



Банк России

июль 2022



**ОБЗОР СОБЫТИЙ
В СФЕРЕ ПРОТИВОДЕЙСТВИЯ
ОТМЫВАНИЮ ДОХОДОВ,
ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ,
И ФИНАНСИРОВАНИЮ
ТЕРРОРИЗМА**

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ	4
РОССИЙСКИЕ НОВОСТИ	5
Федеральные законы.....	5
• О начале работы Платформы ЗСК.....	5
• О Федеральном законе № 279-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений Федерального закона «О порядке формирования и использования целевого капитала некоммерческих организаций».....	6
• О Федеральном законе № 331-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений статьи 5.1 Федерального закона «О банках и банковской деятельности»	7
• О Федеральном законе № 297-ФЗ «О внесении изменений в статью 13.2 Федерального закона от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния»	7
МЕЖДУНАРОДНЫЕ НОВОСТИ.....	8
Новости ФАТФ и региональных групп по типу ФАТФ	8
• О приоритетных направлениях деятельности ФАТФ на период 2022-2024 гг....	8
• О выступлении президента ФАТФ	8
• О докладе ФАТФ «Сбор, анализ и защита данных».....	8
• О руководстве ФАТФ «О применении риск-ориентированного подхода к сектору недвижимости».....	9
• Об итогах первого раунда оценки рисков ОД/ФТ в Евразийском регионе (оценки наблюдаемых механизмов способов) ОД/ФТ).....	9
Новости международных организаций	11
• О докладе МВФ, Всемирного банка и БМР о важности обеспечения трансграничной совместимости и эффективного использования цифровых валют центральных банков	11
Новости европейских стран	11
• О докладе Европола об анализе текущего положения и трендов террористической активности в Европейском союзе.....	11
• О мерах Банка Нидерландов к поставщику услуг в сфере виртуальных активов Binance	12
• Об использовании платформ по обмену информацией между финансовыми организациями и провайдерами финансовых услуг.....	12
Новости других регионов	14
• Об исследовании Chainalysis использования «микшеров» с целью легализации доходов, полученных преступным путём.....	14
• О мерах Народного банка Китая к оператору цифровых платежей DiDi.....	15

Настоящий материал подготовлен
Департаментом финансового мониторинга и валютного контроля

Фото на обложке: Shutterstock.com

Адрес: 107016, Москва, ул. Неглинная, 12
Телефон: +7 499 300 30 00
Официальный сайт Банка России: www.cbr.ru

© Центральный банк Российской Федерации, 2022

СПИСОК СОКРАЩЕНИЙ

ПОД/ФТ/ФРОМУ	Противодействие легализации (отмыванию) доходов, полученных преступным путём, финансированию терроризма и финансированию распространения оружия массового уничтожения
ПОД/ФТ	Противодействие легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма
ОД/ФТ	Легализация (отмывание) доходов, полученных преступным путём, и финансирование терроризма
ОД	Легализация (отмывание) доходов, полученных преступным путём
ПОД	Противодействие легализации (отмыванию) доходов, полученных преступным путём
ФАТФ	Группа разработки финансовых мер борьбы с отмыванием денег
ЕАГ	Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма
РГТФ	Региональные группы по типу ФАТФ
ПУВА	Провайдеры услуг в сфере виртуальных активов
НПК	Надлежащая проверка клиентов

РОССИЙСКИЕ НОВОСТИ

Федеральные законы

1 июля 2022 года начала работать в полном объёме Платформа «Знай своего клиента» (Платформа ЗСК)¹.

В соответствии с изменениями, внесёнными Федеральным законом № 423-ФЗ² в Федеральный закон № 115-ФЗ³, вступившими в силу с 1 июля 2022 года⁴, кредитным организациям с помощью Платформы ЗСК Банком России предоставляется информация об уровне риска вовлечённости в проведение подозрительных операций юридических лиц и индивидуальных предпринимателей⁵.

Кредитные организации ежедневно получают информацию об отнесении своих клиентов и их контрагентов к одной из трёх групп риска проведения подозрительных операций (низкий риск, средний риск и высокий риск) и используют её при реализации процедур «противолегализационного» контроля. Информация Платформы ЗСК является для кредитных организаций вспомогательной, и окончательную оценку о добросовестности бизнеса своих клиентов с точки зрения «противолегализационного» законодательства они должны присваивать самостоятельно.

Ограничительные меры по распоряжению денежными средствами, находящимися на банковских счетах, а также иным имуществом клиента применяются только в том случае, если он отнесён к группе высокого риска и регулятором, и кредитной организацией. Кредитная организация обязана в течение 5 рабочих дней проинформировать клиента о том, что Банк России отнёс его к группе высокого уровня риска (со ссылкой на соответствующие критерии), и сообщить о применении ограничительных мер.

Предприниматели, не согласные с их включением в группу высокого риска, могут обжаловать такое решение в Межведомственной комиссии при Банке России, в которую входят Росфинмониторинг, ФТС России,

¹ Информационный сервис Платформа «Знай своего клиента» (Платформа ЗСК) включает в себя полнофункциональный аналитический программный комплекс, позволяющий аналитикам Банка России без обращения к другим программам и источникам проводить анализ клиента, а также обеспечивающий взаимодействие со всеми кредитными организациями.

² Федеральный закон от 21 декабря 2021 года № 423-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

³ Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма».

⁴ Федеральный закон № 115-ФЗ дополнен новыми статьями 7.6 – 7.8.

⁵ За исключением кредитных организаций, государственных органов и органов самоуправления.

уполномоченный по правам предпринимателей, а также представители банковских и бизнес-объединений.

Юридическому лицу или индивидуальному предпринимателю с низким уровнем риска банк не вправе отказать в открытии счета, проведении операции, если контрагентом также является низкорисковый клиент. Также с клиентом, отнесенным к «зеленой» группе, кредитная организация не может расторгнуть договор банковского счета.

Подробная информация о Платформе ЗСК, критериях отнесения юридических лиц и индивидуальных предпринимателей к группам риска размещена в специальной рубрике «Платформа «Знай своего клиента» в разделе «Противодействие отмыванию денег и валютный контроль» на официальном сайте Банка России в сети Интернет.

Источники информации: «Официальный интернет-портал правовой информации» (<http://www.pravo.gov.ru>), официальный сайт Банка России в сети Интернет.

14 июля 2022 года Президентом Российской Федерации подписан Федеральный закон № 279-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений Федерального закона «О порядке формирования и использования целевого капитала некоммерческих организаций».

Федеральным законом внесены изменения в статью 6 Федерального закона № 115-ФЗ, предусматривающие, что обязательному контролю не подлежат операции по получению и расходованию НКО⁶ денежных средств, связанных с:

- уплатой налогов и сборов, таможенных платежей, страховых взносов в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и иных обязательных платежей в бюджетную систему Российской Федерации, установленных законодательством Российской Федерации;
- оплатой жилого помещения и коммунальных услуг;
- уплатой комиссионного вознаграждения, взимаемого при совершении операций (сделок) организациями, осуществляющими операции с денежными средствами или иным имуществом;
- начислением процентов по вкладам (депозитам) и иным финансовым инструментам.

⁶ НКО – некоммерческая организация, не имеющая извлечение прибыли в качестве основной цели своей деятельности и не распределяющая полученную прибыль между участниками.

Указанные изменения вступили в силу 14 июля 2022 года.

Источник информации: «Официальный интернет-портал правовой информации» (<http://www.pravo.gov.ru>).

14 июля 2022 года Президентом Российской Федерации подписан Федеральный закон № 331-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений статьи 5.1 Федерального закона «О банках и банковской деятельности».

Федеральным законом внесены изменения в статью 6 Федерального закона № 115-ФЗ, предусматривающие:

- повышение порога обязательного контроля для финансовых операций с 600 тыс. рублей до 1 млн рублей (для операций по сделкам с недвижимым имуществом – с 3 до 5 млн рублей);

- новые полномочия Росфинмониторинга по определению операции с денежными средствами или иным имуществом при условии, что сведения о такой операции будут представляться в Росфинмониторинг. При определении операции в качестве подлежащей обязательному контролю будет устанавливаться вид данной операции, сумма её совершения, организации, осуществляющие операции с денежными средствами или иным имуществом, представляющие сведения о данной операции, а также период времени (не превышающий двух лет), в течение которого сведения о такой операции подлежат направлению в Росфинмониторинг.

Указанные изменения вступили в силу 14 июля 2022 года.

Источник информации: «Официальный интернет-портал правовой информации» (<http://www.pravo.gov.ru>).

14 июля 2022 года Президентом Российской Федерации подписан Федеральный закон № 297-ФЗ «О внесении изменений в статью 13.2 Федерального закона от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния».

Федеральным законом определено, что сведения о государственной регистрации актов гражданского состояния из ЕГР ЗАГС ⁷ в рамках межведомственного взаимодействия предоставляются Росфинмониторингу.

Федеральный закон вступил в силу с 25 июля 2022 года.

Источник информации: «Официальный интернет-портал правовой информации» (<http://www.pravo.gov.ru>).

⁷ Единый государственный реестр записей актов гражданского состояния.

МЕЖДУНАРОДНЫЕ НОВОСТИ

Новости ФАТФ и региональных групп по типу ФАТФ

1 июля 2022 года опубликовано заявление Президента ФАТФ Т. Раджи Кумара о приоритетных направлениях деятельности Группы на период 2022-2024 гг. под председательством Сингапура.

Отмечаются следующие ключевые направления деятельности:

- укрепление мер, направленных на возврат активов;
- противодействие незаконным финансовым потокам, связанным с киберпреступностью;
- повышение эффективности глобальных мер в сфере ПОД;
- укрепление партнёрских отношений ФАТФ с РГТФ.

Источник информации: официальный сайт ФАТФ в сети Интернет.

18 июля 2022 года в рамках встречи министров финансов и управляющих центральными банками стран Группы 20 состоялось выступление президента ФАТФ Т. Раджи Кумара.

Президент ФАТФ подчеркнул важность всеобъемлющей имплементации Международных стандартов по ПОД/ФТ/ФРОМУ в части виртуальных активов (ВА). Отметил, что в июне 2022 года опубликован обзор имплементации рекомендаций ФАТФ по ВА, в котором выражены опасения Группы относительно текущего статуса и темпов внедрения странами-членами Глобальной сети ФАТФ пересмотренных в 2019 году рекомендаций ФАТФ, касающихся ВА. В частности, в ходе подготовки обзора было установлено, что из 98 опрошенных стран только 11 в полной мере выполняют соответствующие рекомендации ФАТФ.

Президент ФАТФ призвал страны Группы 20 предпринимать своевременные меры по регулированию сферы ВА и проявлять бдительность в отношении связанных с нею рисков ОД/ФТ.

Источник информации: официальный сайт ФАТФ в сети Интернет.

20 июля 2022 года опубликован обновлённый доклад ФАТФ «Сбор, анализ и защита данных»⁸.

Доклад подготовлен в целях оказания содействия юрисдикциям в укреплении информационного сотрудничества между представителями частного сектора при соблюдении правил защиты данных и конфиденциальности.

В докладе приведены примеры лучших практик стран-членов Глобальной сети ФАТФ по обмену информацией между представителями частного сектора.

⁸ Data Pooling, Collaborative Analytics and Data Protection. Phase 2. Partnership to Fight Financial Crime.

Источник информации: официальный сайт ФАТФ в сети Интернет.

26 июля 2022 года опубликовано актуализированное руководство ФАТФ «О применении риск-ориентированного подхода к сектору недвижимости»⁹.

В руководстве отмечается, что инвестиционная популярность сектора недвижимости делает его особо привлекательным для преступников и других недобросовестных игроков, целями которых является сокрытие доходов от преступной деятельности. Кроме того, обращается внимание на плохое понимание присущих указанному сектору рисков ОД/ФТ, а также неэффективные меры по их снижению его представителями.

Также отмечаются следующие уязвимости сектора недвижимости, которые могут быть использованы преступниками в целях ОД/ФТ: покупка элитной недвижимости (в том числе публичными должностными лицами), использование виртуальных активов, а также использование анонимных компаний и «гейткиперов»¹⁰ в качестве инструментов ОД. В целях минимизации указанных уязвимостей сектору недвижимости необходимо повысить эффективность применяемых мер НПК (в том числе обеспечить доступность информации о бенефициарных владельцах по сделкам с недвижимостью).

Источник информации: официальный сайт ФАТФ в сети Интернет.

27 июля 2022 года ЕАГ опубликовано краткое резюме об итогах первого раунда оценки рисков ОД/ФТ в Евразийском регионе (РОР)¹¹.

По итогам первого раунда РОР установлены следующие наиболее актуальные угрозы в рамках Евразийского региона:

- уклонение от уплаты налогов и иных обязательных платежей, другие налоговые преступления (в том числе манипулирование (мошенничество) с НДС);

⁹ Guidance for a Risk-Based Approach. Real Estate Sector.

¹⁰ «Гейткиперы» (*gatekeepers*) – лица и организации, ответственные за безопасность финансовой системы и осуществление контроля за допуском к ней других лиц, например, клиентов и иных сотрудников той же организации; под такими лицами могут пониматься в том числе юристы, специалисты в области бухгалтерского учёта, налоговые консультанты, инвестиционные брокеры и др.

¹¹ В соответствии с Методологией проведения оценки рисков ОД/ФТ в Евразийском регионе в качестве региональных рисков рассматривались риски ОД/ФТ, имеющие общие признаки, характерные для двух и более государств-членов ЕАГ (а также риски, имеющие трансграничный характер). Проведение региональной оценки рисков охватывает период с 2017 по 2020 гг. В отчёте также приведены наблюдаемые странами тенденции в сфере ОД/ФТ более позднего периода – например, вследствие осложнения обстановки на территории Афганистана в 2021 году.

- взяточничество, иные преступления коррупционной направленности (включая незаконные действия с бюджетными средствами);
- мошенничество (включая незаконные действия с бюджетными средствами);
- незаконный оборот наркотиков;
- уклонение от уплаты таможенных пошлин и сборов и иные преступления в таможенной сфере;
- деятельность финансовых пирамид;
- незаконная предпринимательская деятельность;
- организация и содействие незаконной миграции.

В результате сопоставления угроз и уязвимостей, а также организационных факторов, влияющих на них, установлены региональные риски ОД в виде используемых схем либо их ключевых элементов в сложных и комплексных схемах ОД, придающих правомерный вид преступным средствам.

Среди региональных рисков, требующих значительного внимания и повышенных мер к их снижению выделены следующие риски:

- использование номинальных¹²/ подконтрольных компаний или индивидуальных предпринимателей;
- инвестирование преступного дохода в хозяйственную деятельность юридических лиц, в том числе находящихся в третьих странах;
- использование схем (в том числе фиктивных) приобретения / реализации движимого и недвижимого имущества на территории / за пределами государства;
- проведение «транзитных»¹³ операций по банковским счетам;
- проведение операций, связанных с обналичиванием;
- использование офшорных компаний.

По результатам проведения РОР планируется разработать мероприятия регионального и субрегионального характера, направленные на минимизацию выявленных рисков ОД/ФТ.

Источник информации: официальный сайт ЕАГ в сети Интернет.

¹² Для целей настоящего отчёта под номинальной компанией понимается бездействующая компания, используемая в качестве инструмента для различных финансовых махинаций или бездействующая для будущего использования в каком-либо другом качестве, а равно для сокрытия истинного выгодоприобретателя.

¹³ В контексте данного документа под «транзитными» операциями понимается получение значительных объёмов переводов на счета компании (физического лица) от большого числа лиц с последующим оперативным их списанием в адрес третьих лиц, в том числе с минимальной налоговой нагрузкой (или вовсе без уплаты налогов). Такие операции могут повторяться многократно.

Новости международных организаций

11 июля 2021 года опубликован подготовленный для Группы 20 совместный доклад Международного валютного фонда, Всемирного банка, Инновационного центра и Комитета по платежам и рыночным инфраструктурам Банка международных расчетов о важности обеспечения трансграничной совместимости и эффективного использования цифровых валют центральных банков (ЦВЦБ)¹⁴.

Отмечается, что как в случае с любой системой передачи денег и ценностей, ЦВЦБ могут использоваться для незаконной деятельности, которая подрывает стабильность финансовой системы. На риски ОД/ФТ при осуществлении операций с ЦВЦБ влияют место (страна) проживания потребителя, а также тип и местоположение участвующих в проведении операций посредников.

Важными компонентами противодействия ОД/ФТ в сфере ЦВЦБ являются идентификация клиента и выявление источника происхождения средств, а также обеспечение координации и взаимодействия между центральными банками – эмитентами ЦВЦБ.

В связи с этим центральные банки стран Группы 20 призываются к тесному сотрудничеству с начальных этапов исследования и проектирования ЦВЦБ, чтобы обеспечивать их функциональную совместимость и своевременно принимать решения об их трансграничной доступности.

Источник информации: официальный сайт Банка международных расчетов в сети Интернет.

Новости европейских стран

13 июля 2022 года опубликован доклад Полицией службы Европейского союза (Европол) об анализе текущего положения и трендов террористической активности в Европейском союзе¹⁵.

В докладе содержится описание ключевых событий и тенденций, связанных с террористической активностью в Европейском союзе, с подкрепляющими его количественными показателями.

Так, в 2021 году в Европейском союзе было зафиксировано 15 произошедших и предотвращенных террористических актов; национальными правоохранительными органами стран ЕС арестованы

¹⁴ Opinions for access to and interoperability of CBDCs for cross-border payments. Report to the G20, July 2022.

¹⁵ European Union Terrorism Situation and Trend Report, 2022.

388 подозреваемых в совершении преступлений террористической направленности.

В докладе отмечается возросшая среди террористических групп и связанных с ними лиц популярность краудфандинговых платформ, криптовалютных бирж и иных финтех-компаний (среди них Amazon Pay, GoFundMe, MoneyGram, YouTube, Patreon, Paypal, Wise и Western Union), используемых для целей сбора и перемещения денежных средств.

В 2021 году краудфандинговые платформы в сети Интернет стали для террористических организаций основным инструментом для сбора денежных средств, в то время как иные финтех-компании использовались преимущественно для целей финансирования пропаганды террористической деятельности.

Источник информации: официальный сайт Европола в сети Интернет.

18 июля 2022 года опубликована информация о применении Банком Нидерландов (De Nederlandsche Bank, DNB) к крупнейшему в мире провайдеру услуг в сфере виртуальных активов Binance ¹⁶ штрафных санкций за нарушения нидерландского законодательства в сфере ПОД/ФТ.

Законодательством Нидерландов для целей выполнения требований Пятой Директивой ЕС по ПОД/ФТ (5AMLD)¹⁷ предусмотрена обязательная регистрация ПУВА, осуществляющих свою деятельность на территории страны¹⁸.

Сумма штрафа, применённого к Binance за неисполнение указанного требования в течение продолжительного времени, составила 3,3 млн евро (около 202 млн рублей в эквиваленте).

Источник информации: официальный сайт DNB в сети Интернет.

27 июля 2022 года опубликована информация об использовании финансовыми организациями и провайдерами финансовых услуг платформ по обмену информацией в целях повышения эффективности выявления случаев ОД и других финансовых преступлений.

¹⁶ *Binance* – ведущая мировая блокчейн-экосистема и поставщик инфраструктуры для криптовалютной отрасли с комплексом финансовых продуктов, который включает в себя крупнейшую по объёму биржу торговли цифровыми активами, рыночная капитализация которой в 2021 году достигла более 100 млрд долларов США.

¹⁷ Директива (ЕС) № 2018/843 Европейского Парламента и Совета ЕС о внесении изменений в Директиву (ЕС) № 2015/849 Европейского Парламента и Совета ЕС о предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма и Директивы (ЕС) № 2009/138/ЕС и № 213/36/ЕС.

¹⁸ К настоящему моменту в Нидерландах зарегистрировано около 30 ПУВА, каждый из которых выплачивает комиссию за осуществление надзора за ними в размере 100 тыс. евро в год.

По результатам исследования, проведённого в рамках программы «Перспективы обмена данными финансовой разведки» (Future of Financial Intelligence Sharing, FFIS) британского Королевского объединённого института по исследованию вопросов безопасности и обороны (RUSI)¹⁹, отмечается, что в ряде стран, в том числе США, Великобритании, Нидерландах и Эстонии, функционируют как минимум 15 платформ по обмену информацией, что существенно повысило эффективность выявления преступлений в указанных странах.

Действующие в разных странах платформы по обмену информацией различаются: одни платформы предназначены исключительно для обмена информацией по конкретной проблематике (например, связанной с «денежными мулами»²⁰), другие – предоставляют банкам-участникам только возможности обмена данными с использованием безопасных каналов связи; ряд платформ позволяет субъектам исполнения «противолегализационного» законодательства выполнять его требования посредством применения новейших технологий.

Так, например, платформа мониторинга операций (Transaction Monitoring Netherlands, TMNL), запущенная в 2020 году пятью крупнейшими нидерландскими банками, позволяет с помощью искусственного интеллекта и других новейших технологий эффективно выявлять подозрительные и необычные операции по перечислению денежных средств клиентами банков. Специальные технологии повышения конфиденциальности данных²¹ позволяют платформе TMNL генерировать сигналы о таких операциях²² на основании информации, полученной из пула обезличенных данных, не раскрывая личности клиентов банков, участвующих в их проведении.

К настоящему моменту в США создано и функционирует несколько платформ по обмену данными между финансовыми организациями и провайдерами финансовых услуг. Например, американской компанией-разработчиком программного обеспечения Verafin Inc., был создан портал для передачи и обработки сообщений, с помощью которого около 2,5 тыс. банков-пользователей могут направлять друг другу информационные запросы.

¹⁹ Royal United Services Institute for Defence and Security Studies.

²⁰ «Денежные мулы» (*money mules*) – физические лица, завербованные преступными организациями в качестве посредников в ОД и использующие свои банковские счета для получения и перевода доходов, полученных преступным путём, преимущественно в другие страны. Как правило, в качестве «денежных мулов» преступники вербуют жителей стран с неблагоприятной финансовой ситуацией, студентов и граждан с низкими доходами.

²¹ Privacy enhancing technologies.

²² К настоящему моменту платформой TMNL было сгенерировано около 2 тыс. сигналов, которые были направлены соответствующим банкам для проведения дальнейших расследований.

В заключение отмечается, что для большинства стран одним из ключевых препятствий для более широкого применения таких платформ являются проблемы, связанные с защитой конфиденциальности данных.

Источник информации: информационный портал The Wall Street Journal.

Новости других регионов

14 июля 2022 года опубликовано исследование американской аналитической компании Chainalysis²³, посвящённое проблематике ОД с помощью «микшеров»²⁴ в 2022 году.

На основе анализа движения виртуальных активов (ВА) специалистами-аналитиками Chainalysis было установлено, что примерно 10% всех средств, переводимых с кошельков ВА, принадлежащих киберпреступникам, переводятся исключительно в «микшеры» с конечной целью их легализации. В 2022 году ежемесячный объём средств, полученных преступным путём и проходящих через «микшеры» для анонимизации, удвоился и достиг 51,8 млн долларов США. Согласно анализу данных за второй квартал 2022 года, источниками происхождения большинства поступающих в «микшеры» средств являются мошенничество в сети Интернет и фишинговые атаки.

При этом в исследовании отмечается, что, несмотря на частоту использования «микшеров» с целью легализации доходов, полученных преступным путём, по своей изначальной природе «микшеры» не являются незаконными, а операторы таких сервисов подлежат лицензированию и регулированию как ПУВА. Кроме того, в исследовании подробно описываются механизмы работы трёх основных категорий

²³ Chainalysis является крупнейшей крипто-аналитической компанией США и предоставляет государственным учреждениям и правоохранительным органам инструменты отслеживания операций в блокчейне, а также помогает криптобиржам выявлять злоумышленников.

²⁴ Сервисы, предназначенные для сокрытия IP-адресов, с которых осуществляются операции с ВА, и содействия обеспечения анонимности. В результате применения таких сервисов установить связь между ВА и конкретными операциями оказывается практически невозможно.

«микшеров»²⁵, а также ключевой уязвимости, связанной с их использованием в преступных целях²⁶.

Источник информации: официальный сайт Chainalysis в сети Интернет.

18 июля 2022 года опубликована информация о применении Народным банком Китая штрафных санкций к оператору цифровых платежей DiDi²⁷ за нарушения требований законодательства в сфере ПОД/ФТ.

По итогам проверки, проведённой Народным банком Китая, в деятельности DiDi были установлены следующие нарушения «противолегализационного» законодательства: (i) проведение сомнительных операций; (ii) несвоевременное информирование компетентного органа о высокорисковых с точки зрения ОД/ФТ операциях.

Сумма штрафа для DiDi составила около 4,3 млн китайских юаней (около 39 млн рублей в эквиваленте).

Одновременно сообщается, что китайским надзорным органом в сфере кибербезопасности (Cyberspace Administration of China, CAC) в

²⁵ Большинство «микшеров» можно отнести к одной из следующих категорий: 1) *Централизованные «микшеры»* представляют собой компании, которые за определённую плату получают криптовалюту пользователя и отправляют аналогичную сумму в другой криптовалюте на адрес, заранее указанный таким пользователем. Подобные «микшеры» не обеспечивают полную конфиденциальность, при необходимости правоохранительные органы могут запросить у таких сервисов любые пользовательские данные. Обычно централизованные «микшеры» требуют регистрацию и верификацию личности. 2) *CoinJoin* – это технология для анонимизации транзакций биткоина, предложенная разработчиком Грегори Максвеллом в 2013 г., которая работает по принципу микширования, объединяя несколько переводов в одну транзакцию с большим количеством выходов. При использовании CoinJoin несколько пользователей группируют свои транзакции в одну. Выходы общей транзакции перемешиваются, из-за чего становится невозможным отследить кому и от кого предназначался каждый конкретный платёж. CoinJoin не предоставляет полной анонимности, так как отправители и получатели всё равно будут отображены в блокчейне. 3) *«Микшеры» смарт-контрактов* предлагают другую систему перемешивания криптовалют. Такими сервисами используются различные смарт-контракты для «запутывания» транзакций. По сути подобные сервисы позволяют случайным пользователям объединить свою криптовалюту, а затем перераспределить её таким образом, чтобы каждый участник получил ту же сумму, но в другой криптовалюте. Работают подобные сервисы следующим образом: (i) пользователь вносит свою криптовалюту в пул смарт-контрактов микшера; (ii) монеты (криптовалюта) перемешиваются с активами других участников в смарт-контракте; (iii) уже с другого кошелька пользователь, которые перемешивал свои средства, отправляет запрос на их получение. Для подтверждения права на монеты (криптовалюту) сервисами используются различные методы криптографии; (iv) пользователь получает такую же сумму средств, но в другой криптовалюте.

²⁶ Проведение крупных транзакций делают процесс легализации через «микшеры» неэффективным. Это связано с тем, что в основе работы «микшеров» лежит механизм перемешивания средств, внесённых разными пользователями. Таким образом, попытка использования «микшеров» для целей легализации одним лицом крупной суммы денежных средств в конечном итоге приведёт к тому, что такое лицо получит ВА, которые оно же изначально и внесло, что позволит отследить средства до их первоначального источника.

²⁷ Финансовая организация, входящая в состав одноимённого китайского конгломерата DiDi, предоставляющего транспортные услуги, в том числе услуги агрегатора такси, каршеринга и райдшеринга.

отношении головной компании DiDi в связи с выявленными в её деятельности серьёзными нарушениями в сфере обеспечения кибербезопасности и защиты персональных данных применены штрафные санкции на сумму более 8 млрд китайских юаней (около 73 млрд рублей в эквиваленте).

Источник информации: информационное агентство Thomson Reuters.