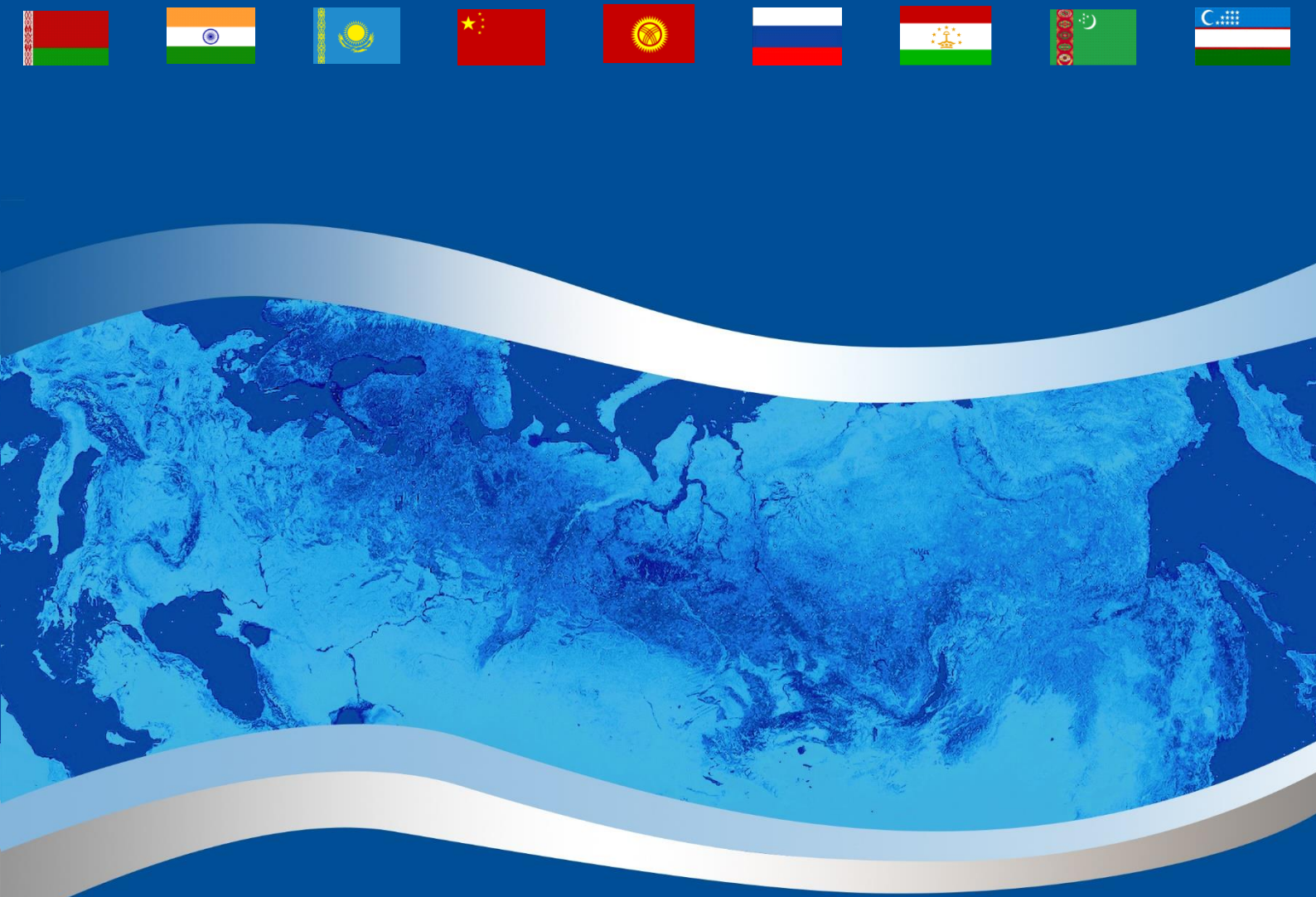
ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов
и финансированию терроризма

EURASIAN GROUP
on combating money laundering
and financing of terrorism



«ЛЕГАЛИЗАЦИЯ (ОТМЫВАНИЕ) ПРЕСТУПНЫХ ДОХОДОВ ОТ КИБЕРПРЕСТУПЛЕНИЙ, А ТАКЖЕ ФИНАНСИРОВАНИЕ ТЕРРОРИЗМА ЗА СЧЕТ УКАЗАННОЙ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ, В ТОМ ЧИСЛЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ДЕНЕГ ИЛИ ВИРТУАЛЬНЫХ АКТИВОВ И ИНФРАСТРУКТУРЫ ИХ ПРОВАЙДЕРОВ»

ТИПОЛОГИЧЕСКИЙ ПРОЕКТ ЕАГ

2022 ГОД

СОДЕРЖАНИЕ

Введение

1. Радикальное изменение социально-экономической конъюнктуры вследствие кризисных явлений в глобальной экономике обуславливают возникновение новых способов совершения преступлений. Все чаще в качестве инструмента платежей и объекта преступного интереса используются виртуальные активы (криптовалюты, токены) и электронные деньги. Динамика распространения преступных деяний с использованием виртуальных активов создает необходимость не только межведомственного, но и наднационального сотрудничества.
2. Легализация преступных доходов может обеспечиваться за счет использования провайдеров услуг виртуальных активов (ПУВА), а также анонимности транзакций в виртуальных активах. Кроме того, такие активы все чаще применяются для финансирования террористических группировок.
3. В ходе реализации проекта достигнуты все поставленные цели:
    - Обеспечение эффективного трехстороннего взаимодействия государства (в лице регуляторов), финансово-кредитных учреждений и частного сектора для сокращения числа киберпреступлений и снижения риска ПОД/ФТ в сфере использования виртуальных активов.
    - Сбор и анализ детальной информации о провайдерах услуг виртуальных активов в государствах-членах ЕАГ.
    - Выявление и классификация характерных особенностей киберпреступлений и преступных деяний, связанных с использованием виртуальных активов, в том числе криптовалют.
    - Систематизация преступлений, совершенных с использованием виртуальных активов.
    - Классификация провайдеров услуг виртуальных активов в государствах-членах ЕАГ.
    - Сбор детальной информации о ПУВА, имеющих представительства или зарегистрированных в юрисдикциях государств-членов ЕАГ. Анализ деятельности незаконных ПУВА.
    - Обмен опытом мониторинга и анализа криптовалютных транзакций и транзакций с использованием электронных средств платежа с целью выявления, пресечения и расследования преступлений, совершенных с использованием виртуальных активов.
4. Выражаем признательность всем странам-участникам и ведомствам, принявшим участие в проекте, и надеемся, что результаты типологического проекта будут использованы заинтересованными лицами: государственными институтами, в частности, надзорными, контрольными, правоохранительными органами, подразделениями финансовой разведки, кредитно-финансовыми организациями и представителями частного сектора.

Особенности правового регулирования оборота виртуальных активов и электронных платежных средств

5. Все 8 государств-членов ЕАГ (Казахстан, Кыргызстан, Таджикистан, Туркменистан, Узбекистан, Китай, Беларусь, Россия) и Монголия (является наблюдателем ЕАГ) относятся к романо-германской (континентальной) правовой семье, причем российская правовая система имеет формально-юридическое сходство с романо-германской правовой семьей, но со своими особенностями, что позволяет ее отнести к смешанной форме.
6. На законодательном уровне вопрос оборота виртуальных валют урегулирован в Казахстане, Кыргызстане, Узбекистане, Беларуси, Монголии. Не урегулирован в Туркменистане, Таджикистане, России.
7. Председателем Правительства Российской Федерации утверждена Концепция законодательного регламентирования механизмов организации оборота цифровых валют № Д-П13-1613; Минфином России внесен в Правительство РФ проект ФЗ «О цифровой валюте». В России на законодательном уровне урегулированы вопросы использования электронных средств платежа и цифровых финансовых активов: ФЗ от 27.06.2011 № 161-ФЗ «О национальной платежной системе», от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле», ФЗ от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Правоприменительная практика в целом исходит из придания виртуальным валютам статуса имущества и в необходимых случаях распространяет на них соответствующие нормы права.
8. В Китае запрещены все виды деятельности, связанные с виртуальными валютами. В сентябре 2021 года Народный банк Китая совместно с компетентными органами выпустил Уведомление о дальнейшем предотвращении и снижении рисков операций с виртуальными валютами и спекуляций.
9. Регулирование деятельности электронных платежных систем находится в ведении Центральных банков большинства стран ЕАГ.

Пример Казахстана:

10. Цифровые активы (цифровое выражение стоимости) являются обеспеченными или необеспеченными (цифровые токены, полученные как вознаграждение за участие в поддержании консенсуса в блокчейне). В соответствии с пунктом 55-1 статьи 1 и Статьи 33-1 (Правовой режим оборота цифровых активов) Закона Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» цифровые финансовые активы признаются имуществом, но не признаются инструментами платежа.
11. Оборот децентрализованных активов допускается исключительно на территории МФЦА (Международный финансовый центр «Астана»), где деятельность с криптовалютой разрешена при соблюдении четких требований.
12. Деятельность с обращением криптовалюты в МФЦА включает в себя:
13. управление объектом торговли цифровыми валютами («криптобиржа»);
14. обеспечение хранения и управления цифровыми валютами, принадлежащими другому лицу.

Электронные платежные системы:

15. Регулирование платежных систем, регламентирование их деятельности и надзор за ними осуществляет Национальный Банк Республики Казахстан в соответствии с законодательством Республики Казахстан о платежах и платежных системах в соответствии со ст.4 Закона Республики Казахстан от 26 июля 2016 года № 11-VI ЗРК «О платежах и платежных системах».
16. В части мер регулирования Национальный Банк Республики Казахстан:

- устанавливает правила и порядок осуществления надзора за платежными системами;
- принимает обязательные для исполнения нормативные правовые акты, направленные на обеспечение эффективности и надежности функционирования платежных систем на территории Республики Казахстан;
- определяет критерии значимости платежных систем;
- устанавливает показатели, при которых платежная система относится к значимым системам;
- определяет правила ведения реестра системно значимых, значимых и иных платежных систем Республики Казахстан, их включения в этот реестр и исключения из него.

17. Оператором системы электронных денег может быть только банк, организация, осуществляющая отдельные виды банковских операций, или платежная организация, получившая соответствующую лицензию на осуществление банковской деятельности или прошедшая регистрацию в качестве платежной организации.

Пример Кыргызстана:

18. Законодательные акты в сфере выпуска, оборота и обмена виртуальных активов:
    - Закон Кыргызской Республики «О виртуальных активах» (от 21 января 2022 года № 12, официально опубликован 28.01.2022 г. и вступает в силу по истечении 6 месяцев со дня опубликования).
    - Налоговый кодекс Кыргызской Республики (№ 3 от 18 января 2022 года).
19. Законодательные акты в сфере выпуска, оборота и обмена виртуальных активов:
    - Закон Кыргызской Республики «О платежной системе Кыргызской Республики» (от 21 января 2015 года № 21).
    - Положение «Об электронных деньгах в Кыргызской Республике» (утверждено постановлением Правления Национального банка Кыргызской Республики от 30 марта 2016 года № 15/6).
20. Законодательно разрешены: покупка и продажа (обмен) виртуальных активов; обмен одного типа виртуальной валюты на другой; хранение, управление виртуальными активами; оказание финансовых услуг, связанных с первичным размещением и (или) продажей виртуальных активов.
21. Банкам, небанковским финансово-кредитным организациям и иным юридическим лицам, поднадзорным Национальному банку, запрещается осуществлять следующие операции: покупка и продажа (обмен) виртуальных активов; обмен между виртуальными активами.
22. Группы участников отношений в сфере оборота виртуальных валют: провайдеры услуг виртуальных активов, майнеры, лица, осуществляющие эмиссию и первичное предложение виртуальных активов.

Электронные платежные системы:

23. Взаимодействие Государственной службы финансовой разведки Кыргызской Республики с операторами электронных платежных систем осуществляется в соответствии с Законом Кыргызской Республики «О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов» от 06.08.2018 года № 87 и Положению о порядке представления информации и документов в орган финансовой разведки

Кыргызской Республики (утверждено постановлением Правительство Кыргызской Республики от 25.12.2018 года № 606).

Пример Узбекистана:

24. Действует Закон Республики Узбекистан от 14.07.2021 № ЗРУ-701 «О лицензировании, разрешительных и уведомительных процедурах» (лицензия для осуществления деятельности в сфере оборота крипто-активов, с подвидом лицензионной деятельности «деятельность крипто-биржи»).
25. Виды операций с виртуальными валютами, которые законодательно разрешены: купля-продажа криптоактивов на фиатную валюту, обмен одного криптоактива на другой криптоактив, выпуск токенов.
26. Законодательно запрещены: операции с анонимными криптоактивами, использование криптоактивов в качестве средства платежа на территории Республики Узбекистан.
27. Группы участников отношений в сфере оборота виртуальных валют: разрешена деятельность по майнингу и провайдеров услуг в сфере оборота крипто-активов. Видами провайдеров услуг в сфере оборота крипто-активов являются крипто-биржа, майнинг-пул, крипто-депозитарий и крипто-магазин.

Электронные платежные системы:

28. Под платежной системой понимается совокупность отношений, обеспечивающих осуществление платежей путем взаимодействия оператора платежной системы, участников платежной системы и (или) платежных организаций посредством применения процедур, инфраструктуры и правил платежной системы, установленных оператором платежной системы.
29. Оператором платежной системы является юридическое лицо, осуществляющее деятельность по обеспечению функционирования платежной системы на территории Республики Узбекистан, имеющее соответствующую лицензию и обеспечивающее функционирование системы электронных денег.
30. Деятельность операторов платежных систем и платежных организаций лицензируется Центральным банком Республики Узбекистан.
31. Отдельно выделяются значимые платежные системы, чья бесперебойная работа способствует стабильному функционированию рынка платежных услуг Республики Узбекистан, а сбои в ее работе могут привести к возникновению рисков на рынке платежных услуг Республики Узбекистан.
32. Платежная система относится к значимой, если она занимает долю рынка платежных услуг свыше значения, установленного Центральным банком для данного рынка, и (или) если через платежную систему осуществляются платежи на территории Республики Узбекистан в течение года в объеме не менее показателей, устанавливаемых Центральным банком.

Пример Беларуси:

33. В части регулирования деятельности субъектов цифровой экономики, выпуска, обмена и оборота цифровых валют на территории Республики Беларусь в Парке высоких технологий (ПВТ) действуют: 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"
34. Объект регулирования: цифровые знаки (токены); электронные деньги.
35. Физические лица вправе владеть токенами и совершать следующие операции: майнинг, хранение токенов в виртуальных кошельках, обмен токенов на иные токены, приобретение/отчуждение за белорусские рубли, иностранную валюту, электронные деньги, дарение и завещание токенов.

36. Юридические лица вправе владеть токенами и совершать операции по:
    - созданию/размещению собственных токенов в Беларуси и за рубежом через резидента ПВТ;
    - хранению токенов в виртуальных кошельках;
    - приобретению/отчуждению токенов через операторов криптоплатформ, операторов обмена криптовалют, иных резидентов ПВТ.
37. Индивидуальные предприниматели - резиденты ПВТ - вправе:
    - осуществлять указанные выше правомочия;
    - через резидента ПВТ создавать и размещать собственные токены в Беларуси и за рубежом;
    - осуществлять иную деятельность с использованием токенов.
38. Виды операций с виртуальными валютами, которые законодательно запрещены: предпринимательская деятельность физических лиц, а также юридических лиц, не являющихся резидентами ПВТ.
39. Выделяются группы участников отношений в сфере оборота виртуальных валют: резиденты ПВТ, оператор криптоплатформы, оператор обмена криптовалют.

Пример Монголии:

40. Действует Закон о провайдерах услуг виртуальных активов. Законодательно разрешены:
    - обмен виртуальных активов на фиатные валюты и обратно;
    - обмен виртуальных валют одного типа на другой;
    - передача виртуальных активов;
    - хранение и управление виртуальными активами или связанными с ними инструментами;
    - предоставление финансовых услуг, связанных с публичной эмиссией виртуальных активов или торговлей виртуальными активами.
41. Запрещается предлагать или продавать виртуальные активы населению без их передачи компании, зарегистрированной в качестве поставщика выше указанных услуг.
42. Группы участников отношений в сфере оборота виртуальных валют: Подразделение финансовой разведки, правоохранительные органы, провайдеры услуг виртуальных активов, Комиссия по финансовому регулированию – в части осуществления деятельности по регистрации и мониторингу.

Международное взаимодействие в сфере регулирования оборота виртуальных активов и электронных денег

43. Международное взаимодействие в государствах-членах ЕАГ осуществляется в рамках ратифицированных международных договоров, соглашений или на основе принципа взаимности. Отдельных правовых актов в части цифровой валюты и цифровых финансовых активов на международном уровне не предусмотрено.
44. Организация взаимодействия с операторами электронных платежных систем лежит в сфере ответственности органов внутренних дел, государственной безопасности и подразделений финансовых разведок.

45. Взаимодействие провайдеров услуг виртуальных активов с ПФР осуществляется в рамках выполнения требований законодательства о ПОД/ФТ в соответствии со следующими документами:
    - Законы о противодействии легализации доходов, полученных преступным путем, финансированию террористической деятельности и финансированию распространения оружия массового поражения;
    - Законы о национальной платежной системе;
    - Законы об ОРД;
    - Законы о связи;
    - Законы об информации, информационных технологиях и о защите информации;
    - 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» (Узбекистан).
46. Взаимодействие ПФР и правоохранительных органов в части ответов на запросы, направляемые провайдерам услуг виртуальных активов, осуществляется в рамках существующих правовых актов и межведомственных инструкций:
47. Международное взаимодействие при проведении расследований преступлений, связанных с оборотом виртуальных активов, осуществляется в рамках уголовно-процессуального законодательства стран (Беларусь, Казахстан, России, Монголии). Компетентным органом направляются поручения об оказании правовой помощи по каналам:
    - НЦБИ (для правоохранительных органов Беларуси, России),
    - МОУП Интерпол (для правоохранительных органов Беларуси, Монголии),
    - Министерства юстиции (Китай), при отсутствии договора о взаимной правовой помощи по дипломатическим каналам (Китай);
    - сети «Эгмонт» (для ПФР Беларуси, Кыргызстана, Монголии, России, Туркменистан),
    - Системы обмена информации в рамках СРПФР СНГ (Кыргызстан).
48. Неформально направляются обращения о получении информации о регистрации собственности, компании, доли участия в юридических лицах и др., не требующих санкции суда: в службу технической поддержки или руководству криптоплатформ посредством электронной почты, используя сеть CARIN (Беларусь), международные сети обмена информацией «Карин» - Европа и Арин Ап – Азия, открытые источники (Казахстан), сеть Арин (Монголия). Используется неофициальная переписка и переговоры (Кыргызстан).
49. В ходе проведения финансовых расследований преступлений, связанных с использованием виртуальных активов, страны руководствуются международными соглашениями и ратифицированными конвенциями, межведомственными соглашениями и меморандумами, национальным законодательством.
50. В целях расследования преступлений, требующих проведения трудоемких и сложных следственных действий, следственными органами могут быть созданы межведомственные следственные группы (Кыргызстан), специализированные группы по конкретным кейсам

(Беларусь), межведомственные и международные рабочие группы в рамках расследования конкретных уголовных дел (Россия).

51. Совместные международные расследования в сфере виртуальных активов проводят Таджикистан, Китай, Россия, Кыргызстан.
52. Организация исполнения и контроль полноты и своевременности выполнения международных запросов лежит на каждом сотруднике компетентного ведомства, в том числе на подразделении/сотруднике, ответственном за международное взаимодействие. Также, например, в Узбекистане имеется внутренний документ Департамента, регулирующий вопросы своевременности (приоритетности) исполнения международных запросов.
53. В запросах, направляемых в ПФР зарубежных юрисдикций в части расследования преступлений, связанных с оборотом виртуальных валют, в зависимости от наличия информации указываются следующие сведения:
    - информация об официальном расследовании или судебном разбирательстве по делу;
    - информация о компетентных органах, вовлеченных в данное расследование;
    - краткая фабула преступления, связь со страной, ПФР которого должно раскрыть информацию;
    - данные фигурантов (ФИО, дата рождения; номер мобильного телефона; реквизиты банковских карт; адрес эл. почты; никнейм фигуранта в ПУВА; номер криптовалютного кошелька/адреса либо аккаунта);
    - наименование и юрисдикция ПУВА в которых фигурант является клиентом, в т.ч. название биржи и обменного сервиса;
    - данные по операции (дата и время совершения операции; hash ID операции; сумма операции);
    - информация о возможной конфискации активов;
    - сумма и тип/сущность активов по данному делу.
54. С целью ускорения исполнения запроса в ряде юрисдикций допускается направление официальных запросов непосредственно в иностранный компетентный орган, владеющий запрашиваемой информацией, минуя отправку запроса в ПФР иностранной юрисдикции. Например:
    - Запрос может быть направлен непосредственно в иностранный компетентный орган, минуя ПФР: через Генеральную прокуратуру, Каналы НЦБ Интерпола, в рамках межведомственных соглашений и меморандумов о взаимопомощи, в иностранные центральные банки/иные органы банковского надзора.
    - Направление отсканированной копии офиц. запроса на эл. почту ПУВА.
    - Неформальное обращение к руководителю органа об ускорении исполнения запроса.
    - Направление запроса с пометкой СРОЧНО.
55. Формальное международное взаимодействие формальное осуществляется в рамках уголовно-процессуального законодательства, также путем направления запросов об оказании правовой помощи по каналам НЦБИ, МОУП Интерпол, Министерства юстиции, Дипломатические каналы, ЭГМОНТ, СОИ СРПФР.

56. Органы формального международного взаимодействия:
    - Судебные органы, Министерство юстиции, Дипломатические каналы, подразделения финансовой разведки, правоохранительные органы.

Роль частного сектора в противодействии ОД/ФТ

57. Участие частного сектора допускается при проведении расследований (в качестве специалиста, эксперта; при подаче финансовыми учреждениями информации в ПФР) в Кыргызстане, Китае, России.
58. Информация, направленная представителями частного сектора: финансовыми учреждениями, нефинансовыми учреждениями, в виде заявления физических и юридических лиц (на бумажном носителе или в виде электронного документа по типовой форме) в инициативном порядке в ПФР, является поводом для проведения финансовых расследований: в Кыргызстане, в Казахстане, в Туркменистане, в России, в Таджикистане, в Беларуси, в Монголии, Китай, в Узбекистане. Направляются сообщения СПО, а также сведения о наличии фактов ОД/ФТ. После анализа информация направляется в правоохранительные органы.

Пример России:

59. Организовано взаимодействие с ПАО «Россети Северный Кавказ» по выявлению организаторов незаконных майнинг-ферм на территории округа. Совместная работа позволила выявить два физических лица, которые, предположительно, причастны к финансированию МТО и связанны с майнингом криптовалюты. Проведено финансовое расследование, материалы переданы в правоохранительные органы для проведения комплекса ОРМ.
60. Проблемы при взаимодействии государственных органов с частным сектором в сфере расследования преступлений, связанных с использованием виртуальных валют:
    - недостаточное регулирование на законодательном уровне;
    - финансовым учреждениям сложно идентифицировать операции с виртуальной валютой;
    - анонимность переводов денежных средств;
    - внутренний контроль кредитных организаций не ориентирован на глубокий анализ переводов между ФЛ;
    - большинство криптоплатформ работают в международном формате, но не имеют официальной привязки к конкретной юрисдикции (усложняет процесс информационного взаимодействия с ними);
    - операции с виртуальными активами обычно осуществляются на основе специальных платформ, а не через финансовые учреждения (как правило, платформы, установлены на серверах в иностранных юрисдикциях);
    - длительные сроки получения запрашиваемых сведений.

Классификация ПУВА и электронных платежных систем в государствах-членах ЕАГ

61. ПУВА являются субъектами экономической деятельности в Казахстане, Кыргызстане, Узбекистане, Таджикистане, Беларуси. Не являются субъектами экономической деятельности в Туркменистане, Монголии, Китае, России.

62. В Казахстане имеются коды деятельности организаций, ведущих выпуск, учет и обращение виртуальных валют.
63. Указанная деятельность классифицируется как предпринимательская в Кыргызстане, деятельность в сфере оборота крипто-активов – в Узбекистане.
64. В Беларуси имеется код в Общереспубликанском классификаторе Республики Беларусь «Виды экономической деятельности» (ОКРБ 005-2011) по направлению: 63111 – Деятельность по майнингу цифровых знаков (токенов).
65. В Казахстане выделяется деятельность по выпуску цифровых активов, организации торгов и предоставлению услуг по обмену цифровых активов на фиатные деньги и обратно. Уполномоченный орган в сфере обеспечения информационной безопасности – Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан определяет порядок выпуска и оборота обеспеченных цифровых активов и цифровых валют.
66. Требования к провайдерам услуг виртуальных активов, предъявляемые в государствах-членах ЕАГ, кроме Китая, где деятельность запрещена, касаются соблюдения законодательства ПОД/ФТ, соответствия лицензионным требованиям. Также выделяются требования к ПУВА: надежность, соблюдение требований в части сохранения конфиденциальности информации, наличие бизнес-плана, осуществление внутреннего контроля, законность происхождения капитала, отсутствие просроченных задолженностей по оплате сборов и т.д., наличие знаний в областях экономики, IT, права и другие.
67. Требования к операторам электронных платежных систем: предоставление отчетности и прочих сведений Центральному банку, бесперебойность работы, соблюдение мер ПОД/ФТ, соблюдение лицензионных требований, конфиденциальность данных.
68. Информационный обмен между провайдерами услуг виртуальных валют и надзорными органами осуществляется посредством электронной почты, письменных запросов. Передача информации о криптовалютных транзакциях и лицах их совершивших на основании запросов от компетентных государственных органов возможна в России, Узбекистане, Таджикистане, Беларуси. Не возможна в Туркменистане, Китае, Монголии, Казахстане.
69. Лицензирование деятельности ПУВА:
    - В Узбекистане ведется электронный реестр лицензий. Лицензионные требования предъявляются к размеру уставного фонда, организации электронной системе торгов, правила торговли, формированию котировок валют и хранению информации о транзакциях.
    - В Казахстане лицензирование осуществляется на площадке МФЦ «Астана».

Пример Узбекистана: Блокировка и отзыв лицензии на деятельность провайдера услуг виртуальных активов.

70. В соответствии с п. 33-35 Положения о порядке лицензирования деятельности криптовалютных бирж» лицензия:
    - приостанавливается в случае выявления нарушений;
    - прекращается на основании заявления о прекращении, ликвидации или реорганизации юридического лица (за исключением преобразования/слияния); в результате систематического / грубого нарушения лицензионных требований; неустранения лицензиатом обстоятельств, повлекших приостановление лицензии;
    - аннулируется в случае, если лицензиат в течение 3 месяцев с момента получения уведомления о выдаче лицензии не представил документ, подтверждающий

уплату государственной пошлины, не подписал лицензионное соглашение, заявление об аннулировании лицензии.

71. Решение о приостановлении/прекращении/аннулировании лицензии может быть обжаловано в судебной инстанции.
72. Классификация провайдеров услуг виртуальных активов осуществляется в Кыргызстане (по возможности использовать услуги электронных платежных платформ, по регистрации в налоговых органах в качестве субъекта налогообложения), в Беларуси (по видам деятельности), в Монголии.
73. Строгие требования к безопасности и эффективности в сфере ПОД/ФТ деятельности предъявляются в странах ЕАГ к операторам электронных платежных систем и собственно платежным системам.

Пример Кыргызстана:

74. Оператор электронной платежной системы обязан принять меры по противодействию финансированию террористической деятельности и легализации преступных доходов и реализации требовании законодательства Кыргызской Республики в сфере противодействия финансированию террористической деятельности и легализации преступных доходов.
75. Оператор осуществляет свою деятельность на основании лицензии, выдаваемой Национальным банком в соответствии с законодательством Кыргызской Республики, и требованиям, установленными в нормативно – правовых актах Национального банка.
76. Оператор должен обеспечивать конфиденциальность и хранение данных о держателях электронных денег и проведенных операциях с использованием электронных денег.
77. Оператор должен разработать внутренние правила и процедуры для обеспечения бесперебойного функционирования своей информационной системы и безопасности проведения платежей.
78. Оператор должен установить в своей информационно системе лимиты для электронных кошельков, выполнять условия по учету электронных денег в соответствии с условиями договора с банком, Положением об электронных деньгах и другими нормативными правовыми актами Национального банка.

Типологии отмывания преступных доходов

79. Страны-участники типологического проекта, руководствуются рекомендациями ФАТФ в сфере оценки рисков отмывания преступных доходов и финансирования терроризма в части использования виртуальных активов и электронных денег.
80. Риск использования виртуальных валют в части финансирования терроризма оценивается в Казахстане, Узбекистане, Таджикистане, Монголии, Китае, России; не оценивается в Туркменистане.
81. Использование виртуальных валют в контексте рисков отмывания преступных доходов и финансирования терроризма, связанных с пандемией коронавируса оценивается в Узбекистане, Китае, России; не оценивается в Казахстане, Туркменистане, Кыргызстане, Таджикистане, Монголии.
82. Эпизоды совершения преступлений, в ходе которых осуществляется хищение виртуальной валюты отмечаются в Беларуси, Монголии, Китае, России; не отмечаются в Казахстане, Туркменистане, Кыргызстане, Узбекистане, Таджикистане.
83. Эпизоды совершения преступлений, в ходе которых осуществляется хищение виртуальной валюты с применением насилия отмечаются в Китае, России; не отмечаются в Казахстане, Туркменистане, Кыргызстане, Узбекистане, Таджикистане, Беларуси, Монголии.

84. Указываются перечни признаков использования виртуальных валют с целью легализации доходов, полученных преступным путем:

Узбекистан (Правила внутреннего контроля по противодействию ЛПД и ФТ и ФРОМУ для лиц, осуществляющих деятельность в области оборота крипто-активов (№ 3309 от 09.06.21):

- крипто-кошельки использовали в преступных целях;
- выявлены операции обмен по заведомо невыгодному курсу;
- манипулирование ценами на крипто-активы;
- отсутствие «White paper»;
- на одном IP-адресе заведено большое количество криптовалютных кошельков;
- отмечается частая смена персональных данных, IP-адреса и домена;
- отсутствуют знания в сфере оборота крипто-активов.

Беларусь (Инструкция о порядке заполнения, представления, регистрации, учета и хранения специальных формуляров регистрации финансовых операций, подлежащих особому контролю, утв. постановлением Совета Министров Респ. Беларусь от 16.03.06 N 367):

- клиент отказывается от предоставления информации или предоставлена недостоверные сведения;
- отмечено дробление суммы транзакций и отсутствие их экономического смысла;
- используются виртуальные кошельки, заведомо связанные с противоправной деятельностью, в частности, в сфере НОН или миксеры и другие варианты обхода выявления контрагентов по транзакциям.

Монголия (Закон о противодействии отмыванию денег и финансированию терроризма):

- выявлен высокий риск клиента;
- определен значительный риск продукции и услуг.

Китай (Законодательство Китая):

- совершено несколько транзакций на значительную сумму в короткие сроки,
- созданы отдельные счета под разными именами.

Пример России (На основе документов методического обеспечения деятельности органов внутренних дел):

85. При изучении торговой площадки «Hydra», располагающейся в закрытом сегменте сети Интернет («Darknet»), установлено, что расчеты между продавцами и покупателями происходят в криптовалюте Bitcoin, кошельки которым предоставляются непосредственно площадкой. Для покупателей наркотиков, фальшивых банкнот и иных запрещенных к свободному обороту предметов, организован ряд сервисов, которые позволяют приобрести криптовалюту Bitcoin за рублевый эквивалент путем их зачисления на электронные кошельки Qiwi, Юmoney, банковские карты или баланс абонентского номера сотовой связи. Д/с, переведенные на реквизиты сервисов, зачисляются на счет в личном кабинете пользователя в виде криптовалюты Bitcoin. Ключевым признаком перевода д/с с QIWI Кошелька, используемого для расчетов, на QIWI Кошелек обменника является появление комиссии при проведении транзакции. В связи с этим сумма операции не является кратной и отображается с копейками. Конвертация д/с в криптовалюту происходит со «служебного» QIWI Кошелька обменника).

Вовлеченность криминальных структур в использование цифровых технологий

86. Анализ деятельности преступных группировок (по данным из открытых источников) проводится в России, Туркменистане, Кыргызстане, Узбекистане, Беларуси, Китае.
87. Вовлеченность криминальных структур и организованных преступных групп в совершение преступлений с использованием виртуальных валют оценивается в России, Кыргызстане, Узбекистане, Китае.
88. Анализ отчетов групп FATF, Egmont по мониторингу состояния киберпреступности проводится в России, Туркменистане, Кыргызстане, Узбекистане, Беларуси, Монголии, Китае.
89. Полученные материалы направляются в правоохранительные органы, используются при проведении финансовых расследований и для повышения квалификации сотрудников подразделений финансовой разведки, оцениваются актуальные и потенциальные риски, актуализируются признаки подозрительности.
90. Взаимодействие с Международными организациями уголовной полиции (Интерпол, Европол) осуществляется в Кыргызстане, Узбекистане, Таджикистане, Беларуси.
91. В Китае роль координатора в сфере сотрудничества с международными организациями уголовной полиции исполняет Министерство общественной безопасности.
92. Влияние транснациональных преступных групп на рынок криптовалют оценивается в России (по материалам СМИ), Узбекистане, Китае; не оценивается в Кыргызстане, Таджикистане, Монголии.
93. В Китае на основе информации зарубежных ПФР и СМИ выявляется участие транснациональных преступных групп в совершении преступлений, связанных с использованием виртуальных активов.

Использование OSINT (Разведка по открытым источникам):

94. Для выявления участия преступных групп в совершении преступлений, связанных с использованием виртуальных активов: используются инструменты анализа транзакций:
    - Wallet explorer – история транзакций биткойн-кошелька,
    - Blockpath.com –просмотр транзакций биткойн-кошелька в виде графика,
95. Инструменты мониторинга сегментов Интернет и Даркнет применяются в России, Узбекистане, Беларуси, Китае, Кыргызстане.
96. Программно-аналитические ресурсы, задействованные для мониторинга сегментов Интернет и Даркнет в России (Росфинмониторинг и МВД России) – Yandex, Google, TOR, Прозрачный блокчейн.

Выявление и расследование преступлений, связанных с оборотом виртуальных активов и электронных денег

97. Анализ состояния, структуры и динамики численности преступлений, связанных с оборотом виртуальной валюты проводится в Казахстане, в Беларуси (МВД ведет ЕГБДП, СК и иные правоохранительные органы наполняют ЕГБДП); в Китае (Народный банк Китая анализирует развивающиеся риски ОД/ФТ, связанные с виртуальными валютами, и направляет предупреждения о рисках и "красные флажки" своим филиалам и подотчетным организациям); в России (запрашиваются правоохранительные органы с целью получения практики по УД, анализируется форма статистического учета ГИАЦ МВД РФ).

98. Компьютерно-техническая экспертиза для установления предполагаемого использования вредоносного программного обеспечения с целью хищения средств осуществляется в Туркменистане, Беларуси, России (входит в компетенцию правоохранительных органов).

99. Сбор информации относительно использования ресурсов-анонимайзеров для сокрытия IP адреса предполагаемым преступником осуществляется в Кыргызстане, Узбекистане, Китае, России.

100. Взаимодействие ПФР с провайдерами услуг виртуальных валют с целью выявления и расследования преступлений, совершенных с использованием виртуальных валют и электронных денег осуществляется в Кыргызстане, в Беларуси, в Узбекистане; не осуществляется в Казахстане, Туркменистане, Таджикистане, Монголии, Китае, России.

101. Традиционные для государств-членов признаки, свидетельствующие о вероятном совершении преступлений, связанных с оборотом виртуальных валют и электронных денег:

- транзакции на значительную сумму в короткие сроки (как правило в течение 24 часов);
- транзакции с использованием нескольких счетов;
- средства поступают с кошелька, связанного с даркмаркетами;
- переводы денежных средств в пользу обменных сервисов для приобретения и продажи криптовалюты;
- использование банковских инструментов, открытых на подставных лиц («дропов»);
- непродолжительный срок работы банковской карты;
- отсутствие платежей в пользу юридических лиц, операций по оплате товаров и услуг;
- пополнение банковских реквизитов на некратные суммы;
- использование VPN-соединения при пользовании банковскими продуктами;
- систематичность обналичивания денежных средств;
- создание, распространение и использование компьютерных программ для нейтрализации средств защиты компьютерной информации, несанкционированной модификации, копирования, уничтожения, блокирования компьютерной информации;
- выявленные хакерские атаки на вычислительную систему;
- ложные обменные пункты и криптобиржи;
- поддельные кошельки для хранения криптовалюты;
- фейковый облачный майнинг криптовалюты – проекты, имитирующие «облачные» майнинг-пулы, не имеющие в своем распоряжении необходимых мощностей и инфраструктуры (часто представляют собой мошеннические схемы под видом венчурных, инвестиционных проектов);
- операции с денежными средствами или иным имуществом лиц, включенных в перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения;

- операции, осуществляемые посредством платежных систем и мобильных приложений на счета, открытые на анонимного владельца, поступление средств из-за рубежа со счетов, открытых на анонимных владельцев (Казахстан).

102. Информация о возможно противоправном характере транзакций поступает в подразделения финансовой разведки государств-участников типологического проекта от зарубежных ПФР, кредитных организаций, правоохранительных органов, провайдеров услуг виртуальных активов, иных источников на бумажном носителе или в электронном виде.

103. Сообщения о подозрительных операциях поступают от кредитных организаций (в Казахстане форма ФМ1 реквизит 3.14, в России доп. код 6001 по коду 1190).

104. СПО не детализируется в Туркменистане, Кыргызстане, Таджикистане, Китае, Монголии. В Таджикистане не имеется системы быстрых сообщений о подозрительных операциях.

105. В ряде стран организуются межведомственные рабочие группы, допускается участие экспертов, специалистов, свидетелей и других, в том числе специалистов по блокчейну в соответствии с уголовно-процессуальным законодательством и ведомственными инструкциями. По результатам проведенных финансовых расследований информация направляется в правоохранительные органы или зарубежные ПФР для получения дополнительной информации. Специальных сроков финансового расследования по ВА нет (по общим правилам). Для расследования преступлений, связанных с виртуальной валютой, могут быть созданы совместные оперативные группы с участием правоохранительных органов и ПФР.

Пример Китая:

106. Народный банк Китая (НБК) проводит административные расследования. Если подозрения в легализации преступных доходов не могут быть устранены после административного расследования, НБК направляет информацию в правоохранительные органы для проведения дополнительных проверочных мероприятий.

Пример Узбекистана:

107. На постоянной основе проводится мониторинг Всемирной сети Интернет. В результате проведенной работы за период 2019-2020 гг. выявлено 6 фактов осуществления деятельности платежных платформ без лицензии. Материалы по выявленным фактам направлены в Департамент при Генеральной прокуратуре и налоговые органы, по итогам их рассмотрения возбуждено 4 уголовных дела. По одному из уголовных дел в доход государства обращено 9,5 биткоинов.

108. Выявлены 6 информационных ресурсов по оказанию незаконных услуг купли-продажи криптовалютных активов.

Пример России:

109. В ходе анализа выписок по банковским картам/счетам лиц, подозреваемых в преступной деятельности, не всегда можно установить, что денежные средства направляются на приобретение криптовалюты. Также не всегда удается установить какой именно криптобирже принадлежит адрес фигуранта или в какой юрисдикции находится данная биржа. В случае наличия соответствующих данных (например, крипто-адресов), направляются запросы в соответствующие ПФР, которые могут получить от соответствующих криптовалютных бирж установочные данные клиентов биржи, сведения о банковских картах и счетах, использующихся для купли-продажи криптовалюты за фиатные деньги и т.д. Однако это возможно лишь в том случае, если действие местного законодательства о ПОД/ФТ распространяется на лиц, оказывающих услуги криптовалютных бирж.

110. Проблемы общего (организационного) характера при проведении расследований преступлений, связанных с использованием виртуальных валют и электронных денег:

- отсутствие/недостаточность нормативно-правовой базы;

- отсутствие единой системы и алгоритма международного информационного взаимодействия с ПУВА (при более тесном взаимодействии с операторами электронных платежных систем);
- отсутствие механизма ареста/конфискации активов и другие.

111. Правовые акты и (или) межведомственные инструкции, регулирующие порядок взаимодействия ПФР и правоохранительных органов в части ответов на запросы, направляемые ПУВА:

- соглашения о взаимном сотрудничестве, межведомственные соглашения,
- инструкции по организации информационного взаимодействия с правоохранительными органами,
- уведомления,
- постановления о порядке ареста, хранения и конфискации.

112. Правоохранительные органы направляют в ПФР информацию в части использования виртуальных валют и электронных денег в противоправной деятельности: письменный запрос, содержащий фабулу, реквизиты уголовного дела, фигурантов, кошельков.

113. Арест активов в ходе расследования преступлений, связанных с использованием виртуальных валют возможен в Казахстане, Таджикистане, Узбекистане, Китае. Арестованные криптоактивы передаются для хранения в уполномоченный орган в Беларуси – путем перевода на специальный государственный кошелек либо путем проведения обмена арестованной криптовалюты на фиатные денежные средства под контролем следователя с последующим зачислением на банковский счет, предназначенный для арестованных денежных средств.

Примеры успешного взаимодействия:

114. Дело "PlusToken" (Китай): финансовая пирамида. В результате уголовного дела конфискованы виртуальные активы на общую сумму 40 млрд юаней.

115. В ДФО России пресечена деятельность финансовой пирамиды, осуществляющей мошеннические действия под видом инвестиционной деятельности и привлекавшей средства граждан РФ в виртуальные валюты и электронные деньги.

116. Операторы электронных платежных систем в Кыргызстане руководствуются в своей деятельности требованиями законодательства в сфере противодействия финансирования террористической деятельности и легализации (отмывания) преступных доходов. Таким образом, по результатам эффективной работы отдела внутреннего контроля электронной платежной системы, а именно по признанию операции подозрительной и направлению соответствующего сообщения в адрес ГСФР, было инициировано финансовое расследование, по результатам которого подготовлен обобщенный материал и направлен в правоохранительные органы.

117. В 2022 году от органов национальной безопасности поступило информирование о подозрительных операциях с банковской карты ДБ АО «Сбербанк России», принадлежавшей гражданке Казахстана «Т». По операциям данной карты проведен анализ, в ходе которого выяснено, что карта возможно используется для финансирования женщин –вдов боевиков ДАИШ, содержащихся в сирийском лагере «Аль-Хол». Также гр. «Т» при осуществлении переводов пользовалась услугами системы денежных переводов «Золотая Корона». Переводы осуществлялись на банковские карты Республики Казахстан и Российской Федерации. Мониторинг финансовых операций выявил группу лиц, которые имели внешние признаки религиозности и возможно причастность к финансированию терроризма. Среди указанных лиц выявлены ранее судимые граждане по фактам терроризма и экстремизма и включенные в

Перечень организаций и лиц, связанных с финансированием терроризма и экстремизма. Материалы переданы правоохранительным органам.

Способы финансирования терроризма с использованием виртуальных валют и электронных денег

Пример России:

118. Информация об осуществлении сборов денежных средств для нужд международных террористических организаций публикуется в закрытых телеграмм каналах, иных мессенджерах, социальных сетях, Qiwi – кошельков. В дальнейшем, аккумулированные средства либо выводятся на карты через несколько уровней карт или распыляются мелкими суммами на ряд других, по большей части не идентифицированных кошельков. Затем снимаются наличными на территории стран с повышенными рисками террористической активности.

119. Финансирование терроризма осуществляется при помощи электронных платежных систем: «Western Union», «Webmoney», «Qiwi», «Золотая корона», «Юнистрим», «Яндекс.Деньги». В качестве наиболее часто применяемого способа (до 95% случаев) отмечается использование «Qiwi» - кошельков.

120. Распространен способ осуществления денежных переводов с целью финансирования терроризма в Российской Федерации через ПАО «Сбербанк» (огромное количество клиентов, удобство использования сервиса интернет-банкинга «Сбербанк Онлайн», подключение банковских карт к международным платежным системам «Visa» и «Mastercard»).

Пример Узбекистана:

121. Гражданин А., находясь в зонах повышенной террористической активности, в социальной сети разместил публикацию, призывавшую переводить пожертвования участникам террористических организаций на его пластиковую карту. Полученные денежные средства впоследствии сконвертированы на валютную пластиковую карту с использованием приложения банка и сняты на территории зонах повышенной террористической активности.

Пример Казахстана:

122. Лицо, выполняющее роль «сборщика», аккумулирует денежные средства от разных лиц посредством денежных переводов через электронные кошельки под видом материальной помощи или благотворительности. В дальнейшем данное лицо лично или через третьих лиц на периодической основе переводит денежные средства через системы денежных переводов, основанием для которых чаще всего является материальная помощь в небольших размерах с целью не привлечения внимания со стороны уполномоченных государственных органов и отделов внутреннего контроля финансовых учреждений в страны с повышенной террористической активностью. Впоследствии денежные средства направляются на поддержу нужд международных террористических организаций.

Пример Китая:

123. Финансирование терроризма осуществляется с использованием электронных платежных систем: небанковские платежные услуги, электронные кошельки и предоплаченные карты.

Заключение

124. Результаты проведенного исследования нацелены на их практическое применение в работе странами, принявшими участие в проекте, а также всего евразийского региона в целом.

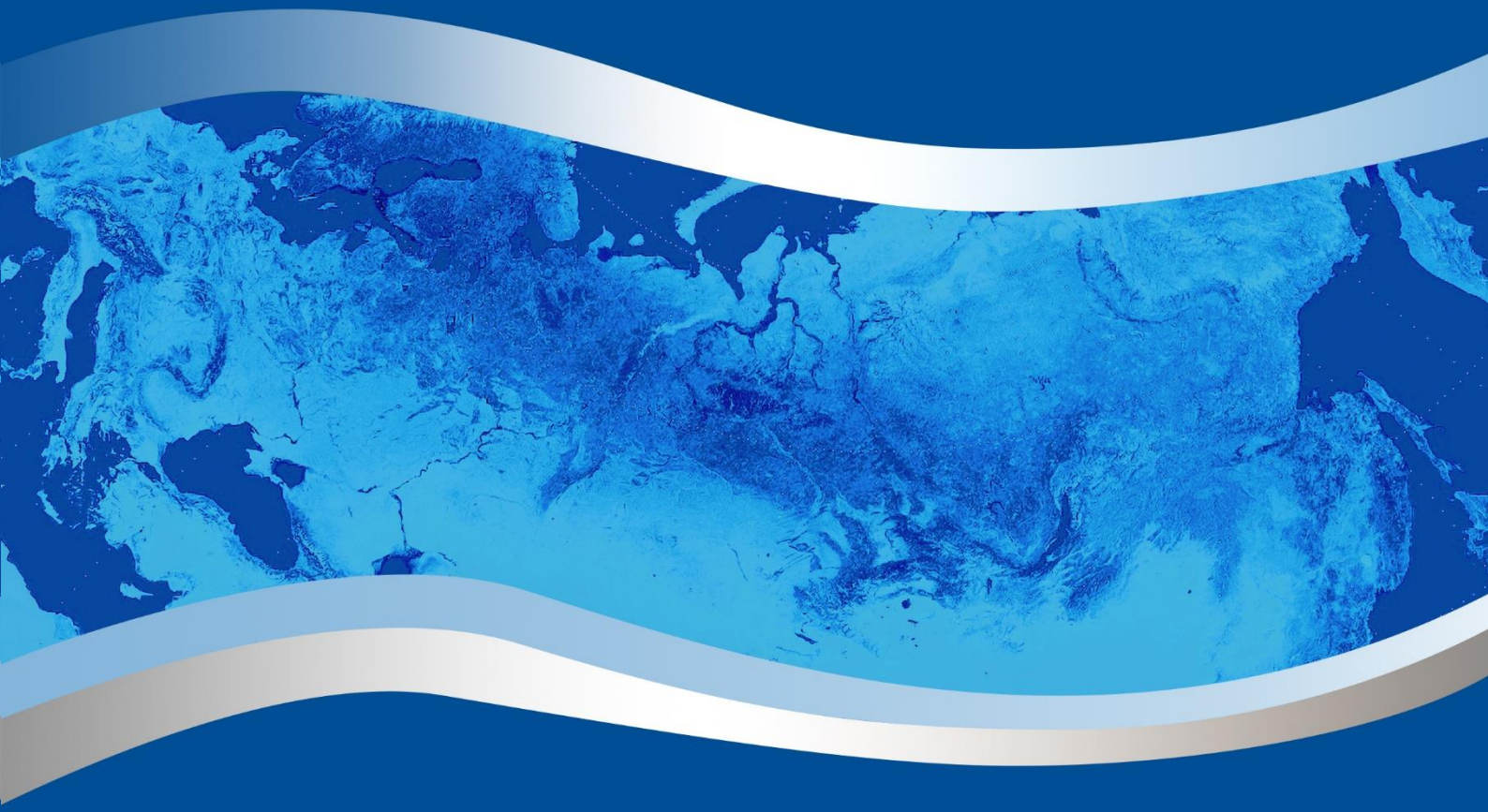
125. В ходе исследования от государств-участников типологического проекта были получены и обработаны сведения о регуляторных механизмах, применяемых в отношении деятельности провайдеров услуг виртуальных активов и операторов электронных платежных систем в рассматриваемых юрисдикциях.

126. Выявлены общие черты и различия в законодательстве стран в сфере организации работы криптовалютных платформ и электронных платежных систем.

127. Изучены принципы межведомственного и международного взаимодействия в части повышения эффективности работы подразделений финансовой разведки государств-участников типологического проекта.

128. Странами предоставлены примеры и типологии легализации преступных доходов с применением виртуальных активов и электронных денег.

129. Выражаем признательность государствам и ведомствам, принявшим участие в проекте.



www.eurasiangroup.org