме средств платежа» (вместе с «Положением об использовании кассового и иного оборудования при приеме средств платежа»).
- Постановление Совета Министров Республики Беларусь от 16 сентября 2016 № 735 «Об утверждении Положения о порядке применения мер, связанных с замораживанием средств и (или) блокированием финансовых операций лиц, причастных к террористической деятельности».
- Постановление Совета Министров Республики Беларусь от 23 ноября 2016 г. № 954 «Об утверждении положения о порядке приостановления и возобновления финансовых операций органом финансового мониторинга с лицами, осуществляющими финансовые операции».

- Постановление Правления Национального банка Республики Беларусь от 24.12.2014 № 818 «О внутреннем контроле при осуществлении банковских операций» (вместе с «Инструкцией о требованиях к правилам внутреннего контроля в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения при осуществлении банковских операций»).
- Постановление Совета Министров Республики Беларусь, Национального банка Республики Беларусь от 22.12.2022 № 902/28 «О реестре поставщиков платежных услуг и видов оказываемых ими платежных услуг» (вместе с «Положением о порядке формирования и ведения реестра поставщиков платежных услуг и видов оказываемых ими платежных услуг»).
- Постановление Правления Национального банка Республики Беларусь от 05.12.2022 № 453 «Об утверждении Инструкции о порядке оказания платежных услуг на территории Республики Беларусь».
- Постановление Правления Национального банка Республики Беларусь от 13.09.2022 № 342 «Об утверждении Правил осуществления операций с платежным программным приложением и иными платежными инструментами».
- Постановление Министерства юстиции Республики Беларусь от 07.04.2017 № 67 «Об утверждении Инструкции по исполнительному производству».
- Постановление Совета Министров Республики Беларусь от 16.03.2006 № 367 «Об утверждении формы специального формуляра регистрации финансовой операции, подлежащей особому контролю, и инструкции о порядке заполнения, представления, регистрации, учета и хранения специальных формуляров регистрации финансовых операций, подлежащих особому контролю».
- Постановление Министерства финансов Республики Беларусь от 06.03.2018 № 16 «О бухгалтерском учете цифровых знаков (токенов)» – порядок формирования в бухгалтерском учете информации о цифровых знаках (токенах) и обязательствах, возникающих при размещении собственных токенов перед владельцами этих токенов, в организациях (за исключением Национального банка, банков, открытого акционерного общества «Банк развития Республики Беларусь»,

небанковских кредитно-финансовых организаций, банковских групп, банковских холдингов, бюджетных организаций).

Кроме того, в отношении резидентов Парка высоких технологий применяются специальные правила:

- Акты Наблюдательного совета Парка высоких технологий (<https://www.park.by/http/legislation/>), в том числе:
- Положение о требованиях, которым должны соответствовать отдельные заявители для регистрации их в качестве резидентов Парка высоких технологий;
- Правила осуществления деятельности оператора криптоплатформы;
- Правила осуществления деятельности оператора обмена криптовалютой;
- Правила оказания услуг, связанных с созданием и размещением цифровых знаков (токенов), и осуществления операций по созданию и размещению собственных цифровых знаков (токенов);

Принят Указ Президента Республики Беларусь от 14.02.2022 № 48 «О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты», содержащий перечень кошельков, вовлеченных в противоправную деятельность.

Республика Казахстан

В Республике Казахстан требования к провайдерам услуг виртуальных активов устанавливаются и их соблюдение регулируется согласно закону Республики Казахстан от 6 февраля 2023 года № 193-VIIЗРК «О цифровых активах в Республике Казахстан».

В Республике Казахстан и Кыргызской Республике законодательно разрешены майнинг, покупка и продажа (обмен) виртуальных активов, хранение, управление и контроль виртуальных активов, эмиссия и первичное размещение виртуальных активов; оказание финансовых услуг, связанных с первичным размещением и (или) продажей виртуальных активов эмитента.

Вопросы регулирования сферы виртуальных активов содержатся также в следующих нормативных актах:

1. Закон Республики Казахстан «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (от 28 августа 2009 года № 191-IV).
2. Совместный приказ Председателя Агентства Республики Казахстан по финансовому мониторингу от 16 августа 2021 года № 7 и Министра национальной экономики Республики Казахстан от 16 августа 2021 года

- № 80 – «Об утверждении критериев оценки степени риска и проверочного листа за соблюдением законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Примечание: цифровые активы являются формой имущества, в связи с чем любые соответствующие критерии применимы к ВА/ЦА.
3. Совместный приказ Председателя Агентства Республики Казахстан по финансовому мониторингу от 28 февраля 2022 года № 20 и Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 28 февраля 2022 года № 68/НК. Зарегистрирован в Министерстве юстиции Республики Казахстан 2 марта 2022 года № 26981. «Об утверждении Требований к правилам внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения для лиц, осуществляющих деятельность по выпуску цифровых активов, организации торгов ими, а также предоставлению услуг по обмену цифровых активов на деньги, ценности и иное имущество» - профильный ПВК.
4. Приказ Председателя Агентства Республики Казахстан по финансовому мониторингу от 22 февраля 2022 года № 13. Зарегистрирован в Министерстве юстиции Республики Казахстан 24 февраля 2022 года № 26924. «Об утверждении Правил представления субъектами финансового мониторинга сведений и информации об операциях, подлежащих финансовому мониторингу, и признаков определения подозрительной операции» - правила предоставления информации от СФМ в ПФР, в том числе от лицензированных ПУВА.

Кыргызская Республика

Согласно статье 29 Закона Кыргызской Республики от 21 января 2022 года № 12 «О виртуальных активах», уполномоченным органом выдается лицензия на осуществление деятельности поставщика услуг виртуальных активов. Срок действия указанной лицензии не ограничен. К поставщикам услуг виртуальных активов предъявляются требования:

- наличие функционирующей Платформы, размещенной на серверах, расположенных на территории Кыргызской Республики, и соответствующей требованиям, предусмотренным законодательством;

- наличие копии документов, удостоверяющих личность руководителей, учредителей и бенефициарных владельцев юридического лица – поставщика услуг виртуальных активов.

Надзор и регулирование деятельности операторов торгов виртуальных активов (криптовбирж) и других поставщиков услуг виртуальных активов осуществляет Служба регулирования и надзора за финансовым рынком при Министерстве экономики и коммерции Кыргызской Республики.

ПУВА были включены в список субъектов системы ПОД/ФТ как подотчетные организации. В связи с чем порядок взаимодействия ПУВА с ПФР осуществляется на общих основаниях. Закон КР о ПФТД/ЛПД от 06.08.2018 №87:

- Статья 9. «Представление и защита информации и документов»;
- Статья 11. Оценка рисков ФТД, ФРОМУ и ЛПД. Подпункт 1, пункта 4, Положения о Комиссии по вопросам ПФТД и ЛПД, утвержденное Постановлением Правительства КР от 25.12.2018 №606.
- Положение о порядке проведения оценки рисков ФТД и ЛПД, утвержденное Постановлением Правительства КР от 25.12.2018 №606. Протокол заседания Комиссии по вопросам ПФТД и ЛПД от 02.03.2023 г. №5 «о проведении оценки рисков в секторе ВА и ПУВА».

Российская Федерация

Отношения, возникающие при обороте цифровых активов и цифровой валюты, в Российской Федерации регулируются Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

В соответствии со статьей 5 Федерального закона № 115-ФЗ операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, и операторы обмена цифровых финансовых активов отнесены к организациям, осуществляющим операции с денежными средствами или иным имуществом (далее - организации). Таким образом, на них в полном объеме распространяются требования, предусмотренные Федеральным законом № 115-ФЗ.

Операторы информационной системы, в которой реализуется выпуск ЦФА, и операторы обмена ЦФА, как субъекты законодательства о ПОД/ФТ, направляют в ПФР информацию в рамках обязательного контроля операций

(статья 6 Федерального закона № 115-ФЗ), на них распространяются требования по идентификации клиентов, направлению СПО и отнесению клиентов к одной из трех групп риска в зависимости от степени риска совершения юридическими лицами подозрительных операций (статья 7 Федерального закона № 115-ФЗ).

В части оценки рисков, согласно требованиям п. 5.14 ст. 7 Федерального закона № 115-ФЗ, организации, осуществляющие операции с денежными средствами или иным имуществом до предоставления новых услуг и (или) программно-технических средств, обеспечивающих возможность совершения клиентами операций с денежными средствами или иным имуществом, обязаны оценивать возможность использования таких услуг и (или) программно-технических средств в целях ОД/ФТ и по результатам этой оценки принимать меры, направленные на снижение (минимизацию) данной возможности. В соответствии с этими положениями организации должны оценивать риски совершения своими клиентами операций в целях ОД/ФТ, принимая во внимание, в частности, результаты НОР и виды используемых продуктов (услуг). Соответствующие требования должны включаться в правила внутреннего контроля.

Меры по управлению рисками и их снижению содержатся в главе 4 Положения Банка России от 02.03.2012 № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Аналогичные требования для некредитных организаций содержатся в главе 4 Положения Банка России от 15.12.2014 № 445-П.

Для разъяснения вопросов в части оценки рисков клиентов организациями действует информационное письмо Росфинмониторинга от 01.03.2019 № 59 «О методических рекомендациях по проведению оценки рисков ОД/ФТ организациями, осуществляющими операции с денежными средствами или иным имуществом и индивидуальными предпринимателями». Также информация содержится в Отчете о прогрессе Российской Федерации 2023 г. по критерию 15.3(с).

Для целей Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» цифровая валюта признается имуществом. В Российской Федерации запрещается распространение информации о предложении и (или) приеме цифровой

валюты в качестве встречного предоставления за передаваемые ими (им) товары, выполняемые ими (им) работы, оказываемые ими (им) услуги или иного способа, позволяющего предполагать оплату цифровой валютой товаров (работ, услуг) (п. 5, 7 ст. 14 Федерального закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»).

Федеральный закон от 8 августа 2024 г. № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» регулирует вопросы майнинга (эмиссии) цифровой валюты в Российской Федерации (вступил в силу с 19 августа 2024 года, положения, касающиеся ведения реестров операторов майнинговой инфраструктуры и лиц, осуществляющих майнинг цифровой валюты, а также контроля за выполнением ими установленных требований, начнут действовать с 1 ноября 2024 года). Предмет регулирования и сфера действия указанного Федерального закона: майнинг цифровой валюты, деятельность майнинг-пулов и лиц, организующих её, майнинговая инфраструктура и оператор майнинговой инфраструктуры. Дополнительно вводится понятие адреса-идентификатора – уникальная последовательность символов, предназначенная для учета в информационной системе приходных и расходных операций с цифровой валютой.

Указанный Федеральный закон устанавливает запрет на рекламу цифровой валюты и любых товаров, работ и услуг, в целях организации обращения и (или) обращения цифровой валюты. Операторы майнинговой инфраструктуры и лица, осуществляющие майнинг цифровой валюты, будут включаться в специальные реестры. При этом неоднократное в течение года нарушение требований антиотмывочного законодательства Российской Федерации будет являться основанием для исключения из указанного реестра.

Кроме того, для индивидуальных предпринимателей, имеющих неснятую или непогашенную судимость, устанавливается запрет на осуществление майнинга, в том числе в качестве участника майнинг-пула. Обозначенный запрет распространяется и на юридические лица в случае, если они сами или их учредители, участники, бенефициарные владельцы или генеральный директор не соответствуют требованиям к деловой репутации в части отсутствия неснятой или непогашенной судимости.

Федеральный закон от 8 августа 2024 года № 223-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»

предусматривает модернизацию подходов к установлению экспериментальных правовых режимов (ЭПР) в сфере цифровых инноваций.

Вопросы регулирования сферы виртуальных активов содержатся также в следующих нормативных актах:

- Федеральный закон от 11 марта 2024 г. № 45-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» об использовании цифровых финансовых активов для международных расчетов.
- Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».
- Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг».
- Федеральный закон от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)».
- Федеральный закон от 02.10.2007 № 229-ФЗ «Об исполнительном производстве».
- Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции».
- Федеральный закон от 03.12.2012 № 230-ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам».
- Федеральный закон от 07.05.2013 № 79-ФЗ «О запрете отдельным категориям лиц открывать и иметь счета (вклады), хранить наличные денежные средства и ценности в иностранных банках, расположенных за пределами территории Российской Федерации, владеть и (или) пользоваться иностранными финансовыми инструментами».
- Указ Президента Российской Федерации от 10 декабря 2020 года № 778 «О мерах по реализации отдельных положений федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».
- Указание Центрального банка Российской Федерации от 3 декабря 2020 г. № 5646-У «О случаях и порядке зачисления цифровых финансовых активов номинальному держателю цифровых финансовых активов, который учитывает права на цифровые финансовые активы, принадлежащие иным лицам».
- Письмо Министерства труда и социальной защиты Российской Федерации от 16 декабря 2020 г. № 18-2/10/В-12085 «О возможности

приобретения цифровых финансовых активов и цифровой валюты и владения ими отдельными категориями лиц».

В Отчете о национальной оценке рисков финансирования терроризма 2022 года содержится информация о рисках, связанных с виртуальными активами, в нем выделен отдельный раздел «Перемещение средств на финансирование террористической деятельности с использованием виртуальных активов».

В разделе 3.1 Отчета о национальной оценке рисков легализации (отмывания) доходов, полученных преступным путем 2022 года описаны риски использования виртуальных активов в целях отмывания преступных доходов.

Туркменистан

Законодательство Туркменистана прямо не запрещает, но и не регулирует деятельность ПУВА.

Республика Узбекистан

Уполномоченным органом по развитию сферы оборота криптовалютных активов, а также лицензированию и разрешительным процедурам определено Национальное агентство перспективных проектов Республики Узбекистан. Полномочия Агентства:

- определение порядка лицензирования и прохождения разрешительных процедур в сфере оборота криптовалютных активов;
- определение размеров и порядка уплаты государственной пошлины за выдачу лицензии на осуществление деятельности в сфере оборота криптовалютных активов.

Нормативно-правовые акты, регулирующие выпуск и оборот криптовалютных активов в Республике Узбекистан:

- Положение о порядке выпуска, регистрации выпуска и обращения крипто-активов резидентами Республики Узбекистан (рег. МЮ № 3397 от 28 ноября 2022 года);
- Положение о порядке регистрации участников Специального режима регулирования в сфере оборота крипто-активов (Специальный режим «регуляторной песочницы») (рег. МЮ № 3409 от 30 декабря 2022 года);
- Положение о порядке выдачи разрешения для осуществления деятельности по майнингу (рег. МЮ № 3461 от 29 сентября 2023 года);

- Правила осуществления торгов крипто-активами на крипто-бирже (рег. МЮ № 3379 от 15 августа 2022 года);
- Положение о порядке лицензирования деятельности провайдеров услуг в сфере оборота крипто-активов (рег. МЮ № 3380 от 15 августа 2022 года);
- Положение об установлении размеров сборов за осуществление деятельности в сфере оборота крипто-активов, порядке их уплаты и распределения (рег. МЮ № 3388 от 28 сентября 2022 года);
- Правила осуществления деятельности крипто-магазина (рег. МЮ № 3395 от 31 октября 2022 года);
- Указ Президента Республики Узбекистан от 24 июля 2017 года № УП-5120 «О мерах по внедрению системы проектного управления в Республике Узбекистан»;
- Постановление Президента Республики Узбекистан от 27 июля 2017 года № ПП-3150 «Об организации деятельности Национального агентства перспективных проектов Республики Узбекистан»;
- Постановление Президента Республики Узбекистан от 3 июля 2018 года № ПП-3832 «О мерах по развитию цифровой экономики и сферы оборота крипто-активов в Республике Узбекистан»;
- Постановление Президента Республики Узбекистан от 2 сентября 2018 года № ПП-3926 «О мерах по организации деятельности крипто-бирж в Республике Узбекистан»;
- Правила внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения для лиц, осуществляющих деятельность в области оборота крипто-активов (рег. МЮ № 3309 от 9 июня 2021 года);
- Правила внутреннего контроля для лиц, осуществляющих деятельность в сфере оборота крипто-активов. (<http://lex.uz/uz/docs/5450936>);
- ПКМ №402 от 29.06.2021 года «О дополнительных мерах по реализации Закона Республики Узбекистан «О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения»» (<http://lex.uz/uz/docs/5489518>);
- Законы Республики Узбекистан «О государственной пошлине», «О лицензировании, разрешительных и уведомительных процедурах», «О противодействии легализации доходов, полученных от преступной

деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения».

Майнинг в Узбекистане – вид деятельности, не подлежащий обязательному лицензированию, но в установленном порядке лицензируется деятельность провайдеров услуг виртуальных активов:

- крипто-биржи;
- майнинг-пулы;
- крипто-депозитарии;
- крипто-магазины.

Рекомендуемые меры:

Государствам и организациям, являющимся членами или наблюдателями в ЕАГ, рекомендуется при проведении оценки уровня развития индустрии виртуальных активов обращать особое внимание на следующие критерии:

- *нормативно-правовой базы;*
- *степени вовлеченности граждан и юридических лиц в выпуск, оборот, обмен виртуальных активов;*
- *деятельность провайдеров услуг виртуальных активов, включая способы их регистрации в специальных реестрах (в случае наличия разрешительных механизмов).*

Практика декларирования доходов, полученных от обмена/оборота виртуальных активов или обладания виртуальными активами для целей налогообложения

Доходы от операций с виртуальными активами (обмен, оборот) декларируются в Кыргызской Республике, Казахстане, Сербии, Монголии. Практика декларирования подобных доходов отсутствует в Беларуси, Узбекистане, Туркменистане, Таджикистане.

Республика Беларусь

В Республике Беларусь токены не подлежат декларированию. Кроме того, согласно подпункту 3.1 пункта 3 Декрета Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики», доходы физических лиц от деятельности по майнингу, приобретения (в том числе в порядке дарения), отчуждения токенов за белорусские рубли, иностранную

валюту, электронные деньги и (или) обмена на иные токены не признаются объектом налогообложения подоходным налогом с физических лиц.

Республика Казахстан

Налоговое законодательство Республики Казахстан не предусматривает всеобщего декларирования, как и декларирования цифровых активов, в частности. Вместе с тем статья 8 Налогового кодекса Республики Казахстан устанавливает презумпцию «добросовестности налогоплательщика», то есть подразумевается, что налогоплательщик действует добросовестно и порядочно, не укрывает свой доход и своевременно уплачивает подоходные налоги. Лицензированными ПУВА МФЦА налажена работа с Комитетом государственных доходов Министерства финансов РК, налогообложение физических лиц – налоговых резидентов Казахстана, получившие доход при реализации имущества (цифровых активов), должно самостоятельно задекларировать доход от прироста стоимости имущества путём заполнения формы налоговой отчётности.

Юридические лица, имеющие регистрацию в органах государственных доходов Казахстана (например, майнеры), должны включить доход от реализации цифровых активов в совокупный годовой компании и после применения всех вычетов и корректировок, предусмотренных налоговым законодательством страны, уплатить корпоративный подоходный налог по ставке 20%. Важно отметить, что, инвестируя через лицензированного ПУВА, зарегистрированного в МФЦА, клиент получит выписку о совершенных операциях, а также может распечатать договор публичной оферты с сайта, более того, может запросить акт выполненных работ (оказанных услуг) и счет-фактуру из бухгалтерии официального ПУВА.

Таким образом, у клиента лицензированного ПУВА будут документы, подтверждающие его доход от прироста стоимости при реализации цифровых активов, а своевременная и полная уплата налогов и других обязательных платежей придает данному доходу законность и прозрачность.

Республика Узбекистан

Постановлением Президента Республики Узбекистан от 3 июля 2018 года № ПП-3832 «О мерах по развитию цифровой экономики и сферы оборота крипто-активов в Республике Узбекистан» определено, что операции юридических и физических лиц, связанные с оборотом крипто-активов, в том числе осуществляемые нерезидентами, не являются объектами налогообложения, а

доходы, полученные по данным операциям, не включаются в налогооблагаемую базу по налогам и другим обязательным платежам.

Вместе с тем, Министерством финансов и Государственным налоговым комитетом Республики Узбекистан принято информационное сообщение о порядке бухгалтерского учета операций с крипто-активами (№ 06/17-01-32/278 и № 2022-42 от 14 декабря 2022 года), предусматривающее разъяснение порядка учета операций с крипто-активами, в частности, операций по майнингу, покупке или продаже крипто-активов.

На сегодняшний день, законодательство Республики Узбекистан не предусматривает практику декларирования доходов граждан, полученных от оборота крипто-активов.

Между тем, налоговая отчетность, необходимая для предоставления в налоговые органы, направляется в установленном законодательством порядке.

Монголия

Налогоплательщик (эмитент, поставщик услуг, участник торговли виртуальными активами) обязан произвести уплату в бюджет в установленные Законом сроки.

В соответствии с Законом о поставщиках услуг виртуальных активов, утвержденным Парламентом Монголии, виртуальные активы определяются как «нематериальное цифровое представление стоимости, которое может быть предметом цифровой торговли или передачи и может быть использовано в платежных или инвестиционных целях».

Механизмы подтверждения фактов обладания виртуальными активами для целей налогообложения имеются в Сербии и Монголии.

Рекомендация:

Определять порядок декларирования дохода от обмена/оборота виртуальных активов, а также фактов обладания виртуальными активами в соответствии с национальным налоговым законодательством.

Угрозы, связанные с использованием виртуальных активов

Участниками типологического проекта отмечается достаточно частое использование виртуальных активов как в рамках осуществления предикатных преступлений и отмыwania полученных доходов, так и для целей финансирования террористической деятельности (средняя доля около 13%).

Участники типологического проекта отмечают факты использования виртуальных активов преимущественно для целей совершения следующих предикатных преступлений:

- мошенничество;
- незаконный оборот наркотиков;
- организация финансовых пирамид;
- незаконная предпринимательская деятельность.

По представленным данным, менее распространены случаи использования виртуальных активов при совершении преступлений, связанных с коррупцией, уклонением от уплаты налогов, хищением государственных средств и др. При этом отмечаются факты использования указанных инструментов для совершения общеуголовных преступлений – в частности, кражи (причем доля таких преступлений, по оценке разных государств-членов, варьируется от незначительной до весьма значимой).

Указанные преступления также являются источником преступных доходов, которые впоследствии отмываются с использованием виртуальных активов.

В свою очередь, участниками проекта отмечено, что организованными группами с использованием виртуальных активов чаще остальных совершаются преступления, связанные с:

- мошенничеством;
- незаконным оборотом наркотиков;
- организацией финансовых пирамид;
- незаконной предпринимательской деятельностью;
- общеуголовными деяниями (кража, взлом).

Для совершения преступлений с применением виртуальных активов в первую очередь используются:

- Биткоин;
- Альткоины биткойна;
- Стейблкоины;
- Иные токены криптовалют.

Уязвимости в части развития рынка виртуальных активов

Участники исследования отмечают наличие проблем законодательного, технологического и организационного характера при осуществлении надзора за деятельностью ПУВА.

Среди наиболее распространенных уязвимостей – экстерриториальный характер виртуальных активов и связанные с этим технические сложности выявления и блокирования компетентными органами отдельно взятой страны транзакций, совершаемых с использованием зарубежных криптобирж, не имеющих лицензии в стране, высокая анонимность проводимых транзакций (которая поддерживается большим количеством дополнительных механизмов, затрудняющих отслеживание цепочек по переводу средств и выявление конечных бенефициарных владельцев), несовершенство законодательного регулирования вопросов выпуска и обращения виртуальных активов, отсутствие конкретных признаков подозрительности для частного сектора, недостаточный опыт работы правоохранительных органов по выявлению и расследованию случаев использования виртуальных активов в преступной деятельности, неэффективная реализация риск-ориентированного подхода в надзоре за ПУВА, отсутствие постоянного обучения и практических руководств для лиц, задействованных в работе по выявлению и пресечению подозрительной деятельности с использованием виртуальных активов, отсутствие специализированного оборудования и программного обеспечения для отслеживания транзакций с виртуальными активами.

Проблематика недостаточной урегулированности использования виртуальных активов на территории государств ЕАГ отмечается и по итогам проведения наднациональной оценки рисков ОД/ФТ в Евразийском регионе⁴.

Республика Беларусь

При выявлении подозрительных операций возникают затруднения в части идентификации конечного бенефициара, а также с оценкой риска применения вновь созданного адреса (идентификатора) виртуального кошелька для осуществления противоправной деятельности или участия в ней. Кроме того, могут использоваться подставные лица (дропы), что создает дополнительные сложности при попытке идентифицировать и отслеживать подозрительные транзакции. В последнее время наблюдается устойчивая тенденция к

⁴ Отчет о проведении оценки рисков ОД/ФТ в Евразийском регионе в 2022 году доступен на официальном сайте ЕАГ: https://eurasiangroup.org/files/uploads/files/Резюме_POP.pdf

использованию аккаунтов, зарегистрированных на дропов, для осуществления единичных транзакций.

Отмечается сложность в своевременном выявлении аккаунтов, переданных в пользование третьим лицам с целью отмывания преступных доходов, полученных в результате мошеннических действий. Выявить такие аккаунты, в основной массе, представляется возможным уже после совершения финансовых операций.

Республика Казахстан

- 1) Технические сложности: Мониторинг и контроль за виртуальными активами требуют специализированных знаний в области блокчейна, криптографии и кибербезопасности, а также специализированного оборудования и программного обеспечения для анализа данных.
- 2) Анонимность и конфиденциальность: Виртуальные активы могут быть анонимными, что затрудняет идентификацию пользователей и отслеживание транзакций.
- 3) Международные аспекты: Виртуальные активы оперируют в международном пространстве, и контроль за ними требует сотрудничества между разными странами и организациями.
- 4) Обучение и образование: потенциальная нехватка комплаенс-специалистов блокчейн-аналитики и отсутствие соответствующего аналитического инструментария.
- 5) В связи с тем, что нелицензированные ПУВА (осуществляющие деятельность за пределами МФЦА без наличия соответствующей лицензии и в нарушение действующих законодательств ПОД/ФТ и регулирования цифровых активов), не являются субъектами финансового мониторинга и, следовательно, не исполняют антиотмывочные обязательства, такие как: направление СПО, регистрация в АФМ и регистрации как предприятия, иным субъектам финансового мониторинга при взаимодействии со своими клиентами приходится проводить углубленные проверки, при наличии подозрений, что клиент является нелицензированным ПУВА (пример, физическое лицо предоставляющее платные услуги по обмену цифровых активов/цифровых валют без предъявления лицензии). В таких случаях клиент не заинтересован в разглашении собственной противозаконной деятельности.

Кыргызская Республика

Кыргызской Республикой, помимо информации, представленной в рамках проекта, в 2023 году проведена отдельная оценка рисков, связанных с виртуальными активами и ПУВА⁵.

Российская Федерация

Согласно результатам национальной оценки рисков ОД/ФТ, проведенной Российской Федерацией в 2022 году⁶, использование виртуальных активов позволяет скрыть источник происхождения средств и конечного бенефициарного владельца, что существенно затрудняет возможность выявления использования виртуальных активов при осуществлении большинства экономических преступлений и финансирования терроризма.

На уровень уязвимости влияют следующие факторы:

- незавершенность законодательного регулирования сферы виртуальных активов;
- сложность получения информации о транзакциях с виртуальными активами, совершаемых провайдерами услуг виртуальных активов, зарегистрированными в иностранных юрисдикциях;
- легкость получения доступа к кошельку виртуальных активов через компьютер или мобильные устройства;
- технические сложности по получению ключа-доступа к цифровому кошельку, на котором хранятся виртуальные активы должника или подозреваемого/осужденного лица, при непредставлении данными лицами соответствующих сведений в добровольном порядке;
- недостаточный опыт работы правоохранительных органов по доказыванию фактов отмывания доходов с использованием виртуальных активов.

Рекомендуемые меры:

⁵ Отчет о проведении Кыргызской Республикой оценки рисков ОД/ФТ в секторе виртуальных активов и ПУВА в 2023 году размещен на официальном сайте ГСФР: <https://fiu.gov.kg/uploads/64d355f436421.pdf>

⁶ Отчеты о проведении Российской Федерацией национальной оценки рисков ОД/ФТ в 2022 году размещены на официальном сайте Росфинмониторинга: <https://www.fedsfm.ru/fm/nor>

- 1) Обеспечить проведение комплексной оценки рисков использования виртуальных активов и инфраструктуры их провайдеров (в рамках проведения очередных НОР или отдельного исследования);
- 2) Разработать для частного сектора признаки подозрительности транзакций, связанных с использованием виртуальных активов (например, в рамках обмена фиатных денег на криптовалюту и в обратном порядке);
- 3) Обеспечить надлежащий уровень риск-ориентированного подхода в надзоре за ПУВА;
- 4) Рассмотреть возможность внедрения единого специализированного программного обеспечения для отслеживания подозрительных транзакций, связанных с виртуальными активами;
- 5) Разработать методические материалы и обучающие курсы для правоохранительных органов и ПФР стран ЕАГ по выявлению и расследованию подозрительной деятельности с использованием виртуальных активов, а также применению риск-ориентированного подхода в отношении субъектов сектора;
- 6) Проработать вопросы эффективного ареста и конфискации виртуальных активов, используемых в рамках преступной деятельности.

Признаки подозрительности операций, связанных с использованием виртуальных активов

Республика Беларусь

Согласно Постановлению Правления Национального банка Республики Беларусь от 24.12.2014 № 818 (ред. от 19.11.2020) «О внутреннем контроле при осуществлении банковских операций» деятельность операторов криптоплатформ и операторов обмена криптовалют относится к факторам, повышающим степень риска работы с клиентом банка при оценке вектора «Риск по профилю клиента» трехвекторной модели распределения рисков. Систематически осуществляемые клиентом финансовые операции, связанные с приобретением и (или) отчуждением цифровых знаков (токенов) относятся к факторам, повышающим степень риска работы с клиентом банка при оценке вектора «Риск по видам операций».

Критериями выявления и признаками подозрительных финансовых операций являются:

- осуществление значительного количества финансовых операций по банковскому счету физического лица на общую сумму, равную или превышающую 2000 базовых величин за анализируемый период, без соответствующей государственной регистрации клиента в качестве субъекта предпринимательской деятельности либо в благотворительных целях, не подтвержденных документально.
- осуществление клиентом финансовой операции в размере, близком по значению или превышающем 2000 базовых величин, связанной с приобретением или отчуждением цифровых знаков (токенов) за белорусские рубли, иностранную валюту, электронные деньги у нерезидентов без участия резидента Парка высоких технологий.

Используются специальные коды для фиатных операций, связанных с покупкой/продажей виртуальных активов:

- 4203: приобретение цифровых знаков (токенов) за наличные денежные средства;
- 4204: приобретение цифровых знаков (токенов) за безналичные денежные средства, электронные деньги;
- 4205: отчуждение цифровых знаков (токенов) за наличные денежные средства;
- 4206: отчуждение цифровых знаков (токенов) за безналичные денежные средства, электронные деньги.

Республика Казахстан

В соответствии с Рекомендацией 15 ФАТФ, Комитетом МФЦА разработаны и внедрены «Критерии подозрительности операций с виртуальными активами (ВА) и провайдеров услуг в сфере виртуальных активов (ПУВА)».

В рамках Приказа Председателя Агентства Республики Казахстан по финансовому мониторингу от 22 февраля 2022 года № 13, «Об утверждении Правил представления субъектами финансового мониторинга сведений и информации об операциях, подлежащих финансовому мониторингу, и признаков определения подозрительной операции» предусмотрены коды по виду субъекта (в том числе ПУВА), и ряд актуальных СПО:

- «Систематические зачисления электронных денег лицом в адрес биржи цифровых активов, не осуществляющей деятельность на территории Международного финансового центра «Астана» либо получение фиатных средств со счетов криптобирж на счета физических лиц (продажа криптовалюты), с вероятностью связи с легализацией преступного дохода от незаконного оборота наркотиков»;
- «Совершение операций с адресами цифровых активов или банковскими картами, связанными с известными аферами мошенничества, вымогательством или применением программных средств»;
- «Клиент часто меняет свои идентификационные данные, включая адреса электронной почты, IP-адреса и финансовую информацию, либо осуществляет вход в систему предоставления услуг цифровых активов с разных IP-адресов, либо клиент неоднократно проводит операции с определенным кругом физических лиц, получая при этом значительную прибыль или убытки (что может свидетельствовать о завладении данными чужого счета и на попытку снятия остатка средств посредством торговли или о применении схемы отмывания доходов для сокрытия потоков средств)»;
- «Операции по внесению крупного первоначального депозита при установлении новых отношений с лицами, осуществляющими деятельность по выпуску цифровых активов, организации торгов ими, а также предоставлению услуг по обмену цифровых активов на деньги, ценности и иное имущество (ПУВА), сумма которого не соответствует профилю клиента и/или вывод активов без дополнительных операций, либо в кратчайшие сроки после их появления на счете»;
- «Открытие нескольких счетов под разными именами с целью обхода ограничений, установленные лицами, осуществляющие деятельность по выпуску цифровых активов, организации торгов ими, а также предоставлению услуг по обмену цифровых активов на деньги, ценности и иное имущество (ПУВА) на торговлю и снятие средств, в том числе с ненадежных IP-адресов в странах или территориях, находящихся под санкциями или подозрительных IP-адресов»;
- «Средства клиента получены с биржи цифровых активов либо направляются в работу на биржу цифровых активов, которая, по данным СФМ, не зарегистрирована и/или не имеет соответствующей лицензии»;
- «Клиент использует биржу цифровых активов или зарубежный сервис перевода денег или ценностей (MVTs), который по информации СФМ

находится в государстве (на территории), не выполняющей рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ)»;

- «Транзакции, вовлекающие несколько цифровых активов, или, с несколькими счетами, либо в разных юрисдикциях по невыгодным, экономически нецелесообразным условиям, либо не свойственные профилю клиента»;

- «Операции с цифровыми активами, существенную долю в которых составляют транзакции, связанные с сервисами онлайн-гэмблинга либо операции, связанные с миксерами (включая встроенные в кошельки) либо связанные с адресами цифровых активов, на которых, как было установлено ранее, находились украденные средства, или с адресами, привязанными к держателям украденных средств»;

- «Совершение операций с адресами цифровых активов, имеющими связь с незаконной деятельностью (финансированием терроризма, торговлей людьми, незаконно торговлей оружием и боеприпасами)».

Российская Федерация

Определены основания направления частным сектором СПО, связанным с покупкой/продажей виртуальных активов – согласно Положению Банка России от 02.03.2012 № 375-П, среди признаков, указывающих на необычный характер операции, имеется код 1190 («Операция, связанная с оборотом цифровой валюты»).

В дополнение к этому, при проведении компетентными органами проверочных мероприятий отмечаются следующие признаки, свидетельствующие о возможном использовании цифровых активов в преступных расчетах, легализации полученных доходов и финансировании терроризма:

- зачисление на банковский счет денежных средств (электронных денежных средств) из разных источников.
- фальсификация оснований возникновения прав на денежные средства (электронные денежные средства) или иное имущество, приобретенное преступным путем (в результате совершения преступления), в том числе гражданско-правовых договоров, первичных учетных документов и т.п.
- использование P2P-переводов.
- осуществление операций с низким порогом сумм (до 15000 рублей) фиатных денежных средств.

- использование различных платежных систем мгновенного перевода денежных средств (в том числе иностранных), не позволяющих идентифицировать плательщика.
- использование банковских карт, оформленных на третьих лиц (дропов).
- сложности в выявлении признаков подозрительных фиатных операций, связанных с оборотом цифровых валют, поскольку затруднительно установить связь между такими операциями и соответствующими виртуальными активами.

Туркменистан

Отсутствие законодательных норм, регулирующих порядок регистрации и (или) лицензирования криптовалютных бирж и обменников, а также выпуск и оборот виртуальных активов. Государственный классификатор видов экономической деятельности не предусматривает как вид деятельности деятельность, связанную с операциями с виртуальными активами.

Республика Узбекистан

В феврале 2021 года Межведомственной комиссией был утвержден отчет по итогам секторальной оценки рисков легализации доходов, полученных от преступной деятельности и финансирования терроризма в сфере оборота крипто-активов в Республике Узбекистан. Критерии риска приведены в данном отчете, однако сам отчет является документом конфиденциального характера.

Согласно Постановлению Президента Республики Узбекистан «О мерах по развитию цифровой экономики и сферы оборота крипто-активов в Республике Узбекистан» (03.07.2018г., №ПП-3832) с 1 января 2023 года граждане и юридические лица, зарегистрированные на территории Республики Узбекистан, могут осуществлять операции по покупке, продаже и (или) обмену крипто-активов исключительно через национальных провайдеров услуг в порядке, установленном актами законодательства. Операции граждан и юридических лиц Республики Узбекистан проверяются лицензированными национальными провайдерами услуг на предмет соответствия требованиям законодательства о ПОД/ФТ. Операции нерезидентов Республики Узбекистан осуществляются через коммерческие банки, где все операции нерезидентов относятся к высокому риску и по отношению к ним применяются усиленные меры по надлежащей проверке клиентов.

Признаки подозрительности операций с крипто-активами согласно Правилам внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения для лиц, осуществляющих деятельность в области оборота крипто-активов (рег. МЮ № 3309 от 9 июня 2021 года):

- предоставленные документы на проведение операции вызывают сомнение в их подлинности (достоверности), и (или) сведения об операции, в том числе о какой-либо из ее сторон, не соответствуют имеющейся информации;
- операция не имеет явного экономического смысла и не соответствует характеру и виду деятельности клиента;
- немотивированный отказ в предоставлении клиентом сведений, запрашиваемых в связи с необходимостью идентификации, в том числе о доверителе (если клиент выступает в качестве поверенного);
- немедленное прекращение деловых отношений по инициативе клиента при применении по отношению к нему требований, предусмотренных настоящими Правилами;
- невозможность завершения идентификации или получения по результатам надлежащей проверки данных, указывающих на нецелесообразность установления с клиентом деловых отношений;
- пренебрежение клиентом более выгодными условиями оказания услуг, а также предложение клиентом необычно высокого вознаграждения, заведомо отличающегося от обычно оплачиваемого при оказании такого рода услуг;
- крипто-активы или денежные средства переводятся за пределы Республики Узбекистан в пользу лиц, постоянно проживающих или зарегистрированных в оффшорных зонах;
- один из участников операции является лицом, постоянно проживающим, находящимся или зарегистрированным в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения;
- выявление неоднократного совершения операций или сделок, которые дают основания полагать, что целью их осуществления является уклонение от процедур контроля, установленных законодательством;

- регулярный перевод крипто-активов в одинаковой сумме на один тот же крипто-кошелек или несколько крипто-кошельков, в том числе открытых на крипто-биржах;
- многократный обмен крипто-активов друг на друга с последующим выводом на крипто-кошельки, открытые на других крипто-биржах или крипто-платформах по обмену, хранению и покупке/продаже крипто-активов либо на частные крипто-кошельки;
- совершение большого числа крупных сделок с крипто-активами в течение 24 часов, а также с использованием вновь открытых крипто-кошельков или ранее не использовавшихся в течение длительного периода времени;
- внезапный перевод крипто-активов лицам, осуществляющим деятельность в области оборота крипто-активов, в странах, в которых клиент явно не может вести деловые отношения;
- вложение на крипто-кошельки крипто-активов и их перевод в частные или анонимные крипто-кошельки в течение короткого промежутка времени;
- получение крипто-активов с крипто-кошельков, которые ранее были использованы в преступных целях, а также с крипто-кошельков лиц, ранее владевших такими крипто-кошельками;
- внесение на крипто-кошельки крупных размеров крипто-активов, явно несоответствующих обычному обороту клиента;
- обмен крипто-активов на иностранную или национальную валюту с большей комиссией либо по невыгодному курсу;
- быстрый рост стоимости недавно эмитированного крипто-актива и его обращение исключительно в рамках одной крипто-биржи или крипто-платформы по обмену, хранению и покупке/продаже крипто-активов;
- наличие признаков манипулирования ценами на крипто-активы;
- получение широко известных и обращающихся длительное время крипто-активов в обмен на вновь эмитированные крипто-активы с последующим мгновенным их выводом на различные крипто-кошельки либо обмен на иностранную или национальную валюту;
- отсутствие у вновь эмитированного крипто-актива декларации «White paper» (документ, содержащий сведения о деятельности эмитирующей организации для которой привлекаются инвестиции посредством размещения крипто-активов и токенов) либо несоответствия действительности, содержащейся в ней информации, включая

безосновательное указание на гарантирование крипто-актива со стороны правительств отдельных стран или известных международных компаний, а также направление полученных денежных средств на реализацию подозрительных инвестиционных проектов;

- постоянное использование клиентом сервисов для сокрытия IP-адреса и других приложений, предоставляющих анонимность;
- отличия фактического домена клиента или его контрагента по операции от домена страны, в которой он зарегистрирован;
- открытие клиентом большого числа крипто-кошельков с одного IP-адреса;
- частая смена идентификационных данных, включая адреса электронной почты, IP-адреса и домена, сведений о держателях крипто-кошельков;
- клиент не обладает знаниями в сфере оборота крипто-активов;
- источником происхождения крипто-активов являются сервисы, оказывающие услуги по организации и проведению игр, основанных на риске (азартных игр), в режиме онлайн;
- наличие любых подозрений, что денежные средства или иное имущество, использованные при осуществлении операции, имеют преступное происхождение или предназначены для финансирования терроризма либо финансирования распространения оружия массового уничтожения».

В части анализа поступающих сведений о фиатных операциях, связанных с покупкой/продажей виртуальных активов соответствующие подразделения ПФР, на которые в соответствии с НПА возложены задачи по проведению анализа СПО, имеют полный доступ к базе данных сообщений о подозрительных финансовых операциях.

Приказом начальника ПФР (рег. 3419 МЮ. от 07.02.2023 г.) утвержден шаблон направления организациями, осуществляющим операции с денежными средствами или иным имуществом СПО в ПФР. Пунктом 29 шаблона предоставления СПО установлена информация об операциях, связанных с крипто-активами.

Рекомендуемые меры:

- *Учитывать риски, связанные с возможным использованием виртуальных активов (ВА) в преступных целях, выявляемые юрисдикциями. Особое внимание обращать на использование миксеров, высоко анонимных типов виртуальных активов.*

- *Выявлять и применять меры к незаконно действующим на территории страны и использующим оборудование страны ПУВА. Поставить на постоянный мониторинг происхождение средств, получаемых ПУВА, действующими на территории страны. Наладить взаимодействие или противодействие с иностранными ПУВА, работающими на территории страны.*

Риски использования виртуальных активов в преступных целях

Участники проекта (Республика Беларусь, Республика Казахстан, Российская Федерация) отметили выявляемые схемы легализации доходов, полученных преступным путем, и финансирования терроризма.

Так, среди наиболее актуальных способов легализации преступных доходов были отмечены расслоение средств с использованием множества криптокошельков, зарегистрированных на подставных лиц, а также «транзитных» переводов по значительному количеству криптокошельков, использование мелких криптобирж, не соблюдающих требования ПОД/ФТ, и финансовых сервисов-«матрешек» для обхода требований по идентификации.

В целях «транзитного» перемещения средств также могут задействоваться и крупные криптобиржи (операции на которых осуществляются между внутренними счетами клиентов и не попадают в открытый блокчейн). При этом для перевода преступного дохода из фиатной валюты в криптоактивы (и в обратную сторону) используются P2P-переводы между банковскими картами, оформленными, с одной стороны, на заказчиков средств, а с другой – на подставных физических лиц, счета которых являются инфраструктурой незаконных обменных пунктов.

В качестве одного из вариантов усложнения криптовалютных цепочек могут применяться возможности (услуги) децентрализованных финансовых протоколов (DeFi), децентрализованных криптобирж (работающих на смарт-контрактах) и обменников (DEX), не требующих проведения проверки клиентов.

Наиболее вероятным способом интеграции преступных доходов, полученных или переведенных в криптовалютную форму, является приобретение недвижимости, транспортных средств и иного имущества (в частности, в государствах, где подобные транзакции разрешены).

В свою очередь, наиболее вероятным способом использования криптокошельков для сбора средств на цели финансирования терроризма является размещение платежных реквизитов в социальных сетях, интернет-сайтах и рассылка посредством мессенджеров.

Инструменты противодействия преступной деятельности, связанной с использованием виртуальных активов

В Республике Казахстан, Кыргызской Республике и Монголии оценивается риск использования тех или иных виртуальных активов для совершения преступных деяний.

Так, в Казахстане Комитет МФЦА запрещает деятельность, связанную с использованием высоко анонимных активов, таких как Monero (XMR), Zcash (ZEC) и другими.

В Республике Сербия действует Закон «О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма», который запрещает использование миксеров виртуальных активов. Согласно ему, эмитент виртуальных активов и поставщик услуг виртуальных активов не могут использовать IT-ресурсы, которые позволяют и/или способствуют сокрытию личности клиента и/или предотвращают и/или затрудняют мониторинг транзакций с виртуальными (цифровыми) активами.

В рамках процедур лицензирования и надзора надзорные органы (Национальный банк Сербии и Комиссия по ценным бумагам) контролируют все услуги, которые поставщики услуг виртуальных активов планируют предоставлять или предоставляют, в частности, чтобы определить, соответствует ли предоставление этих услуг упомянутому закону, например, не предоставляют ли они услуги миксера виртуальных активов.

Несмотря на то, что были проанализированы многие несанкционированные поставщики услуг виртуальных активов, власти не выявили миксеров виртуальных активов, действующих на территории Республики Сербия.

Цифровые инструменты и специализированное программное обеспечение для выявления преступной деятельности, связанной с использованием виртуальных активов

Республика Беларусь

В Республике Беларусь для отслеживания совершенных между криптовалютными адресами транзакций используются преимущественно инструменты, находящиеся в открытом доступе в сети Интернет:

<https://explorer.bitquery.io/>,
<https://bitinfocharts.com/>,
<https://clankapp.com/>,
<https://explorer.crystalblockchain.com/>,
<https://ethplorer.io/>,
<https://tronscan.org/>,
<https://explorer.btc.com/>.

Предоставлен доступ к сервису «Прозрачный блокчейн» нескольким сотрудникам ПФР Беларуси для загрузки в табличном виде криптовалютных транзакций интересующего адреса, отображения их в графическом виде, разметки отдельных адресов, принадлежащих институциональным участникам криптовалютного рынка.

Лицензируемые белорусские провайдеры услуг виртуальных активов обязаны использовать:

1. Программное обеспечение, выполняющее обобщение и анализ использования клиентами (потенциальными клиентами) их адресов (идентификаторов) виртуальных кошельков, в том числе позволяющее определить:
 - торговые площадки, на которых адреса (идентификаторы) виртуальных клиентов (потенциальных клиентов) использовались,
 - адреса (идентификаторы) виртуальных кошельков контрагентов клиентов (потенциальных клиентов),
 - связи адресов (идентификаторов) виртуальных кошельков клиентов (потенциальных клиентов) с другими адресами (идентификаторами) виртуальных кошельков и др.),
 - уровень риска применения адресов (идентификаторов) виртуальных кошельков клиентов (потенциальных клиентов) для осуществления противоправной деятельности (участия в ней);
2. Услуги иных лиц (исполнителей) по обобщению, анализу и оценке:
 - Elliptic Enterprises Limited (Великобритания),
 - Elliptic Vault Limited (Великобритания),
 - Chainalysis, Inc (США),

- Coinfirm Limited (Великобритания),
- Neutrino srl (Италия),
- Crystal Blockchain B.V. (Нидерланды).

Республика Казахстан

В Республике Казахстан применяются программные продукты: Crystal, пилотная версия системы Chainanalysis.

Комитет МФЦА использует следующие технологии для определения источника и назначения цифровых активов:

- процедура KYC (Know Your Customer – Знай своего клиента) обязывает лицензируемых Участников Центра идентифицировать каждого учредителя и ключевых сотрудников, проверка производится посредством сервисов: Thomson Reuters World check, Adata и Sumsb.
- процедура KYT (Know Your Transaction – Знай свою транзакцию) предоставляет возможность отследить блокчейн транзакции на платформе ПУВА, проверка производится посредством сервиса Coinfirm, Sumsb.

В части технологического обеспечения деятельности провайдеров услуг виртуальных активов, выставляются требования к:

- а. Правилам Внутреннего Контроля (ПВК) СФМ МФЦА;
- б. «НПК» по дистанционному установлению деловых отношений.

Кроме того, ПУВА должны разработать и внедрить политику по информационной безопасности, включающую процедуры:

- обеспечения информационной безопасности;
- управления данными;
- управления доступом;
- обеспечения системной и сетевой безопасности;
- обеспечения непрерывности деятельности;
- управления поставщиками ИТ-услуг.

Процедуры и политики по ИТ-безопасности должны быть одобрены Комитетом МФЦА. При лицензировании Участников Центра, требуется заключение ИТ аудитора.

Российская Федерация

В Российской Федерации реализуются мероприятия в части идентификации участников транзакций при проверке возможной причастности к противоправной деятельности с применением виртуальных валют в рамках информационного взаимодействия с подразделениями финансовой разведки иных юрисдикций.

Для выявления, анализа и визуализации операций с криптовалютами используется разработанный Росфинмониторингом аналитический программный сервис «Прозрачный блокчейн» и иные аналитические инструменты с открытым исходным кодом. Установлению подлежат данные лиц, возможно причастных к совершению преступлений и легализации преступных доходов, реквизиты банковских карт, электронных кошельков и обменных сервисов для приобретения криптовалюты.

Цифровой сервис «Прозрачный блокчейн» – инструмент мониторинга транзакций в криптовалюте. С помощью встроенных в функционал сервиса алгоритмов осуществляется разметка, кластеризация и деанонимизация участников рынка криптовалют. В сервис «Прозрачный блокчейн» внедрен алгоритм оценки индикаторов риска транзакций в криптовалюте.

Республика Узбекистан

В соответствии с постановлением Национального агентства проектного управления при Президенте Республики Узбекистан, Департамента по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан «Об утверждении Правил внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения для лиц, осуществляющих деятельность в области оборота крипто-активов» (зарегистрировано МЮ от 09.06.2021 г., рег. номер 3309) определено, что лица, осуществляющие деятельность в области оборота крипто-активов должны обеспечить разработку и утверждение внутренних правил. В них, в том числе, должен быть отражен порядок осуществления мер по выявлению, оценке, мониторингу, снижению и документированию уровня рисков, включая использование программного обеспечения, осуществляющего анализ по операциям с криптовалютными активами.

Указанное программное обеспечение должно позволять определять торговые площадки, на которых адреса крипто-кошельков клиентов

использовались, адреса крипто-кошельков контрагентов клиентов, связи адресов крипто-кошельков клиентов с другими адресами крипто-кошельков и др. и оценивать риск использования адресов крипто-кошельков клиентов в противоправной деятельности.

Используются различные программные продукты для осуществления мониторинга и контроля за транзакциями с крипто-активами.

Монголия

Используются цифровые инструменты для выявления и отслеживания подозрительных криптовалютных потоков, такие как Chainalysis и TRM Labs.

Республика Сербия

Комиссия по ценным бумагам Сербии не использует специализированные программные инструменты для цифровых активов, но в сотрудничестве с Советом Европы был запущен проект, целью которого является создание программного обеспечения, которое будет использоваться для мониторинга крипто-транзакций.

Министерство внутренних дел Сербии использует Chainalysis Reactor, который позволяет идентифицировать мошенничество, Ransomware, кластер Dark Net.

Рекомендуемые меры:

- *применять и (или) развивать специальные сервисы мониторинга для выявления высокорисковых транзакций и участников;*
- *проводить оценку риска деятельности провайдеров услуг виртуальных активов с помощью сервисов мониторинга криптовалютных транзакций;*
- *выработать меры по предотвращению работы незарегистрированных ПУВА с использованием оборудования на территории и с гражданами стран.*

Применение наиболее анонимизированных виртуальных активов

На территории всех государств-членов и наблюдателей ЕАГ, принявших участие в проекте, запрещены транзакции в наиболее анонимизированных виртуальных валютах (Monero, ZCash и другие).

В Монголии ПУВА должны ежемесячно предоставлять отчет о торговле и отчет о потребителях. В отчете ПУВА предоставляют подробный отчет о каждом виртуальном активе, которым торгуют/обмениваются.

Согласно отчетам и данным, полученным от ПУВА, анонимизированные виртуальные активы (такие как Monero, Zcash) не используются на внутреннем рынке виртуальных активов.

В Республике Сербия Закон о противодействии отмыванию денег и финансированию терроризма прямо указывает, что выпуск или предоставление услуг, связанных с виртуальными (цифровыми) активами, которые прямо или косвенно позволяют скрыть личность клиента («монеты конфиденциальности»), и осуществление сделок с использованием таких виртуальных (цифровых) активов запрещены.

В рамках процедур лицензирования и надзора надзорные органы (Национальный банк Сербии и Комиссия по ценным бумагам) контролируют все услуги, которые поставщики услуг виртуальных активов планируют предоставлять или предоставляют, в частности, чтобы определить, соответствует ли предоставление этих услуг упомянутому закону, например, не предоставляют ли они услуги, связанные с виртуальными активами, которые прямо или косвенно позволяют скрыть личность клиента. Соискатель лицензии обязан предоставить надзорным органам список видов виртуальных активов, в отношении которых он намерен предоставлять услуги по виртуальным активам. После получения лицензии поставщик услуг виртуальных активов обязан уведомить надзорный орган о любых изменениях в указанном списке.

Комитет МФЦА в Республике Казахстан исключает допуск к торгам анонимизированных виртуальных активов. ПУВА обязаны согласовывать цифровые активы, планируемые к обороту на платформе.

В соответствии с законодательством Республики Узбекистан осуществление майнинга анонимных крипто-активов, в том числе осуществление операций с анонимными криптоактивами со стороны провайдеров услуг в сфере оборота крипто-активов, запрещено.

Рекомендуемые меры:

- *Запретить оборот монет повышенной анонимности на зарегистрированных ПУВА.*
- *Противодействовать деятельности миксеров и ПУВА, не осуществляющих надлежащие усилия в области ПОД/ФТ.*

Минимизация рисков и угроз, связанных с виртуальными активами

Республика Беларусь

ПФР Республики Беларусь участвует в разработке нормативно-правовых актов в сфере виртуальных активов на национальном уровне.

При наличии оснований полагать, что финансовые операции связаны с получением и (или) легализацией преступных доходов, финансированием терроризма и финансированием распространения оружия массового поражения, материалы направляются ПФР в правоохранительный орган.

Создан и наполняется реестр адресов (идентификаторов) виртуальных кошельков, которые имеют связь с финансированием противоправной деятельности. ПФР является получателем сведений из него и осуществляет мониторинг транзакций, связанных с соответствующими криптовалютными адресами.

Республика Казахстан

В Республике Казахстан Комитет МФЦА, МЦРИАП (Министерство цифрового развития, инноваций и аэрокосмической промышленности) и ПФР на регулярной основе проводят рабочие встречи по обмену опытом и обсуждению текущих тенденций рисков в сфере ОД/ФТ.

В части типологий по пресечению схем ОД с использованием виртуальных активов, Комитет МФЦА, в том числе, руководствуется регулярными публикациями и обновлениями ПФР, ЕАГ и ФАТФ. Комитет МФЦА, в рамках текущей деятельности, выявляет активность ПУВА с признаками подозрительной деятельности. В случае подтверждения информации и выявления устойчивых методов нелегальной деятельности, Комитет МФЦА, во взаимодействии с ПФР, вырабатывают типологию ОД с использованием криптовалюты и других виртуальных активов. Кроме того, постоянно ведётся взаимодействие с уполномоченными органами по оптимизации механизмов передачи материалов по подозрению и совершению уголовно-наказуемых правонарушений Участниками МФЦА в структурное подразделение ПФР для принятия соответствующих мер реагирования.

Согласно п. 4.3.1 Правил МФЦА о ПОД/ФТ, политики, процедуры и системы контролей ПУВА МФЦА обязаны включать в себя соответствующие

программы подготовки и повышения осведомлённости сотрудников о ПОД/ФТ. Так, предусмотрена обязанность ПУВА МФЦА принять надлежащие меры по доведению до своих сотрудников законов о ПОД/ФТ, проводить регулярные тренинги по идентификации подозрительных операций, обеспечить понимание сотрудниками политик, процедур и контролей относящихся к ПОД/ФТ, а также обеспечить понимание сотрудниками типов подозрительных операций в рамках контекста бизнеса компании и необходимость уведомления ответственных лиц за ПОД/ФТ в компании; обеспечить осведомлённость о трендах ОД/ФТ, понимание рисков «уведомления» клиента, рассматриваемого в рамках СОП, и как их избежать, а также иные важные аспекты ПОД/ФТ. Исполнение ПУВА МФЦА вышеуказанных требований контролируется Комитетом МФЦА в рамках системы отчётности, плановых и внеплановых проверок и тематических проверок деятельности ПУВА МФЦА.

Проводятся следующие мероприятия:

- Проверка наличия принятых руководством ПУВА правил и политики в области ПОД/ФТ.
- Требование к ПУВА на этапе получения лицензии о назначении ответственного сотрудника по ПОД/ФТ.
- Обязательное подтверждение у сотрудника отсутствия судимости и наличия соответствующего опыта работы или знаний в области ПОД/ФТ, проведение интервью с кандидатом.
- Требование к ПУВА о внедрении процедур идентификации отправителей и получателей цифровых активов.
- Установлено требование идентификации всех участников торгов.
- Мониторинг наличия миксеров и связей с сомнительными аккаунтами.
- Требование по внедрению инструментов и процедуры биометрической идентификации клиента при установлении отношений удалённо.
- Требование к ПУВА проверки цифровых активов перед допуском к торгам.
- Получение одобрения Комитета МФЦА для допуска цифровых активов к торгам.

Российская Федерация

Для выявления и пресечения противоправных операций физических лиц в Российской Федерации, а также принятия дополнительных мер по повышению безопасности и защите P2P-сервисов от их использования

недобросовестными субъектами Банком России выпущены Методические рекомендации №16-МР от 06.09.2021 о повышении внимания кредитных организаций к отдельным операциям клиентов-физических лиц.

В целях снижения рисков использования инфраструктуры кредитных организаций, Банк России рекомендует кредитным организациям оценивать операции по банковским счетам дропов или операций с использованием предоставленных им электронных средств платежа для установления клиентов-физических лиц, осуществляющих переводы денежных средств, связанные с покупкой (продажей) цифровых валют, в пользу дропов, а также клиентов-физических лиц, в пользу которых от дропов осуществляются переводы денежных средств, связанные с покупкой (продажей) цифровых валют. Для указанных целей выпущены Методические рекомендации Банка России от 29 февраля 2024 г. № 4-МР «По усилению контроля за отдельными операциями клиентов-физических лиц».

Указанием Банка России от 20 октября 2020 года №5599-У «О внесении изменений в Положение Банка России от 2 марта 2012 года № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» определены следующие признаки, указывающие на необычный характер операции (сделки):

- операции, связанные с обращением цифровых прав, которые характеризуются однонаправленностью, регулярностью, на крупные суммы;
- операция, связанная с оборотом цифровой валюты.

При выявлении указанных операций субъекты первичного финансового мониторинга (частный сектор) направляют соответствующие сообщения в подразделение финансовой разведки для анализа и принятия дальнейших мер реагирования (проведение финансовых расследований, организация межведомственного взаимодействия, подготовка законодательных инициатив и т.п.).

Кроме того, в соответствии с Положением Банка России №375-П от 2 марта 2012 года введен в действие дополнительный код подозрительности операций, связанных с оборотом цифровой валюты (доп. код 1190). Сведения по коду 1190 направляются с 1 октября 2021 года, включая операции, предшествующие этой дате.

Кыргызская Республика

ПФР Кыргызской Республики проведена оценка рисков финансирования террористической деятельности и легализации (отмывания) преступных доходов в секторе виртуальных активов и поставщиков услуг виртуальных активов, по итогам которого будут выработаны меры по минимизации рисков и угроз. Отчет об оценке рисков утвержден протоколом заседания Комиссии по вопросам противодействия финансированию террористической деятельности и легализации (отмыванию) преступных доходов от 28 июля 2023 года № 6 Кабинета Министров Кыргызской Республики.

Туркменистан

В Туркменистане в целях минимизации рисков СФМ совместно с различными международными и учебными организациями (ООН, ОБСЕ, ЕАГ, МУМЦФМ и др.) проводятся обучающие мероприятия на тему виртуальных активов и ПУВА для представителей правоохранительных органов и частного секторов.

Республика Узбекистан

Департаментом по борьбе с экономическими преступлениями и Национальным агентством перспективных проектов Республики Узбекистан производятся меры по выявлению рисков в секторе оборота виртуальных активов, результаты которого будут отражены в секторальной оценке рисков.

Монголия

ПФР Монголии сотрудничает с Комиссией по финансовому регулированию в проведении тренингов, семинаров и разработке руководств для поставщиков услуг виртуальных активов с целью повышения осведомленности и углубления понимания требований и обязательств по ПОД/ФТ. Кроме того, ПФР Монголии разработало «Руководство по заполнению СПО» и опубликовало его на своем веб-сайте.

Республика Сербия

Администрация по предотвращению отмывания денег (ARML - подразделение финансовой разведки Сербии) принимает участие в национальных оценках рисков, в том числе в области ВА и ПУВА, чтобы знать сектор и понимать риски, связанные с этой областью. На основании результатов НОР 2021 года и

понимания рисков в План действий Национальной стратегии ПОД/ФТ на 2020-2024 годы был включен ряд мероприятий по снижению выявленных рисков.

Эти мероприятия включают, среди прочего, внедрение механизмов обмена информацией между компетентными органами в области ВА, которое осуществляется совместно с Департаментом по борьбе с киберпреступностью Министерства внутренних дел. Некоторые другие мероприятия включают улучшение оперативного сотрудничества между компетентными органами в отношении уголовных или других разбирательств, связанных с цифровыми активами, путем проведения регулярных встреч, что является текущей деятельностью. ПФР также участвует в деятельности, в рамках которой будет подготовлен Сравнительный анализ международного опыта и оценка вариантов улучшения отчетности в отношении операций, связанных с цифровыми активами, с использованием карточных платежных систем и иностранных учреждений электронных денег.

ПФР Сербии принимает участие в вышеуказанных мероприятиях либо как ведущее агентство, либо как партнер по реализации.

В рамках своих обязанностей по Закону о ПОД/ФТ ПФР проводит лицензионные экзамены для комплаенс-офицеров и их заместителей, что является еще одним превентивным инструментом, помогающим повысить осведомленность и знание сотрудниками ПФР своих обязанностей в области ПОД/ФТ.

Для улучшения своей оперативной работы ПФР сотрудничает с зарубежными организациями-партнерами с целью получения соответствующих ИТ-инструментов для облегчения мониторинга операций, связанных с ВА. Одна из таких работ ведется в рамках проекта по ПОД/ФТ в Сербии стоимостью 2,3 млн. евро, финансируемого Швецией и реализуемого Советом Европы, целью которого является анализ и приобретение наиболее подходящего ИТ-решения для мониторинга операций с ВА. Сотрудники ПФР также следят за успехами других национальных органов в этой области и регулярно обмениваются знаниями.

ПФР Сербии также принимает участие в процедурах проверки соответствия требованиям, проводимых по мере необходимости и по требованию регулятора/надзорного органа в области ВА/ПУВА, в основном Национального банка Сербии.

Пресечение деятельности высокорисковых ПУВА

В Республике Беларусь, Кыргызской Республике, Российской Федерации, Республике Узбекистан и Туркменистане проводятся мероприятия по предупреждению и пресечению деятельности тех ПУВА, в частности, обменников виртуальных активов, которые предоставляют клиентам возможность осуществления транзакций с криминальными адресами.

Республика Беларусь:

Так, в Республике Беларусь осуществляется привлечение к уголовной ответственности по ст. 243 УК Республики Беларусь либо к административной ответственности по ст. 13.2 ч.3 КоАП Республики Беларусь в зависимости от суммы полученного дохода, периода деятельности и средств совершения преступления.

Следственный комитет Республики Беларусь отмечает, что установлена административная ответственность за незаконную предпринимательскую деятельность в отношении лиц, причастных к нелегальному обмену виртуальных активов, а также за уклонение от уплаты налогов, если лица действовали как субъект хозяйствования и при этом не были зарегистрированы в качестве резидента Парка высоких технологий.

Примеры:

1. Органами финансовых расследований совместно со Следственным комитетом Республики Беларусь проведена операция по пресечению деятельности нелегального криптообменника, являющегося частью международной сети криптообменников, имеющих представительство в девяти странах. Так, в марте 2023 г. возбуждено уголовное дело по признакам преступления, предусмотренного ч.33 ст. 243 (уклонение от уплаты налогов, сборов) УК Республики Беларусь, в отношении представителя сети нелегальных обменников в Республике Беларусь Т., гражданина Российской Федерации З., организатора и управляющего данной сетью гражданина Республики Армения Д. и иных лиц, которые с 2019 года по 2023 год с использованием подконтрольных им ресурсов в сети Интернет осуществляли на территории Республики Беларусь без государственной регистрации предпринимательскую деятельность, связанную с приобретением и продажей цифровых знаков (токенов), в результате чего получили доход на общую

сумму не менее 9,9 млн. рублей. С полученного дохода путем уклонения от представления налоговой декларации и сокрытия налоговой базы не исчислено и не уплачено подоходного налога в особо крупном размере – в сумме не менее 1.5 млн. рублей. Особенностью сети указанных криптообменников являлось проведение сделок за наличные средства в специально оборудованных офисах. Дневной оборот наличных денежных средств только белорусского офиса достигал сотен тысяч долларов США, а количество клиентов – десятков тысяч.

2. К., при пособничестве Т., Г. и С. осуществлял без государственной регистрации сделки по приобретению и отчуждению токенов, обмену токенов одного вида на другие, получив доход в виде 16 710 945,76 единиц токенов, что эквивалентно 2 222 876 долларов США, от уплаты подоходного налога уклонился. Приговором суда Т., Г. и С. осуждены за пособничество в уклонении от уплаты налогов, повлекшем причинение ущерба в особо крупном размере. К. находится в розыске.

Кыргызская Республика

По результатам оценки рисков сектора виртуальных активов и ПУВА в Кыргызской Республике были приняты меры по разработке руководящих документов для сектора. Подготовлен План действий по снижению рисков, одним из положений которого является разработка признаков/критериев подозрительных операций, организация обучающих мероприятий как для самих подотчетных лиц, так и для правоохранительных и надзорных органов, и др.

Российская Федерация

В Российской Федерации проводится мониторинг состояния финансового рынка Российской Федерации и осуществления Банком России надзорной деятельности. Результаты свидетельствуют о том, что расчеты по сделкам с виртуальными активами осуществляются преимущественно с помощью P2P-операций по счетам подставных физических лиц – «дропов», что является недопустимой практикой.

Общие объемы высокорисковых P2P-операций, как и количество вовлеченных в них граждан, оцениваются Банком России как высокие и требуют принятия комплексных мер.

Противодействие P2P-операциям на сегодняшний день является приоритетным направлением финансового мониторинга. В 2021 году Банк

России выпустил методические рекомендации, которые ориентируют кредитные организации при реализации процедур внутреннего контроля в рамках ПОД/ФТ обратить повышенное внимание на отдельные операции физических лиц, совершаемые в целях осуществления незаконной предпринимательской деятельности и иных противоправных целях, в частности, связанных с обеспечением расчетов «теневого» игорного бизнеса (незаконных «онлайн-казино» и «онлайн-лотерей»), нелегальных участников финансового рынка, а также в целях совершения операций в криптообменниках.

В 2024 году Банк России ориентировал кредитные организации на выявление и снижение рисков использования их услуг в противоправных целях участниками теневого бизнеса по сделкам с криптовалютами. В частности, кредитным организациям рекомендовано выявлять операции, направленные на покупку или продажу криптовалют с использованием счетов, оформленных на подставных физических лиц – «дропов».

У граждан, которые осуществляют такие операции, кредитные организации могут запрашивать дополнительную информацию и документы, а также учитывать полученные сведения при оценке их уровня риска.

В настоящее время Банк России в плотном взаимодействии с банками разрабатывает и внедряет подходы по противодействию высокорисковым P2P-операциям. Данные подходы включают меры по повышению оперативности выявления таких операций, счетов физических лиц – «дропов» и реагирования на выявляемые риски.

Туркменистан

В Туркменистане работа проводится в соответствии с Уголовным и Уголовно-процессуальным Кодексами.

Республика Узбекистан

В соответствии с Постановлением Президента Республики Узбекистан от 03.07.2018 года № ПП-3832 «О мерах по развитию цифровой экономики и сферы оборота крипто-активов в Республике Узбекистан» начиная с 1 января 2023 года граждане и юридические могут осуществлять операции по покупке, продаже и (или) обмену крипто-активами исключительно через провайдеров услуг в установленном порядке.

Кроме того, за незаконную деятельность, связанную с оборотом крипто-активов, установлена уголовная и административная ответственность.

На постоянной основе в Республике Узбекистан производится блокировка крипто-платформ, осуществляющих незаконную деятельность.

Пресечение использования виртуальных активов для целей НОН и коррупционных преступлений

Российская Федерация и Республика Казахстан относят преступления коррупционной направленности и в сфере НОН, совершенные с применением виртуальных активов, к тем типам преступных деяний, по которым наиболее сложно выявить факты отмывания преступных доходов. Дополнительно выделяются:

- уклонение от уплаты налогов (Республика Беларусь);
- мошенничество (Российская Федерация);
- преступления в бюджетной сфере (Российская Федерация и Республика Казахстан).

Республика Беларусь

В 2023 году органами финансовых расследований выявлен первый факт получение взятки должностным лицом в USDT.

Пример:

Т., руководитель лаборатории по проведению испытаний виртуальных игорных заведений ООО «А», с апреля по сентябрь 2021 г. получил взятку в особо крупном размере от руководителя организатора азартных игр ООО «Бел» за благоприятное решение в интересах этой организации испытания ее виртуальных игорных заведений в виде 61494 единиц криптовалюты USDT (Tether). Уголовное дело рассматривается судом.

М. и Д. вошли в состав организованной группы, которая осуществляла незаконный оборот наркотических средств через Интернет-магазин. Оплата наркотиков осуществлялась в биткоинах через специально созданный Телеграм-канал. Впоследствии криптовалюта выводилась на анонимные кошельки.

М. и Д. выполняли роль «закладчиков», то есть фасовали крупные партии наркотиков на более мелкие и размещали их в тайники для конечных потребителей. Оплата их преступной деятельности осуществлялась

биткоидами.

Приговором суда М. и Д. осуждены к 12 и 11 годам лишения свободы, соответственно. Расследование уголовного дела в целях выявления иных участников организованной преступной группы продолжается.

Республика Казахстан

В подразделении финансовой разведки предусмотрены профильные подразделения по коррупционным преступлениям и преступлениями в сфере НОН и по мониторингу каналов виртуальных активов, которые проводят соответствующую работу.

Пример:

В 2022 году ДКНБ по г. Алматы расследовалось уголовное дело по ст. 218 УК (легализация) в отношении гражданки О., организовавшей нарколабораторию на территории г. Алматы, которая отмывала преступные доходы путем приобретения имущества.

В результате анализа официальных доходов и фактических расходов фигуранта дела, наличия движимого/недвижимого имущества установлен факт легализации преступного дохода, выразившегося в приобретении земельного участка с частным домом стоимостью около 100 млн. тенге, а также дополнительно обнаружены добытые преступным путем денежные средства в сумме 76 млн. 783 тысяч 375 тенге и 4 автомашины марок «Subaru Legacy», «Volkswagen Transporter», «Jeep Wrangler», «Nissan Qashqai». Кроме того, органом расследования из незаконного оборота изъяты 6,651 bitcoin-средств путем их обналичивания через фиатные деньги в сумме 67 млн. 582 тысяч 60 тенге.

09.12.2022 приговором суда г. Алматы О. осуждена к 16 годам лишения свободы с конфискацией вышеуказанных имуществ и денежных средств.

Кыргызская Республика

Работа по пресечению коррупционных преступлений осуществляется на основе УПК и Закона Кыргызской Республики от 8 августа 2012 года № 153 «О противодействии коррупции». Пресечение коррупционных преступлений с использованием виртуальных активов проводится на общих основаниях.

Пресечение незаконного оборота наркотических средств, с использованием виртуальных активов проводится на общих основаниях, в соответствии с УПК Кыргызской Республики.

Российская Федерация

Сотрудниками МВД России организована работа по выявлению и установлению платежных инструментов, используемых в сфере незаконного оборота наркотиков для обналичивания и легализации (отмывания) доходов. Основной массив указанной информации поступает в ходе мониторинга ресурсов, располагающихся в закрытом сегменте сети Интернет, так называемом «Darknet». Полученные данные используются в работе по делам об отмывании наркодоходов и предикатным к ним составам при планировании оперативно-розыскных мероприятий и следственных действий (включая постановку вопросов для экспертного исследования и далее экспертизы), в том числе в целях определения источников получения первичной информации и оригиналов банковских и иных документов, имеющих доказательственное значение. Кроме того, в части данной тематики просим ориентироваться на итоги проекта «Отмывание преступных доходов, полученных от незаконного оборота наркотиков и их прекурсоров».

Пресечение коррупционных преступлений является приоритетной задачей правоохранительных органов. Факты взяточничества, в которых в качестве взаиморасчетов используются виртуальные активы, документируются обычным образом (в соответствии с п. 10 статьи 8 Федерального закона от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции» цифровая валюта признана имуществом).

В Российской Федерации предусмотрены⁷ следующие наказания:

1. Наложение административного штрафа на должностное лицо, лицо, выполняющее управленческие функции в коммерческой или иной организации.
2. Иностранное должностное лицо либо должностное лицо публичной международной организации – наложение административного штрафа на юридических лиц в размере до трехкратной суммы денежных средств, стоимости ценных бумаг, иного имущества, услуг

⁷ Согласно итоговому отчету по типологическому проекту ЕАГ «Отмывание преступных доходов, полученных от коррупционных преступлений и преступлений против интересов государственной службы», утвержденному 39-м Пленарным заседанием ЕАГ

[https://eurasiangroup.org/files/uploads/files/Public_typology_reports/WGTyp_\(2023\)_7_rev_1_rus.pdf](https://eurasiangroup.org/files/uploads/files/Public_typology_reports/WGTyp_(2023)_7_rev_1_rus.pdf)

имущественного характера, иных имущественных прав, незаконно переданных или оказанных либо обещанных или предложенных от имени юридического лица.

3. В случае совершения преступления в крупном размере (свыше одного миллиона рублей): наложение административного штрафа на юридических лиц до тридцатикратного размера суммы денежных средств, стоимости ценных бумаг, иного имущества, услуг имущественного характера, иных имущественных прав, незаконно переданных или оказанных либо обещанных или предложенных от имени юридического лица, но не менее двадцати миллионов рублей с конфискацией денег, ценных бумаг, иного имущества или стоимости услуг имущественного характера, иных имущественных прав.
4. В случае совершения преступления в особо крупном размере (свыше двадцати миллионов рублей): наложение административного штрафа на юридических лиц в размере до стократной суммы денежных средств, стоимости ценных бумаг, иного имущества, услуг имущественного характера, иных имущественных прав, незаконно переданных или оказанных либо обещанных или предложенных от имени юридического лица, но не менее ста миллионов рублей с конфискацией денег, ценных бумаг, иного имущества или стоимости услуг имущественного характера, иных имущественных прав. Кроме того, может быть произведена конфискация без вынесения обвинительного приговора, если такое требование соответствует принципам внутреннего законодательства (когда преступник не может быть привлечен к ответственности по причине смерти, бегства, отсутствия или если его личность не установлена). Кроме того, в случае если публичное должностное лицо не раскрывает источник происхождения своего имущества для предъявления обвинения, то такое имущество может быть конфисковано судом в рамках гражданского иска.

Республика Узбекистан

Крипто-магазинами и иными провайдерами услуг виртуальных активов для минимизации рисков использования их инфраструктуры в преступных целях внедрены повышенные лимиты единоразовой продажи виртуальных активов для клиентов.

Международное взаимодействие для нейтрализации угроз и уязвимостей в части виртуальных активов

Республика Беларусь

ПФР Республики Беларусь регулярно осуществляет международный информационный обмен в части получения сведений о владельцах электронных кошельков, которые были задействованы в схемах совершения преступных деяний.

При расследовании преступлений, связанных с противоправным использованием виртуальных активов, осуществляется направление поручений и просьб о взаимной правовой помощи, поручений посредством канала НКП24 МВД Республики Беларусь, НЦБ Интерпола в Республике Беларусь, запросов в криптобиржи.

Взаимодействие между компетентными органами осуществляется правоохранительными органами в общем порядке в рамках Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступностью (25 ноября 1998 г., г. Москва), Соглашения об обмене информацией в сфере борьбы с преступностью (22 мая 2009 г., г. Астана), а также в рамках двусторонних межправительственных соглашений.

Отдельных нормативных правовых актов, регламентирующих международное взаимодействие в ходе проведения финансовых расследований преступлений, связанных с оборотом виртуальных активов, нет.

Республика Казахстан

Комитет МФЦА Республики Казахстан рассматривает сотрудничество с другими регулируемыми и контрольно-надзорными органами в качестве важного компонента своей надзорной деятельности. Эффективные соглашения о сотрудничестве обеспечивают оперативный обмен информацией по вопросам надзора, расследований и правоприменения.

Подход к надзору основывается на:

- использовании последовательной системы оценки рисков для оценки риск-профиля участников МФЦА;
- эффективном использовании ресурсов на основании проведённой оценки риск-профиля участника;

- предотвращении несоразмерного регуляторного бремени и упрощении технологического прогресса;
- использовании подходящих метрик для мониторинга и надзорных инструментов для осуществления эффективного надзора;
- установлении тесных взаимоотношений с участниками. Комитет МФЦА является членом The Global Financial Innovation Network (GFIN).

Также, Комитет МФЦА является членом ключевых международных нормотворческих организаций, а именно:

- Международной организации комиссий по ценным бумагам (IOSCO).
- Международной ассоциации органов страхового надзора (IAIS).
- Группы органов банковского надзора из Центральной и Восточной Европы (BSCEE), Региональной группы Базельского комитета по банковскому надзору.
- Совета по исламским финансовым услугам (IFSB)
- Организации по бухгалтерскому учету и аудиту для исламских финансовых учреждений (AAOIFI).

Двусторонние меморандумы о взаимопонимании подписаны со следующими регуляторами:

- Правлением Abu Dhabi Global Market (ADGM) относительно финансовых технологий.
- Банком Литвы (финансовые технологии).
- Валютным управлением Сингапура (финансовые технологии).
- Управление по регулированию и надзору в сфере финансовых услуг Дубая относительно финансовых услуг.
- Правлением Финансового центра Катар – относительно финансовых услуг;
- Национальным банком Грузии.
- Банком Литвы (финансовые технологии).
- Агентством банковского надзора Турции (BRSAT).
- Комиссией по финансовым услугам Республики Корея и Службой финансового надзора Республики Корея.

- Меморандум о взаимопонимании с Национальным Банком Кыргызской Республики.
- Меморандум о взаимопонимании с Министерством финансов Республики Таджикистан.
- Меморандум о взаимопонимании между Агентством Республики Казахстан по финансовому мониторингу и BN KZ Technologies Limited (Binance).

Комитет национальной безопасности Республики Казахстан отмечает, что для расследования преступлений, совершенных с использованием виртуальных активов в преступных целях, международное взаимодействие осуществляется путем направления правоохранными и специальными органами запросов в компетентные органы иностранных партнеров посредством систем международного обмена информацией. Общий порядок взаимодействия в рамках расследования преступлений определен двусторонними и многосторонними договорами и соглашениями по оказанию правовой помощи по уголовным делам, а также Разделом 12 Уголовно-процессуального Кодекса.

Международное взаимодействие обеспечивает Подразделение международных отношений Агентства Республики Казахстан по финансовому мониторингу на основании ответов профильных подразделений. При направлении международных запросов указываются: номера кошельков, используемый тип виртуальных активов, наблюдаемые обороты, суммы, аффилированные лица, факты правонарушения, описание предполагаемой схемы совершения правонарушения.

Кыргызская Республика

В Кыргызской Республике осуществляется международное взаимодействие для нейтрализации угроз и уязвимостей в части виртуальных активов. Неоднократно проводились семинары и рабочие встречи с международными экспертами по актуальным вопросам для сотрудников ПФР, Национального Банка, Службы регулирования и надзора за финансовым рынком, правоохранных органов Кыргызской Республики.

Согласно Руководства по вопросам проведения финансового расследования, утвержденного Приказом Генеральной прокуратуры, Государственного комитета национальной безопасности, МВД и ГСФР от 26 декабря 2022 года №86/13/863/156 «О вопросах проведения финансового расследования», международное сотрудничество осуществляется на

основании международных договоров, а также на основании принципа взаимности в соответствии с законодательством Кыргызской Республики.

При запрашивании информации от ПФР иностранных государств через каналы связи Группы Эгмонт необходимо предоставлять в ГСФР конкретные реквизиты, идентифицирующие проверяемых юридических и физических лиц, сведения о финансовых операциях, данные, указывающие на связь операций с запрашиваемым государством, а также иные сведения согласно установленной формы Группы Эгмонт.

Отмечаются сложности в обмене и предоставлении информации по линии противодействия ОД или предикатным преступлениям, совершенным с использованием виртуальных активов при взаимодействии с ПФР иностранных государств, а именно ПФР офшорных зон.

Российская Федерация

Виртуальные активы признаются имуществом для целей законодательства о ПОД/ФТ, а также для антикоррупционного законодательства и исполнительного производства. Указанное означает, что в отношении виртуальных активов предусмотрен весь существующий спектр мер по ПОД/ФТ/ФРОМУ, в том числе в рамках расследований преступлений. Так, например, Глава IV Федерального закона № 115-ФЗ регулирует международное взаимодействие в сфере борьбы с ОД/ФТ/ФРОМУ. Кроме того, в рамках сотрудничества ПФР-ПФР осуществляется взаимодействие в целях ПОД/ФТ, в том числе в части противодействия преступности с использованием ИТ-технологий.

Сотрудничество с компетентными органами иностранных государств и международными организациями по вопросам ПОД/ФТ/ФРОМУ обеспечивает Управление международных связей Росфинмониторинга, непосредственно осуществляет информационный обмен в соответствии с международными договорами Российской Федерации, меморандумами о сотрудничестве и взаимопонимании, на основе принципа взаимности или иных формах взаимодействия с уполномоченными органами иностранных государств в сфере ПОД/ФТ/ФРОМУ, в том числе по вопросам, связанным с использованием криптовалют в преступных целях.

Обмен информацией регламентируется международными договорами Российской Федерации, меморандумами о сотрудничестве и взаимопонимании. Обмен осуществляется в письменной форме, в том числе с

использованием технических средств передачи текста, по инициативе или на основании запросов ПФР. Запрос как правило содержит:

- а) наименование запрашивающего ПФР;
- б) наименование запрашиваемого ПФР;
- в) краткое изложение существа запроса и его обоснование (если запрос является срочным, запрашивающий ПФР обязан обосновать необходимость срочного запроса);
- г) описание содержания запрашиваемой информации;
- д) цель использования запрашиваемой информации;
- е) другие сведения, необходимые для его исполнения.

В случае необходимости запрашиваемый ПФР может запросить у запрашивающего ПФР дополнительную информацию, необходимую для надлежащего исполнения запроса.

При осуществлении международного взаимодействия возникают определенные сложности, такие как:

1. Некоторые ПФР готовы предоставлять информацию по запросу только при наличии возбужденного уголовного дела в отношении фигуранта.
2. Недостаточный опыт правоохранительного блока по данному направлению.
3. ПФР может предоставить информацию о клиентах криптобирж, их криптокошельках и т.д. только в случае, когда действие местного законодательства о ПОД/ФТ распространяется на лиц, оказывающих услуги криптовалютных бирж. Вместе с тем в период с 2022 г. по настоящее время ряд ПФР не предоставлял по запросам необходимой информации в отношении криптокошельков, открытых на лицензированных биржах в данных юрисдикциях. В связи с непоступлением необходимой для проведения финансовых расследований информации проведение проверочных мероприятий по указанным материалам было прекращено или приостановлено.

Республика Узбекистан

Республика Узбекистан в рамках Совета руководителей ПФР СНГ (СРПФР) участвует в реализации проекта по созданию реестра криптовалютных кошельков. Данный проект направлен на повышении качества и результативности международных финансовых расследований противоправного использования

виртуальных активов, путем формирования единой базы данных о криптовалютных кошельках и их адресах.

Департамент имеет доступ к аналитической платформе «Chainanalysis», посредством которой осуществляет деятельность финансовой разведки в сфере оборота крипто-активов. Кроме того, Департамент напрямую взаимодействует с международными крипто-биржами.

Республика Сербия

Комиссия по ценным бумагам Республики Сербии как член IOSCO заключила меморандум о сотрудничестве со всеми членами IOSCO, в отношении тем, связанных с цифровыми активами, в юрисдикциях, где она регулируется.

Национальный банк Сербии заключил в феврале 2023 года Соглашение о сотрудничестве с Комиссией по надзору за финансовым сектором (Commission de Surveillance du Secteur Financier, CSSF), которая отвечает за регистрацию, надзор и правоприменение в целях ПОД/ФТ поставщиков услуг виртуальных активов в Великом Герцогстве Люксембург. Поскольку Соглашение о сотрудничестве было подписано совсем недавно, оценка влияния этого меморандума пока не может быть дана.

Монголия

Для эффективной борьбы с преступной деятельностью ПФР Монголии сотрудничает и осуществляет обмен информацией с другими юрисдикциями по каналам Egmont Group, Интерпола и ARIN-AP. Кроме того, Национальное полицейское агентство направляет запросы о вызове в суд в адрес зарубежных криптовалютных платформ.

Достигнута договоренность с криптовалютной биржей Binance о быстром замораживании любых счетов, связанных с отмыванием денег или деятельностью по финансированию терроризма, по запросу правоохранительных органов.

Рекомендуемые меры:

- *развивать международное сотрудничество в части взаимного обогащения сведениями по направлению развития индустрии виртуальных активов и обмена сведениями о физических и юридических лицах, участвующих в транзакциях в виртуальных валютах.*
- *создавать и на регламентной основе наполнять специальные реестры подозрительных криптовалютных кошельков, которые использовались в преступной деятельности.*

- обеспечить скорость взаимодействия по получению данных от ПУВА зарегистрированных в странах
- обеспечить взаимодействие по блокированию использования незарегистрированными ПУВА:
 - национальных доменов
 - IP адресного фонда провайдеров
 - национальных провайдеров
 - финансовых каналов финансовой системы стран
 - участия в незарегистрированных ПУВА граждан стран и физических офисов работы

Межведомственное взаимодействие для нейтрализации угроз и уязвимостей в части виртуальных активов на национальном уровне

Республика Беларусь

В соответствии с Указом Президента Республики Беларусь от 14.02.2022 № 48 «О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты» (далее – Указ), в Республике Беларусь создан реестр адресов виртуальных кошельков, использовавшихся (использующихся) для осуществления противоправной деятельности, в котором содержатся сведения об адресах (идентификаторах) виртуальных кошельков, использованных (используемых) для осуществления террористической, экстремистской деятельности и иных деяний, ответственность за совершение которых предусмотрена законодательством об административных правонарушениях или уголовным законом.

Указанный реестр формируется заинтересованными государственными органами, которым стало известно об использовании адресов виртуальных кошельков в противоправной деятельности. В случае, если клиент криптовалютной биржи или обменного пункта, зарегистрированных на территории Республики Беларусь, попытается осуществить операцию с адресом из реестра, в совершении операции ему будет отказано.

Межведомственное взаимодействие осуществляется на основании Закона № 165-З и двусторонних соглашений.

Правоохранительные органы направляют в ПФР следующую информацию в части использования виртуальных валют и электронных денег в противоправной деятельности:

1. Сведения, указывающие на признаки легализации доходов,

полученных преступным путем;

2. Сведения о предикатном преступлении.

Правоохранительные органы направляют информацию о виртуальных кошельках, использовавшихся (использующихся) для осуществления противоправной деятельности, в ГУ «Администрация Парка высоких технологий» в порядке, предусмотренном Указом Президента Республики Беларусь от 14.02.2022 № 48 «О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты». В последующем сведения об указанных виртуальных кошельках в виде реестра направляются заинтересованным государственным органам, в том числе Комитету государственного контроля, одним из органов которого является Департамент финансового мониторинга.

Алгоритм взаимодействия правоохранительных органов с ПФР Республики Беларусь:

1. Взаимодействие органов финансовых расследований Комитета государственного контроля и Департамента финансового мониторинга осуществляется в порядке, установленном Инструкции о порядке взаимодействия Департамента финансового мониторинга и органов финансовых расследований Комитета государственного контроля по вопросам противодействия легализации доходов, полученных преступным путем, и финансированию террористической деятельности.
2. Направление официальных запросов в иные правоохранительные органы.
3. Неформальные каналы не используются.
4. Правоохранительные органы получают информацию:
 - Сведения об основных контрагентах хозяйствующих субъектов, сводные данные о платежах, информация, поступившая в отношении фигурантов в соответствии со специальными формулярами;
 - Информация о подозрительных операциях фигурантов, которые могут быть связаны с легализацией преступных доходов;
 - Материалы и сведения в отношении фигурантов, полученные ПФР в результате международного взаимодействия.

В роли руководителя межведомственной группы выступает представитель ведомства, в чьем производстве находится уголовное дело. Руководитель следственной группы принимает уголовное дело к своему

производству, организует ее работу, руководит действиями других следователей, принимает решения о соединении и выделении дел; прекращении производства по уголовному делу в целом или его части; приостановлении или возобновлении производства по уголовному делу; возбуждении ходатайств о продлении срока следствия; применении в качестве мер пресечения заключения под стражу, домашнего ареста и их продлении; привлечении в качестве обвиняемого.

Деятельность межведомственных групп регулируется Уголовно-процессуальным кодексом Республики Беларусь. Предварительное следствие в Республике Беларусь производится следователями Следственного комитета, Комитета государственной безопасности, прокурорами.

В случае сложности и трудоемкости уголовного дела расследование может быть поручено следственной группе. Сотрудники органов, уполномоченных законом осуществлять дознание, оперативно-розыскную деятельность (органы внутренних дел, органы финансовых расследований и др.) могут производить следственные и другие процессуальные действия, оперативно-розыскные мероприятия по поручению следователей. Сотрудники иных государственных органов, не являющихся правоохранительными, могут привлекаться к участию в производстве по делу в качестве экспертов, специалистов. Координация внутри межведомственных групп осуществляется руководителем следственной группы из числа представителей ведомств: Следственный комитет, Комитет государственной безопасности, Министерство внутренних дел, Департамент финансовых расследований Комитета государственного контроля, органы прокуратуры.

Изъятие, арест и конфискация преступных доходов в криптовалюте осуществляется в порядке, установленном для изъятия, ареста и конфискации имущества и преступных доходов в соответствии с Уголовно-процессуальным кодексом Республики Беларусь, а также с учетом требований Указа Президента Республики Беларусь от 14.02.2022 № 48 «О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты».

При изъятии, аресте и конфискации преступных доходов в криптовалюте сложность представляет поиск всех используемых в противоправной деятельности криптовалютных кошельков; необходимость в специальных познаниях для совершения операции по переводу криптовалюты с кошельков фигурантов уголовного дела в адрес кошельков, принадлежащих органам уголовного преследования.

Согласно сведениям Следственного комитета Республики Беларусь имеются следующие трудности:

- в доступе к виртуальным кошелькам при отсутствии реквизитов доступа;
- в получение ключа доступа к цифровому кошельку при непредставлении подозреваемыми (обвиняемыми) соответствующих сведений в добровольном порядке;
- невозможность реализации криптовалюты на белорусских криптобиржах в ходе исполнения приговоров и иных судебных решений, которыми криптовалюта конфискована либо обращена на возмещение ущерба, если криптовалюта имеет связь с сомнительными ресурсами.
- недостаточное законодательное регулирование порядка оборота криптовалюты.

Следственный комитет Республики Беларусь особо отмечает отсутствие служебных виртуальных кошельков с необходимыми веб-адресами определенных типов криптовалют и (или) их ограниченным количеством для целей проведения финансовых расследований по соответствующей линии.

Республика Казахстан

Комитетом МФЦА Республики Казахстан заключён Меморандум о сотрудничестве и обмене информацией по вопросам надзора и регулирования с Агентством Республики Казахстан по регулированию и развитию финансового рынка (АРРФР) и Национальным Банком Республики Казахстан (НБ).

В 2021 г. между Комитетом МФЦА и Агентством Республики Казахстан по финансовому мониторингу заключён меморандум о взаимопонимании и сотрудничестве в сфере ПОД/ФТ, и обмене информацией. Меморандум направлен на обеспечение сотрудничества между Комитетом МФЦА и Агентством в сфере ПОД/ФТ, обмена информацией, в том числе конфиденциальной, с целью эффективного выполнения Комитетом МФЦА регуляторных целей в данной сфере. Меморандум позволил сторонам обеспечить и повысить эффективность контроля и мониторинга Участников МФЦА, а также содействует обеспечению стабильности финансовой системы и защиты прав потребителей финансовых услуг. Комитет МФЦА является постоянным членом таких рабочих групп, организованных Агентством, как:

- Межведомственная Рабочая группа по вопросам ПОД/ФТ;
- Межведомственный Совет по вопросам ПОД/ФТ;
- Межведомственная Комиссия по вопросам ПОД/ФТ;
- Рабочая группа по подготовке к Взаимной Оценке ЕАГ Казахстана и Национальной Оценке рисков.

Координация деятельности межведомственных рабочих групп осуществляется руководителем межведомственной группы, который определяется совместным постановлением начальников следственного отдела или органов дознания.

В проведении межведомственных расследований преступлений, связанных с противоправным использованием виртуальных активов, могут принимать участие: Агентство Республики Казахстан по финансовому мониторингу, Генеральная Прокуратура, Комитет национальной безопасности и Министерство внутренних дел Республики Казахстан.

Изучение финансовых аспектов преступной деятельности в рамках уголовных дел о предикатных преступлениях и отмыывании доходов осуществляется расследующими их подразделениями органов внутренних дел, антикоррупционной службы, службы экономических расследований и органов национальной безопасности, а также в отдельных случаях прокурорами.

В рамках расследования может быть поручено проведение налоговых и иных проверок, а также аудита.

Ст. 18 Закона РК «О противодействии легализации (отмыыванию) доходов, полученных преступным путем, и финансированию терроризма» (от 28 августа 2009 года № 191-IV) – «Взаимодействие уполномоченного органа с государственными органами Республики Казахстан» - регулирует данный вопрос, в том числе предусматривает запрашивание информации при наличии санкции прокуратуры, наличия уголовного дела, в том числе связанных с использованием виртуальных активов.

Комитет национальной безопасности Республики Казахстан:
Взаимодействие с Агентством Республики Казахстан по финансовому мониторингу осуществляется путем следующих рекомендаций:

- Правила проведения оценки рисков легализации (отмыывания) доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения;
- Критерии отбора лиц, возможно причастных и имеющих потенциальные риски к финансированию терроризма;

- Методические рекомендации по выявлению финансирования терроризма на стадии сбора и изъятия средств;
- Критерии отбора физических лиц для включения в Перечень СБ ООН.

Согласно ст. 16 Закона «О противодействии легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма» (далее – Закон), при приостановлении проведения подозрительной операции в соответствии с частью 1 пункта 3 и пунктом 5 статьи 13 Закона, а также при наличии оснований полагать, что деятельность физических, юридических лиц и иностранных структур без образования юридического лица связана с легализацией (отмыванием) доходов, полученных преступным путем, и (или) финансированием терроризма (далее – ОД/ФТ), с совершением иного уголовного правонарушения, связанного с ОД/ФТ, уполномоченный орган – АФМ направляет информацию в правоохранительные и специальные государственные органы в соответствии с их компетенцией с уведомлением Генеральной прокуратуры и далее осуществляет взаимодействие с правоохранительными и специальными государственными органами по переданной информации.

Порядок данного взаимодействия определен совместным приказом, имеет пометку о содержании информации ограниченного распространения.

На основании ст.17 Закона ПОД/ФТ и вышеуказанного совместного приказа запросы, направляемые правоохранительными и специальными органами в подразделение финансовой разведки АФМ, подписываются должностным лицом, осуществляющим досудебное расследование, утверждаются первым руководителем государственного органа и санкционируются руководителем органа прокуратуры.

Соответствующие правоохранительные и специальные государственные органы после принятия решения по направленной информации в течение двух рабочих дней направляют в АФМ и Генеральную прокуратуру информацию о принятых мерах.

Также в соответствии со ст.18 Закона правоохранительные и специальные государственные органы по уголовным делам и материалам, зарегистрированным в установленном законодательством порядке, связанным с противодействием ОД/ФТ, с санкции органов прокуратуры направляют в АФМ запросы о предоставлении сведения и информации об операции, подлежащей финансовому мониторингу.

Исполнение этих запросов осуществляется АФМ в пределах, имеющих в республиканской базе данных в сфере противодействия ОД/ФТ

сведений и информации об операциях, подлежащих финансовому мониторингу, а также в пределах полученных сведений и информации от компетентных органов иностранных государств в сфере противодействия ОД/ФТ.

В соответствии со статьей 194 УПК досудебное расследование по делу в случае его сложности или большого объема может быть поручено группе следователей и сотрудников органа дознания (следственной, следственно-оперативной группе), о чем выносится постановление.

Решение об этом вправе принять начальник следственного отдела или органа дознания. В постановлении должны быть указаны все следователи, сотрудники органа дознания, которым поручено производство расследования, в их числе следователь – руководитель группы.

В группу могут входить следователи, сотрудники органа дознания нескольких органов, осуществляющих досудебное расследование. Решение о создании такой группы может быть принято, как по указанию прокурора, так и по инициативе начальников следственного отдела или органа дознания. Такое решение оформляется совместным постановлением, выносимым с соблюдением требований, указанных в части 1 статьи 194 УПК.

Генеральная Прокуратура Республики Казахстан:

Для обмена информацией в рамках межведомственного взаимодействия используется защищенный канал связи «СЕРТЕКС».

Агентство Республики Казахстан по финансовому мониторингу:

Межведомственное взаимодействие осуществляется по официальным каналам передачи данных с направлением запросов.

Ст. 18 Закона Республики Казахстан «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (от 28 августа 2009 года № 191-IV) – «Взаимодействие уполномоченного органа с государственными органами Республики Казахстан» - регулирует данный вопрос, в том числе предусматривает запрашивание информации при наличии санкции прокуратуры, наличия уголовного дела.

В соответствии со ст.194 УПК РК досудебное расследование по делу в случае его сложности или большого объема может быть поручено межведомственной следственно-оперативной группе, куда могут входить следователи, сотрудники органа дознания нескольких правоохранительных и специальных государственных органов (специальные прокуроры,

Министерство внутренних дел, Служба экономических расследований, Агентство по противодействию коррупции, КНБ).

Решение о создании такой группы может быть принято, как по указанию прокурора, так и по инициативе начальников следственного отдела или органа дознания. Такое решение оформляется совместным постановлением.

Для выявления лиц, предположительно совершивших правонарушение, связанное с противоправным использованием виртуальных активов, проводятся мероприятия:

- Проведение обысков, выемок и осмотров в целях изъятия и экспертного исследования компьютерных и иных технических устройств, которые могли быть использованы для активизации и управления виртуальными кошельками, а также для обнаружения записей пользователя с реквизитами, паролями (шифрами) доступа к соответствующим кошелькам.
- Проведение допросов свидетелей, подозреваемых лиц с целью получения полной информации об использованных в преступных целях виртуальных активов, их движениях, реквизитах, паролях доступа и иных идентификаторах криптокошельков.
- Направление запросов в ПФР на получение информации о подозрительных операциях физических и юридических лиц.
- Изучение банковских передвижений денег.
- Изучение истории посещения интернет-ресурсов.
- Инициирование комплекса негласных следственных действий, в т.ч. негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации.
- Направление поручения в оперативно-техническое подразделение для проверки информации в отношении лица, в чьих действиях усматриваются признаки противоправной деятельности, связанной с криптовалютой.
- Направление запросов в иностранные компетентные органы в рамках международных договоров об оказании правовой помощи по уголовным делам.
- При наличии доступа к криптокошельку в рамках осмотра соответствующего интернет-ресурса осуществляется изъятие виртуальных активов путем их обращения в фиатные деньги на

специально предусмотренный банковский счет для последующего наложения на них ареста.

- Идентификация в Децентрализованных биржах, отслеживание средств после проведения через «миксеры» и установление бирж кошелька – основные сложности при проведении соответствующих финансовых расследований.

Подразделение финансовой разведки является органом-гибридного типа – Агентство Республики Казахстан по финансовому мониторингу также включает в себя и правоохранный блок. Кроме того, Административный Процедурно-Процессуальный Кодекс Республики Казахстан от 29 июня 2020 года регулирует общий порядок обращений лиц в правоохранные, специальные и государственные органы Республики Казахстан, в том числе от зарегистрированных ПУВА, имеющих лицензию МФЦА (легальные предприятия имеют статус юридического лица).

Примеры положительного взаимодействия правоохранных органов и ПФР:

1. В ходе расследования следственным управлением Департамента КНБ по г. Алматы в 2019 году уголовного дела №197500041000135 по фактам организации незаконного игорного бизнеса преступной группой, легализации имущества, полученного преступным путем, уклонения от уплаты налогов, и другим преступлениям в сфере экономической деятельности, в результате взаимодействия с ПФР АФМ установлено и в последующем подвергнуто аресту большое количество незаконно добытых активов на территории РК и за рубежом - 11 квартир, 10 общественно-деловых учреждений, 5 складских помещений, 5 земельных участков с частными домами, а также 4 воздушных судов, 17 автомашин и 3 мототранспорта. На основании полученной информации ПФР в США направлено международное поручение в отношении множества установленных иностранных банковских счетов и юридических лиц, аффилированных с подозреваемыми лицами.
2. В ходе расследования следственным управлением Департамента КНБ по г. Астана в 2019 году уголовного дела №197100041000050 по факту хищения бюджетных средств в рамках гособоронзаказа, на основании полученной от ПФР информации установлена и в последующем подвергнута конфискации дорогостоящая элитная недвижимость на территории Республики Беларусь, которая виновным лицом была

приобретена на похищенные средства в сумме около 200 тыс. долларов США.

Российская Федерация

Взаимодействие осуществляется на основании Приказа Генпрокуратуры России № 511, Росфинмониторинга № 244, МВД России № 541, ФСБ России № 433, ФТС России № 1313, Следственного комитета Российской Федерации России № 80 от 21.08.2018 «Об утверждении Инструкции по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств или иного имущества, полученных преступным путем». Так, в разделе II указанного документа определен порядок взаимодействия Росфинмониторинга с правоохранительными органами, в том числе при направлении запросов о представлении информации.

Надзорные и правоохранительные органы во взаимодействии с финансовыми учреждениями участвуют в Совете комплаенс, являющемся рабочей группой при Межведомственной комиссии по противодействию легализации (отмыванию) доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения (МВК по ПОД/ФТ/ПРОМУ), в компетенцию которого входит обмен информацией о новых тенденциях и типологиях ОД/ФТ между государством и частным сектором (действует в соответствии с Положением о Совете комплаенс, утвержденном Председателем МВК по ПОД/ФТ/ПРОМУ 06.07.2016 г.).

Кроме того, на общих основаниях они имеют право, в соответствии со статьей 2 Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», направлять в государственные органы власти обращения для получения разъяснений по интересующим вопросам в соответствующей сфере деятельности.

Согласно пункту 5 Приказа Генпрокуратуры России № 511, Росфинмониторинга № 244, МВД России № 541, ФСБ России № 433, ФТС России № 1313, Следственного комитета Российской Федерации России № 80 от 21.08.2018, информационное взаимодействие между правоохранительными органами и Росфинмониторингом осуществляется на федеральном уровне, на уровне федеральных округов и субъектов Российской Федерации.

Кроме того, поскольку, согласно статье 3 Федерального закона № 115-ФЗ, цифровая валюта признается имуществом, различий в части взаимодействия правоохранительных органов и Росфинмониторинга в сфере

расследования преступлений, связанных с использованием виртуальных валют, не имеется, оно осуществляется на общих основаниях.

Согласно пункту 7 указанного приказа, информационное взаимодействие осуществляется в следующих формах:

- взаимное предоставление информации и документов, необходимых для установления связи операций с ОД/ФТ;
- исполнение запросов Росфинмониторинга;
- доступ правоохранительных органов к ЕИС Росфинмониторинга;
- информирование Росфинмониторингом правоохранительных органов о выявленных фактах нарушений законодательства Российской Федерации, а также о причинах и условиях, им способствующих;
- обмен статистическими, аналитическими и справочными материалами, методическими рекомендациями, представляющими взаимный интерес.

При этом механизм информационного взаимодействия в электронной форме определяется межведомственными соглашениями, заключаемыми Росфинмониторингом с заинтересованными правоохранительными органами. Кроме того, в качестве межведомственных механизмов действуют:

- Межведомственная рабочая группа по противодействию незаконным финансовым операциям (МРГ) в соответствии с Распоряжением Президента Российской Федерации от 28.07.2012 № 344-рп «О межведомственной рабочей группе по противодействию незаконным финансовым операциям»;
- МВК по ПОД/ФТ/ФРОМУ в соответствии с Приказом Росфинмониторинга от 21.09.2016 № 304 «О Межведомственной комиссии по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения»;
- Межведомственная комиссия по принятию Российской Федерации мер по итогам четвертого раунда взаимных оценок ФАТФ, согласно распоряжению Президента Российской Федерации от 12.06.2020 № 156-рп «О Межведомственной комиссии по принятию Российской Федерацией мер по результатам четвертого раунда взаимных оценок Группы разработки финансовых мер борьбы с отмыванием денег».

В соответствии с пунктом 6 Приказа Генпрокуратуры России № 511, Росфинмониторинга № 244, МВД России № 541, ФСБ России № 433, ФТС России № 1313, СК России №80 от 21.08.2018 установлено, что вопросы информационного взаимодействия относятся к компетенции руководителей Росфинмониторинга и правоохранительных органов, а также их заместителей и иных уполномоченных лиц, указанных в названном пункте для каждого органа исполнительной власти.

Также, согласно пункту 9 указанного приказа, запросы, направляемые в рамках информационного взаимодействия, подписываются руководителями ведомств, их заместителями, начальниками центральных и территориальных подразделений, управлений соответствующих государственных органов, а также прокуроров субъектов.

Сроки проведения расследований регламентируются уголовно-процессуальным законодательством России и применяются к расследованиям преступлений вне зависимости от сферы их совершения на общих основаниях, в том числе и в части виртуальных активов.

Общий срок предварительного следствия, согласно статье 162 Уголовно-процессуального кодекса Российской Федерации, составляет 2 месяца со дня возбуждения уголовного дела. Вместе с тем возможно продление срока предварительного следствия до 12 месяцев, дальнейшее продление сроков осуществляется в исключительных случаях в связи с сложностями категорий дел и в порядке, установленном Уголовно-процессуальным кодексом Российской Федерации.

В соответствии со ст. 163 УПК РФ расследование любых наиболее сложных преступлений, к числу которых относятся и расследования преступлений, связанных с виртуальными активами, поручается следственной группе, в состав которой включаются сотрудники, осуществляющие оперативно-розыскную деятельность. Таким образом могут быть созданы межведомственные или международные следственно-оперативные группы.

Деятельность межведомственных групп регулируется ст. 163 УПК РФ, которая предусматривает возможность производства предварительного расследования следственной группой. В соответствии с ч. 2 ст. 163 УПК РФ решения о производстве предварительного следствия следственной группой и об изменении ее состава принимает руководитель следственного органа.

В рамках межведомственного взаимодействия по вопросам, затрагивающим сферу противодействия незаконному использованию

виртуальных активов, сложностей не возникает. Тем не менее, отмечаются затруднения при идентификации фигурантов финансовых расследований.

При проведении финансовых расследований, в частности, при установлении конечных бенефициаров, отмечаются особенности:

1. Использование приватных/анонимных виртуальных активов.
2. В случае идентификации используемого фигурантом ПУВА запрос осуществляется исключительно через ПФР страны, где зарегистрирован ПУВА. Вместе с тем отмечаем отсутствие ответов некоторых ПФР на запросы.
3. При проведении финансовых расследований возникают сложности, связанные с выявлением юридических адресов криптовалютных бирж/обменников, что затрудняет процесс направления запроса.
4. Возможности анонимизации, использование миксеров.
5. Ряд криптовалютных бирж/обменников не предоставляет сведения в отношении клиентов, которые не являются гражданами запрашивающего государства. Нередкими становятся случаи, когда учетная запись криптовалютной биржи/обменника регистрируется на иностранного гражданина для создания препятствий в выявлении настоящих держателей виртуальных активов.
6. Получение от операторов соответствующих криптовалютных бирж установочных данных клиентов биржи, сведений о банковских картах и счетах, использующихся для купли-продажи криптовалюты за фиатные деньги и т.д. возможно лишь в случае, когда действие местного законодательства о ПОД/ФТ распространяется на лиц, оказывающих услуги криптовалютных бирж.
7. Не все иностранные криптовалютные биржи/обменники отвечают на запросы правоохранительных органов. Необходимость направления запросов по линии международно-правового сотрудничества, что негативно влияет на сроки получения запрашиваемой информации.
8. В ходе взаимодействия с сервисами по обмену криптовалют возникают проблемы, связанные с получением информации или отсутствием полных сведений о владельцах кошельков и совершаемых ими операциях, поскольку большинство криптобирж и обменников расположены за пределами территории Российской Федерации.

Вопросы процессуального характера, касающиеся механизмов по изъятию/аресту/конфискации, техническая сложность получения приватного

ключа кошелька, на котором хранятся виртуальные активы, а также отсутствие специальных знаний и практического опыта у сотрудников правоохранительных органов – основные сложности, возникающие при необходимости изъятия, ареста и конфискации преступных доходов, полученных от операций с виртуальными активами.

Кроме того, использование современных возможностей дистанционного управления денежными средствами позволяет преступникам маскировать связь с источником незаконного происхождения активов, включая виртуальные активы, с целью избежания уголовной ответственности. Это вызывает сложности в процессе доказывания преступного происхождения доходов фигурантов, умысла совершить отмыwanie незаконно полученных средств, а также затрудняет определение их точной суммы.

При судебном рассмотрении уголовных дел о преступлениях, инструментом которых выступали виртуальные активы, основные сложности возникают в части определения правового статуса виртуальных активов, а также осуществления защиты нарушенных прав с учетом обстоятельства обязательной задекларированности виртуальных активов в установленном порядке.

Кыргызская Республика

В Кыргызской Республике осуществляется международное взаимодействие для минимизации угроз и уязвимостей в части виртуальных активов. В рамках проводимой оценки рисков финансирования террористической деятельности и легализации (отмыwania) преступных доходов в секторе виртуальных активов и поставщиков услуг виртуальных активов в КР рабочая группа состоит из числа сотрудников правоохранительных органов, органов национальной безопасности, надзорных органов за ПУВА (Национальный банк Кыргызской Республики и Госфиннадзор).

Деятельность межведомственных групп регулируется в соответствии с УПК и Законом КР «Об оперативно-розыскной деятельности». Также в соответствии с УПК, Генеральная прокуратура рассматривает и решает вопрос о создании совместных следственных, следственно-оперативных групп по запросу органов, осуществляющих досудебное производство КР, и компетентных органов иностранных государств.

Межведомственное расследование преступлений с виртуальными активами осуществляется ведомствами: Государственный комитет

национальной безопасности, Министерство внутренних дел, Государственная служба финансовой разведки Кыргызской Республики.

Республика Узбекистан

У правоохранительных органов Республики Узбекистан имеются соответствующие полномочия запрашивать и получать информацию как в рамках уголовного дела, так и в период проведения оперативно-розыскных мероприятий.

Межведомственное расследование преступлений допускается в соответствии с нормами УПК с участием ведомств: правоохранительные, следственные органы и ПФР.

Межведомственные рабочие группы, деятельность которых направлена на повышение эффективности и качества взаимодействия, могут быть созданы как на основании нормативно-правовых актов, так и на основании решения отдельных государственных органов или по их согласованию.

При этом ограничений для включения каких-либо компетентных органов в составы данных групп не предусмотрено. Например, сотрудники Национального агентства перспективных проектов могут быть привлечены и привлекаются в качестве экспертов и специалистов.

Туркменистан

В Туркменистане одним из инструментов взаимодействия является созданная в 2022 году Координационная межведомственная комиссия по противодействию ОД/ФТ/ФРОМУ (Постановление Президента Туркменистана № 209 от 29.07.2022), которая обеспечивает взаимодействие и координацию по вопросам выработки и реализации политики и деятельности в области ПОД/ФТ и, в соответствующих случаях, в области противодействия финансированию распространения ОМУ. В состав межведомственной комиссии входят представители 16 министерств и ведомств на уровне руководителей и заместителей глав ведомств, под руководством Министра финансов и экономики. Полномочия комиссии прописаны в Положении о МВК, а сама комиссия является постоянно действующей.

Порядок оперативного взаимодействия правоохранительных органов и ПФР закреплён в Меморандумах о взаимном сотрудничестве и обмене информацией ПФР с Минюстом, Государственной таможенной службой, Министерством национальной безопасности, Министерством внутренних дел и Генеральной Прокуратурой Туркменистана.

В проведении межведомственных финансовых расследований могут участвовать: ГП, МНБ, МВД.

Республика Армения

В соответствии с Законом Республики Армения «О борьбе с отмыванием денег и финансированию терроризма» в целях эффективного осуществления борьбы с отмыванием денег и финансированием терроризма ПФР взаимодействует с органами оперативно-розыскной деятельности путем заключения двусторонних соглашений или без таковых.

Подразделение финансовой разведки взаимодействует с правоохранительными органами посредством специальной платформы обмена информацией.

На основании запроса органов, осуществляющих оперативно-розыскную деятельность, ПФР предоставляет имеющуюся в его распоряжении информацию, в том числе конфиденциальную, если запрос содержит достаточное обоснование в отношении подозрения в ОД/ФТ.

Монголия

Проведена оценка рисков ОД/ФТ по методологии Всемирного банка. 7 января 2022 года Советом по финансовой стабильности Монголии была создана рабочая группа по оценке риска ПУВА. В состав рабочей группы вошли 29 сотрудников из 12 государственных учреждений, включая Комиссию по финансовому регулированию, Банк Монголии, ПФР, Национальный совет по борьбе с терроризмом, Министерство юстиции и внутренних дел, правоохранительные органы и другие соответствующие организации.

Осуществляется межведомственное сотрудничество для устранения угроз и уязвимости виртуальных активов на национальном уровне. Комиссия по финансовому регулированию, Национальное полицейское агентство и ПФР Монголии работают вместе на национальном уровне для обеспечения безопасности и сохранности виртуальных активов. Проводится совместная оценка 66 местных поставщиков виртуальных валют.

Республика Сербия

Согласно Закону о цифровых активах Сербии, надзорный орган и другие компетентные органы в Республике сотрудничают и обмениваются данными с целью осуществления и совершенствования надзора, принятия решений в административных процедурах и выполнения других задач, установленных этим

законом. Комиссия по ценным бумагам и Национальный банк Сербии подписали специальное соглашение о сотрудничестве, поскольку Комиссия по ценным бумагам отвечает за часть, связанную с цифровыми токенами, а Национальный банк – за часть, связанную с виртуальными валютами.

Национальный банк Сербии и Комиссия по ценным бумагам (органы надзора и лицензирования в секторе виртуальных активов Республики Сербия) заключили в июне 2021 года Соглашение о сотрудничестве, специально посвященное вопросам виртуальных активов (способы сотрудничества и обмена данными с целью осуществления и улучшения надзора, лицензирования и выполнения других задач, определенных Законом о цифровых активах). Соглашение о сотрудничестве было полностью реализовано на практике, и надзорные органы регулярно обмениваются соответствующей информацией и документами и проводят встречи (не реже двух раз в год, но также и по мере необходимости).

Рекомендуемые меры:

- *Развивать координационные группы с участием подразделения финансовой разведки, правоохранительных органов, иных государственных ведомств, создавать межведомственные Комиссии и Соглашения о сотрудничестве на национальном уровне для минимизации рисков и угроз в части расширения применения виртуальных активов.*
- *Выработать стандарты в обмене сообщениями и запросами, связанными с финансовыми расследованиями в криптовалютах.*

Приложение 1. Примеры противоправного применения виртуальных активов

Информация по кейсам, представленным в разделе, была озвучена участниками Форума ЕАГ по ПОД/ФТ (2023 год)⁸.

Республика Беларусь

Опыт противодействия нелегальным сервисам обмена криптовалют

Пример 1. Криптообменник 1

Деятельность обменника охватывает ряд государств (рис. 1):

- Азербайджан;
- Армения;
- Узбекистан;
- Грузия;
- Украина;
- Беларусь;
- Россия;
- Казахстан;
- ОАЭ.



Рис. 1. Схема деятельности обменного пункта криптовалют

Результаты расследования:

- возбуждено уголовное дело за уклонение от уплаты налогов в особо крупном размере;

⁸ Презентации кейсов предоставлены Секретариатом ЕАГ для учета в рамках Типологического проекта «Минимизация рисков использования виртуальных активов в преступных целях».

- сумма неуплаченных налогов более 500 тысяч долларов США;
- изъято свыше 1 миллиона долларов (наличными);
- получена база данных клиентов;
- задержан представитель сети криптообменных сервисов в Беларуси;
- задержан организатор всей сети криптообменных сервисов;
- уголовное дело расследуется Следственным комитетом Республики Беларусь.

Пример 2. Криптообменник 2



Рис. 2. Схема деятельности обменного пункта криптовалют

Результаты расследования:

- возбуждено уголовное дело за уклонение от уплаты налогов в особо крупном размере;
- сумма неуплаченных налогов превышает 400 тысяч долларов США;
- изъято более 600 тысяч долларов США наличными и в криптовалюте;
- установлено свыше 100 использовавшихся в противоправной деятельности криптовалютных адресов;
- более 80% клиентов – покупатели запрещенных веществ в Даркнете;
- задержан организатор противоправной деятельности;
- уголовное дело расследуется Следственным комитетом Республики Беларусь.

Республика Казахстан

Пример 1. Нелегальный пункт обмена криптовалюты

Расследование деятельности нелегального пункта обмена криптовалют «Мистер Х», который:

- осуществляет деятельность без регистрации и лицензии;
- принимает переводы на карту только в Тенге.

Поступили сообщения от комплаенс-служб банков по поводу движения одинаковых сумм в пользу разных адресатов с разницей в несколько минут (рис. 3).

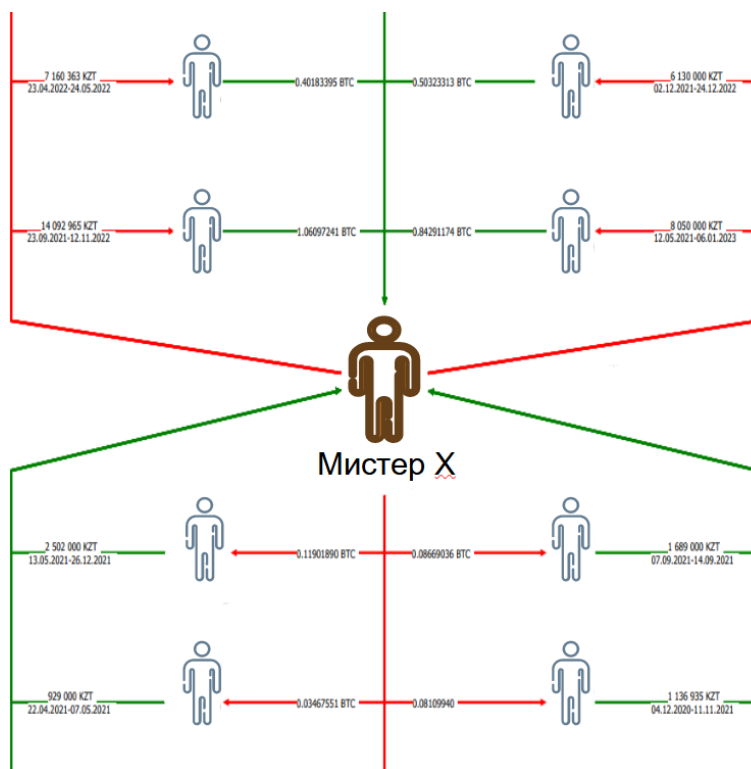


Рис. 3. Схема операций обменного пункта «Мистер Х»

Проведены необходимые мероприятия для проверки, уточнения и подтверждения сведений (Табл. 1).

Таблица 1. Результаты сопоставления транзакций обменного пункта «Мистер Х»

Выписки со счетов в банке второго уровня	Выписка из секции P2P криптобиржи «L»
01.07.2023 (15:30) Входящий перевод от Иванова И.И. на сумму 200 000 тенге	Исходящий перевод «Мистером Х» 0.02 BTC на 5 минут позже, чем операция по переводу с карты на карту

02.07.2023	(22:30)	Входящий перевод «Мистеру Х» в сумме
Исходящий перевод Николаеву Н.Н.	0.10 BTC в 22:34	
на сумму 1 200 000 тенге		

Пример 2. Нелегальный майнинг

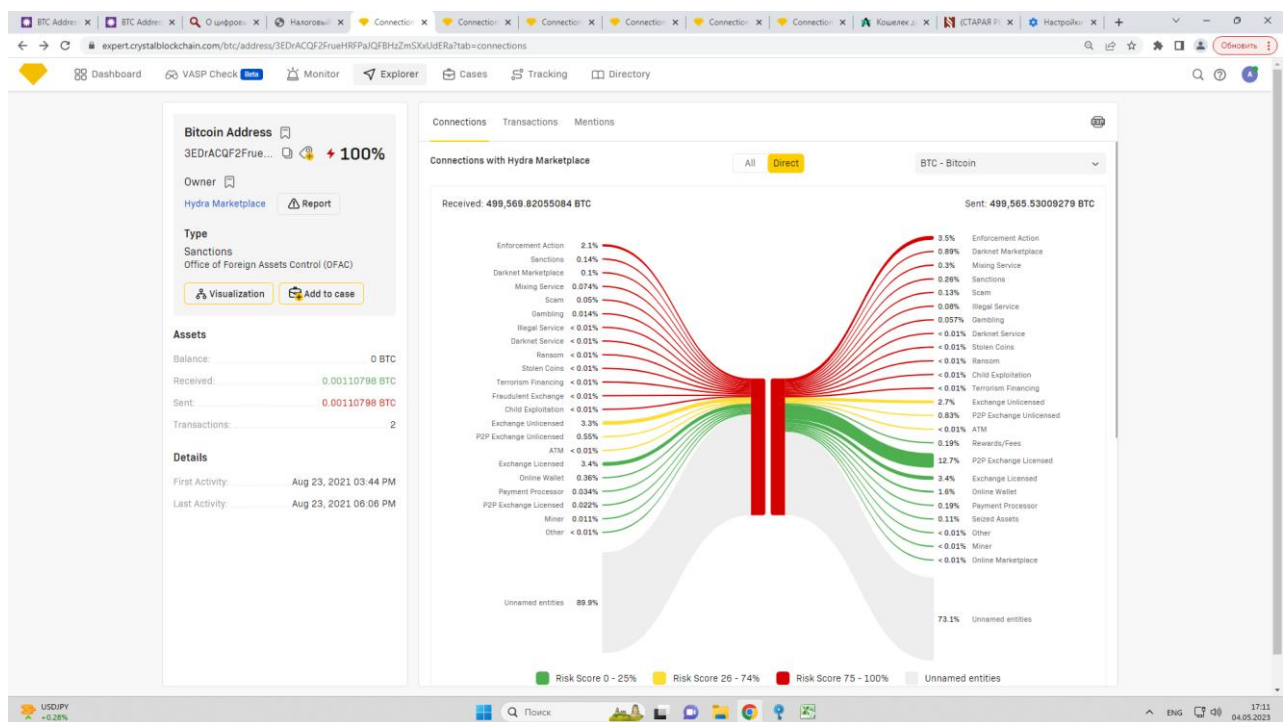
Фигурант осуществлял деятельность по майнингу криптовалюты, не уведомляя соответствующие контролирующие и надзирающие органы.

Действовал без регистрации ИП/юридического лица, что предусмотрено для подобного рода деятельности.

Не оплачивал фиксированную плату за электричество, израсходованное на майнинг криптовалют.

Проведен детальный анализ криптовалютных транзакций лица, с оценкой их риска (рис. 4). Определена высокорисковая деятельность «майнера».

Рис. 4. Анализ транзакций в криптовалюте



Кыргызская Республика

ПФР Кыргызской Республики были получены СПО от подотчетного лица относительно подозрительной деятельности одного из клиентов финансового учреждения под названием «КЛИНИКА». В результате анализа СПО установлено, что «КЛИНИКА» получала денежные средства от

иностранных физических лиц за разработку программного обеспечения и информационные услуги. В последующем денежные средства переводились субъектам другого иностранного государства за информационные услуги и в рамках договора за услуги.

ПФР в рамках сбора сведений направлены запросы в государственные органы и международные запросы по линии Группы Эгмонт.

По результатам сбора сведений было установлено, что компания «КЛИНИКА» не зарегистрировала на территории Кыргызской Республики программные продукты в качестве интеллектуальной собственности, а также не импортировала/экспортировала серверные оборудования или другие компьютерные комплектующие.

В рамках полученного ответа от иностранного партнера установлено, что ранее перечисленные денежные средства со счета компании «КЛИНИКА» были использованы для приобретения виртуальных активов.

Таким образом, со стороны ПФР была выявлена сомнительная деятельность компании «КЛИНИКА», которая занималась предположительно куплей-продажей виртуальных активов в пользу граждан другого государства, замаскировав свою деятельность под оказание услуг и поставки товаров.

Данный факт был направлен в адрес правоохранительных органов Кыргызской Республики для дальнейшей реализации и дачи юридической оценки.

В данной схеме были задействованы свыше 60 граждан иностранного государства, 5 компаний нерезидентов и 1 компания резидент.

В настоящее время по данному факту возбуждено и расследуется уголовное дело со стороны следственных органов.

Выявленные три особенности при исследовании данного факта:

- предоставление разных контрактов и договоров по содержанию, но с одинаковыми реквизитами (номер контракта и дата) в банковские учреждения со стороны участников сделки;
- использование разных юрисдикций в финансовых комбинациях, и использование кыргызской компании для аккумуляции денежных средств и возможного сокрытия фактов приобретения виртуальных активов;
- преимущественно использование сферы предоставления услуг или приобретения продуктов интеллектуальной работы, ценность которых трудно определить.

Приложение 2. Свод рекомендаций

1. Государствам членам-членам ЕАГ, странам и организациям наблюдателям рекомендуется проводить оценку уровня развития индустрии виртуальных активов на основе анализа:

- нормативно-правовой базы;
- степени вовлеченности граждан и юридических лиц в выпуск, оборот, обмен виртуальных активов;
- деятельности провайдеров услуг виртуальных активов, включая способы их регистрации в специальных реестрах (в случае наличия разрешительных механизмов).

2. Проводить комплексную оценку рисков использования виртуальных активов и инфраструктуры их провайдеров. Оценивать возможные, в том числе макроэкономические эффекты деятельности ПУВА.

3. Учитывать риски, связанные с возможным использованием виртуальных активов в преступных целях, выявляемые юрисдикциями. Особое внимание обращать на использование миксеров, высоко анонимных типов виртуальных активов.

4. Определять порядок декларирования дохода от обмена/оборота виртуальных активов, а также фактов обладания виртуальными активами в соответствии с налоговым Законодательством конкретной юрисдикции.

5. Применять и (или) развивать специальные сервисы мониторинга для выявления высокорисковых транзакций и участников.

6. Проводить оценку риска деятельности провайдеров услуг виртуальных активов с помощью сервисов мониторинга криптовалютных транзакций.

7. Развивать международное сотрудничество в части взаимного обогащения сведениями по направлению развития индустрии виртуальных активов и обмена сведениями о физических и юридических лицах, участвующих в транзакциях в виртуальных валютах.

8. Развивать координационные группы, межведомственные Комиссии и Соглашения о сотрудничестве на национальном уровне для минимизации рисков и угроз в части расширения применения виртуальных активов.

9. Учесть в регулировании R2P площадки как ПУВА, распоряжающиеся криптоактивами третьих лиц – разграничить с точки зрения регулирования ответственность площадки и физических лиц, торгующих на них.

10. Выработать критерии для отделения лиц, использующих P2P площадки для проведения регулярной профессиональной деятельности в области криптообменных операций.

11. Выявлять и применять меры к незаконно действующим на территории страны и использующим оборудование страны ПУВА. Поставить на постоянный мониторинг происхождение средств, получаемых ПУВА, действующими на территории страны. Наладить взаимодействие или противодействие с иностранными ПУВА, работающими на территории страны.

12. Выработать меры по предотвращению работы незарегистрированных ПУВА с использованием оборудования на территории и с гражданами стран.

13. Запретить оборот монет повышенной анонимности на зарегистрированных ПУВА.

14. Противодействовать деятельности миксеров и ПУВА, не осуществляющих надлежащие усилия в области ПОД/ФТ.

15. Обеспечить скорость взаимодействия по получению данных от ПУВА, зарегистрированных в странах.

16. Обеспечить взаимодействие по блокированию использования незарегистрированными ПУВА:

- национальных доменов;
- IP адресного фонда провайдеров;
- национальных провайдеров;
- финансовых каналов финансовой системы стран;
- участия в незарегистрированных ПУВА граждан стран и физических офисов работы.

17. Выработать стандарты в обмене сообщениями и запросами, связанными с финансовыми расследованиями в криптовалютах.