МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

АЛМАТИНСКАЯ АКАДЕМИЯ
ИМЕНИ МАКАНА ЕСБУЛАТОВА

ПРОТИВОДЕЙСТВИИ ОТМЫВАНИЮ ДОХОДОВ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА В УСЛОВИЯХ ЦИФРОВОГО РАЗВИТИЯ РЕСПУБЛИКИ КАЗАХСТАН

Методические рекомендации

Алматы
2024

Обсуждено и одобрено на заседании научно-методическом совете Алматинской академии МВД Республики Казахстан им. М. Есбулатова (протокол №8 от «17» октябрь 2024 года)

Рецензенты:

Бимолданов Е.М. – заместитель начальника Алматинской академии МВД Республики Казахстан, к.ю.н., ассоциированный профессор, полковник полиции

Абикулов Д.Е. – заместитель начальника Управления по противодействию экстремизма Департамента полиции по г. Алматы подполковник полиции

Разуев Д.А., Нарбаев Б.М., Еркенов Б.Д., Кабылбекова А.С. Противодействие отмыванию доходов и финансированию терроризма в условиях цифрового развития Республики Казахстан. / Методические рекомендации. – Алматы: ООНИиРИР Алматинской академии МВД Республики Казахстан им. М. Есбулатова, 2024. – 64 с.

В методическом рекомендациях рассмотрены основные понятия цифровых активов, их классификация, технологий блокчейн; правовое обеспечение детальности правоохранительных органов при противодействии преступности в условиях цифрового развития. Рекомендации предлагают пути совершенствования организационно-правовых и прикладных мер, направленных на противодействие в сфере использования цифровых активов и блокчейн технологий.

Методические рекомендации предназначены для использования как в практической деятельности органов внутренних дел, так и в учебном процессе при изучении правоохранительной деятельности.

© Алматинская академия МВД
Республики Казахстан
им. М. Есбулатова, 2024

Введение

Отмывание доходов и финансирование терроризма (ОД/ФТ) два неразрывных понятия, поскольку международные нормы и национальное законодательство рассматривают их в одном контексте.

Таким образом, настоящие методические рекомендации составлены в рамках темы отмывания доходов и финансирования терроризма.

Отмывание доходов и финансирование терроризма – глобальная угроза, представляющая серьезную опасность для международной безопасности, стабильности и процветания. Терроризм, как известно, использует различные средства для достижения своих целей, включая насилие, запугивание и подрывную деятельность. Финансовые ресурсы, необходимые для реализации этих действий, зачастую добываются незаконными способами, такими как отмывание денег, контрабанда, мошенничество и другие виды криминальной деятельности.

В последние годы цифровизация общества и стремительное развитие технологий существенно изменили ландшафт финансовых преступлений, включая ФТ. Киберпреступность, криптовалюты, онлайн-платформы и другие цифровые инструменты стали для террористов мощными средствами для привлечения и перевода средств, затрудняя при этом традиционные методы противодействия.

Актуальность темы

– тема противодействия отмыванию доходов и финансированию терроризма в условиях цифрового развития преступности приобретает особую актуальность по нескольким причинам:

– усиление масштабов угрозы: Цифровые инструменты позволяют террористическим организациям действовать более эффективно и анонимно, что увеличивает масштабы угрозы.

– сложность выявления и пресечения ОД/ФТ: Цифровые технологии позволяют террористам легко маскировать происхождение и траекторию финансовых потоков, затрудняя их выявление и пресечение.

– необходимость международного сотрудничества: в условиях трансграничной природы цифрового пространства борьба с ОД/ФТ требует тесной координации и сотрудничества между различными странами и международными организациями.

Цель исследования

Целью настоящего исследования является анализ современных тенденций и вызовов, связанных с использованием цифровых технологий в сфере отмывания доходов и финансирования терроризма, а также разработка рекомендаций по эффективному противодействию этой угрозе.

Задачи исследования

– рассмотреть современные тенденции в сфере отмывания доходов и финансирования терроризма с использованием цифровых технологий.

– проанализировать основные методы и инструменты, используемые террористическими организациями для привлечения и перевода финансовых средств.

– изучить слабые места традиционных систем противодействия ФТ в условиях цифрового развития преступности.

– предложить новые подходы и инструменты для борьбы с ФТ, адаптированные к современным реалиям.

– разработать рекомендации для государственных органов, финансовых институтов и международных организаций по укреплению мер противодействия финансированию терроризма.

Методы исследования

В исследовании будут использоваться следующие методы:

– анализ научной литературы и документации: Изучение существующих исследований, отчетов международных организаций и законодательных актов, посвященных ОД/ ФТ.

– сбор и анализ данных: Изучение данных о практических случаях ОД/ФТ с использованием цифровых технологий.

Данное исследование призвано внести вклад в повышение осведомленности о проблеме финансирования терроризма в условиях цифрового развития преступности, а также разработать практические рекомендации по укреплению мер противодействия этой угрозе. Результаты исследования могут быть полезны для государственных органов, правоохранительных структур, финансовых институтов и международных организаций, занимающихся борьбой с терроризмом.

В данной работе будут подробно рассмотрены следующие темы:

Цифровые технологии, используемые для финансирования терроризма: криптовалюты, онлайн-платформы, платежные системы, интернет-магазины и т.д.

Методы привлечения средств: мошенничество, отмывание денег, контрабанда, торговля оружием, похищение людей, сбор пожертвований и т.д.

Методы перевода средств: электронные кошельки, криптовалютные биржи, платежные системы, онлайн-платформы, анонимные сети и т.д.

Проблемы для правоохранительных органов: анонимность, трансграничный характер, сложность отслеживания финансовых потоков.

Рекомендации по противодействию ФТ: усиление международного сотрудничества, создание специальных подразделений по борьбе с киберпреступностью, развитие законодательной базы, повышение уровня осведомленности, совершенствование механизмов финансового мониторинга, создание единых баз данных, обучение сотрудников правоохранительных органов.

Данная работа представляет собой комплексный анализ проблемы финансирования терроризма в условиях цифрового развития преступности и предлагает практические решения для ее решения. Она является актуальной и востребованной, учитывая растущую угрозу со стороны террористических организаций, использующих современные технологии для финансирования своих действий.

Тема 1. Современные тенденции и вызовы в сфере отмывания доходов и финансирования терроризма с использованием цифровых технологий

1.1. Понятие, сущность, классификация криптовалют

Криптовали́та – разновидность цифровой валюты, учёт внутренних расчётных единиц которой обеспечивает децентрализованная платёжная система (нет внутреннего или внешнего администратора, или какого-либо его аналога) [1][2], работающая в полностью автоматическом режиме. Сама по себе криптовалюта не имеет какой-либо особой материальной или электронной формы – это просто число, обозначающее количество данных расчётных единиц, которое записывается в соответствующей позиции информационного пакета протокола передачи данных и зачастую даже не подвергается шифрованию, как и вся иная информация о транзакциях между адресами системы.

Термин криптовалюта закрепился после публикации статьи о системе Биткойн «Crypto currency» (Криптографическая валюта), опубликованной в 2011 году в журнале Forbes [3]. При этом и создатель биткойна, и многие другие авторы использовали термин «электронная наличность» (англ. electronic cash).

Внутренняя игровая валюта (виртуальная валюта) создавалась как часть виртуального мира игры, в которой есть какая-либо внутренняя экономическая составляющая.

Важнейшее отличие (как и любой другой виртуальной валюты) от иных форм денег в том, что она хранится в памяти ЭВМ (будь то персональный компьютер, мобильный телефон, планшетный компьютер и т.п.) в виде кода. Обращаем внимание, что это не код доступа к наличным банкнотам, находящимся в кредитной организации, а сами деньги в виде компьютерного файла. В этой связи они схожи с наличными деньгами в кошельке. Их можно передать на любое устройство, называемое электронным кошельком, через флешку или посредством электронной связи, при этом какой-либо наличный эквивалент у криптовалюты отсутствует. Поскольку при использовании криптовалюты платеж осуществляется без передачи физически осязаемой валюты, то такие деньги следует отнести к разряду безналичных. Кроме того, операции с криптовалютой проводятся при помощи электронных вычислительных машин (ЭВМ) – компьютеров. Широта применения компьютеров в повседневной жизни существенно увеличивает возможности использования криптовалюты и одновременно значительно упрощает ее оборот. Все это вводит некоторых ученых в заблуждение, будто криптовалюта суть то же, что и наличные деньги. На самом деле удобство и широта использования не являются основанием для постановки «тождества» между наличными деньгами и криптовалютой. У виртуальной валюты в целом и криптовалюты в частности есть существенное отличие от наличных денег – у нее изменчивая сущность. В то время как наличная оплата имеет постоянную сущность в виде защищенной бумаги определенного размера, цвета, с символами определенного шрифта и даже нумерацией, что в совокупности является доказательством ее ценности, то сущность криптовалюты непостоянна: она бывает ячейкой в памяти компьютерной системы, сигналом, передаваемым от ЭВМ к ЭВМ, рисунком на экране компьютера или телефона, оформленным любым знаком, любым символом и даже в эквиваленте наличной валюты. В этой же связи стоит отметить, что виртуальная валюта

способна к мгновенной конвертации, к примеру, одни и те же «Биткоины» могут выразиться в рублях, потом конвертироваться в фунты, евро, марки, юани и обратно в электронные деньги без потери стоимости, в то время как для полной конвертации наличных денег придется осуществлять банковские обменные операции.

Ее можно **классифицировать:** по форме выражения: на конвертируемые и неконвертируемые; а также – на фиатные и нефиатные; по устройству системы: закрыто циркулирующие и открыто циркулирующие системы; по способу эмиссии и управления: централизованные и децентрализованные. Отсюда следует, что криптовалюта представляет собой конвертируемую нефиатную децентрализованную виртуальную валюту на базе открыто циркулирующей системы, защищенной криптографическим шифрованием. Криптовалюта – это товар, генерируемый и управляемый при помощи ЭВМ с использованием криптографического шифрования, применяемый в качестве безналичной меры стоимости, средства накопления, платежа и обращения и заключающийся в информации о своей ценности [4].

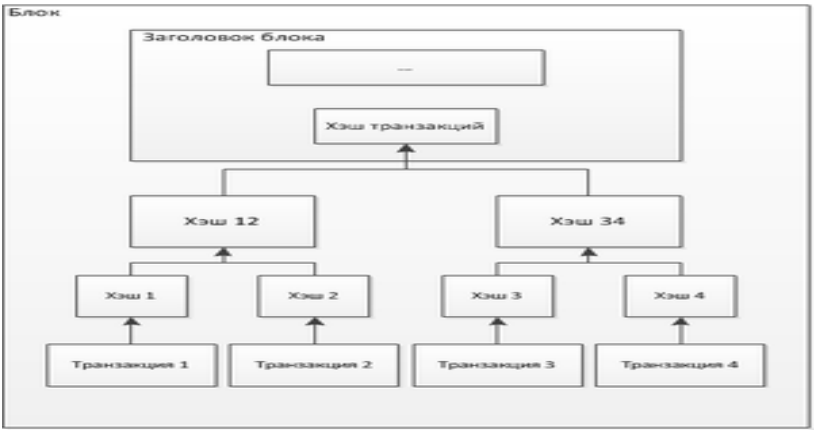
1.2. Виды и принципы работы технологии блокчейн

Блокче́йн (англ. *blockchain* – цепь из блоков) – выстроенная по определённым правилам непрерывная последовательная цепочка блоков *(связный список)*, содержащих какую-либо информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму *(результат обработки данных хэш-функцией)* и хеш-сумму предыдущего блока *(см. рисунок №1)*. Изменение любой информации в блоке изменит его хеш-сумму. Чтобы соответствовать правилам построения цепочки, изменения хеш-суммы нужно будет записать в следующий блок, что вызовет изменения уже его собственной хеш-суммы. При этом предыдущие блоки не затрагиваются.

Если изменяемый блок последний в цепочке, то внесение изменений может не потребовать существенных усилий. Но если после изменяемого блока уже сформировано продолжение, то изменение может оказаться крайне трудоёмким процессом. Дело в том, что обычно копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга [5].

Впервые термин появился как название полностью реплицированной распределённой базы данных, реализованной в системе «Биткойн», из-за чего блокчейн часто отождествляют с реестром транзакций в различных криптовалютах. Однако технология цепочек блоков может быть распространена на любые взаимосвязанные информационные блоки[4]. Появившаяся в октябре 2008 года система Биткойн стала первым применением технологии блокчейн [6].

Рисунок №1



Виды блокчейн:

Блок транзакций

Блок транзакций – специальная структура для записи группы транзакций в системе Биткойн и аналогичных ей [7]. Транзакция считается завершённой и достоверной («подтверждённой»), когда проверены её формат и подписи, и ко-

гда сама транзакция объединена в группу с несколькими другими и записана в специальную структуру – блок. Содержимое блоков может быть проверено, так как каждый блок содержит информацию о предыдущем блоке. Все блоки выстроены в одну цепочку, которая содержит информацию обо всех совершённых когда-либо операциях в базе. Самый первый блок в цепочке – первичный блок (англ. genesis block) – рассматривается как отдельный случай, так как у него отсутствует родительский блок [8].

Блок состоит из заголовка и списка транзакций. Заголовок блока включает в себя свой хеш, хеш предыдущего блока, хеши транзакций и дополнительную служебную информацию. В системе Биткойн первой транзакцией в блоке всегда указывается получение комиссии, которая станет наградой майнеру за созданный блок. Далее идёт список транзакций, сформированный из очереди транзакций, ещё не записанных в предыдущие блоки. Критерий отбора из очереди задаёт майнер самостоятельно. Это не обязательно должна быть хронология по времени.

Например, могут включаться только операции с высокой комиссией или с участием заданного списка адресов. Для транзакций в блоке используется древовидное хеширование [7], аналогичное формированию хеш-суммы для файла в протоколе BitTorrent.

Величина целевого числа, с которым сравнивается хеш, в системе Биткойн корректируется через каждые 2016 блоков. Запланировано, что вся сеть системы Биткойн должна тратить на генерацию одного блока примерно 10 минут, на 2016 блоков – около двух недель. Если 2016 блоков сформированы быстрее, то целевое число немного уменьшается и получить удовлетворяющий ему хеш подбором параметра nonce становится труднее, в противном случае целевое число увеличивается. Изменение сложности вычислений не влияет на надёжность сети Биткойн и требуется лишь для того, чтобы система генерировала блоки почти с постоянной скоро-

стью, не зависящей от вычислительной мощности участников сети [9].

Цепочка блоков

Блоки одновременно формируются множеством «майнеров». Удовлетворяющие критериям блоки отправляются в сеть, включаясь во все репликации распределённой базы блоков. Регулярно возникают ситуации, когда несколько новых блоков в разных частях распределённой сети называют предыдущим один и тот же блок, то есть цепочка блоков может ветвиться. Специально или случайно можно ограничить ретрансляцию информации о новых блоках (например, одна из цепочек может развиваться в рамках локальной сети).

В этом случае возможно параллельное наращивание различных ветвей. В каждом из новых блоков могут встречаться как одинаковые транзакции, так и разные, вошедшие только в один из них. Когда ретрансляция блоков возобновляется, майнеры начинают считать главной цепочку с учётом уровня сложности хеша и длины цепочки. При равенстве сложности и длины предпочтение отдаётся той цепочке, конечный блок которой появился раньше.

Таким образом, цепочка блоков содержит историю владения, с которой можно ознакомиться, например, на специализированных сайтах [10].

Блокчейн формируется как непрерывно растущая цепочка блоков с записями обо всех транзакциях. Копии базы или её части одновременно хранятся на множестве компьютеров и синхронизируются согласно формальным правилам построения цепочки блоков. Информация в блоках не шифрована и доступна в открытом виде, но отсутствие изменений удостоверяется криптографически через хеш-цепочки [7] (*элемент цифровой подписи*).

База публично хранит в незашифрованном виде информацию обо всех транзакциях, подписываемых с помощью асимметричного шифрования. Для предотвращения многократной траты одной и той же суммы используются метки

времени [7], реализованные путём разбиения БД на цепочку специальных блоков, каждый из которых, в числе прочего, содержит в себе хеш предыдущего блока и свой порядковый номер. Каждый новый блок осуществляет подтверждение транзакций, информацию о которых содержит и дополнительное подтверждение транзакций во всех предыдущих блоках цепочки. Изменять информацию в блоке, который находится в цепи, не практично, так как в таком случае пришлось бы редактировать информацию во всех последующих блоках. Благодаря этому успешная double-spending атака (повторная трата ранее израсходованных средств) на практике крайне маловероятна [11].

Публичные блокчейны

Публичные блокчейны общедоступны. Любой может читать блоки, отправлять в них информацию и участвовать в механизме консенсуса. При этом пользователи могут оставаться анонимными. Такие блокчейны обычно полностью децентрализованы, то есть не имеют администраторов или центров доверия. Неизменность и целостность информации обеспечивают экономические стимулы и криптографические проверки с использованием таких механизмов, как доказательство выполнения работы или доказательство доли владения.

Публичные блокчейны обычно имеют существенные ограничения в объёме и скорости размещения данных в блоках.

Пользователи публичных блокчейнов во многом защищены от произвола разработчиков: разработчики изначально отказались от действий без согласования с представителями пользователей. С одной стороны, это увеличивает уверенность, что программа не будет иметь скрытых от пользователей функций. С другой стороны, при давлении со стороны государственных органов разработчики искренне могут говорить, что у них нет полномочий сделать это, даже если бы они хотели. При этом изменения в работе сети могут стать проблемой, поскольку не менее половины участников долж-

ны согласиться с нововведениями, но и это не защищает от разделения блокчейна на параллельные проекты, поддерживающие разные протоколы.

Большинство криптовалют используют публичные блокчейны [12].

Частные блокчейны

В частных блокчейнах правом записи информации обладает только один участник или узлы, уполномоченные этим единственным администратором. Это централизованные персонифицированные системы, поскольку существует иерархия полномочий. Сбои можно быстро исправить вручную. Нет смысла применять доказательство выполнения работы или доказательство доли владения – информация без задержки попадает в блоки, формируемые по мере необходимости, и не требует дополнительного подтверждения, что максимизирует скорость работы сети и минимизирует стоимость транзакций.

В частном блокчейне легко реализуются не только изменения правил, но и отмены транзакции, изменения информации и т.д. Это необходимо, например, в земельных кадастрах – без возможности исправить ошибки подобные системы могут стать неуправляемыми и утратить легитимность [12].

Если узлы начинают действовать злонамеренно, это легко обнаружить и заблокировать им доступ к сети.

Консорциумные блокчейны

В консорциумных блокчейнах процесс согласования обеспечивается несколькими заранее оговорёнными равноправными узлами. Например, консорциум из 15 банков договаривается считать действительным блок с мультиподписью не менее 10 участников консорциума. Скорость появления новых блоков может быть весьма высокой. При этом участники концерна доступ к информации из блокчейна могут сделать как общедоступным, так и ограничить избранным кругом или ввести иные количественные, содержательные

или временны́е ограничения. Эти блокчейны можно считать «частично децентрализованными».

Ограниченное количество доверенных узлов позволяет модернизировать систему гораздо проще, чем при публичном блокчейне. Но работа такой сети возможна только при условии, что основная часть узлов работает добросовестно [12].

1.3 Виды криптовалют, их основные отличия

В 2008 году Сатоши Накамото представил концепцию децентрализованной цифровой валюты, не зависящей от центральных банков или государственных институтов. Это стало революционным шагом в финансовой индустрии. Виталик Бутерин продолжил путь инноваций и в 2015 году представил миру Ethereum – криптовалюту и платформу для создания децентрализованных приложений (dapp) на базе смарт-контрактов. Благодаря Ethereum и внедрению стандарта ERC-20, в мире криптовалют появилось множество новых типов токенов, каждый из которых служит различным целям в рамках блокчейн-экосистемы. С тех пор Ethereum занимает второе место по величине рыночной капитализации среди криптовалют.

Биткоин

В ответ на финансовый кризис 2007-2008 годов, Сатоши Накамото предложил Bitcoin как децентрализованную цифровую валюту. Эта валюта защищена от государственного вмешательства и манипуляций благодаря использованию криптографии, что обеспечивает прозрачность и равенство всех участников сети. Благодаря структу-

ре, основанной на принципе peer-to-peer (P2P), Bitcoin позволяет осуществлять транзакции напрямую между пользователями, минуя финансовых посредников. Инновационный подход, заложенный в Bitcoin, положил начало появлению новых криптовалют.

Альткоины

Альткоины – это криптовалюты, появившиеся после Биткоина, предназначенные для расширения его возможностей и предложения новых инноваций. Они могут отличаться от Bitcoin множеством параметров: от скорости транзакций до используемых алгоритмов консенсуса, таких как Proof of Work (PoW) или Proof of Stake (PoS).

Примеры известных альткоинов:

Ethereum (ETH): занимает первое место среди самых популярных и широко используемых альткоинов. Ethereum – это децентрализованная платформа, которая позволяет создавать и запускать смарт-контракты и децентрализованные приложения (dapps), обеспечивая их работу без риска цензуры, мошенничества или любого вмешательства третьих сторон;

Ripple (XRP): Ripple представляет собой как технологию платежной системы, так и криптовалюту, разработанные с целью ускорения и снижения стоимости международных платежей. В отличие от большинства других криптовалют, Ripple активно сотрудничает с традиционными финансовыми институтами, предоставляя им быстрое и эффективное средство для осуществления международных переводов;

Litecoin (LTC): если биткоин называют «цифровым золотом», то Litecoin «серебром». Litecoin является одним из первых альткоинов, созданных на основе кода Bitcoin с из-

менениями, направленными на ускорение времени обработки блоков.

Токены

Многие путают токены с монетами, считая их синонимами. Однако, несмотря на сходство, существуют фундаментальные отличия между этими двумя понятиями. Монеты или коины функционируют на собственных блокчейнах, в то время как токены создаются на базе существующих.

Например, Ethereum – это монета, которая работает на своем блокчейне, а ARB – ERC-20 токен на блокчейне Ethereum. Для глубокого понимания различий между монетами и токенами важно учитывать не только их техническое строение и платформу, но и экономическую, функциональную и юридическую роль в криптовалютной экосистеме.

Монеты обычно служат средством обмена, единицей счета и средством сохранения стоимости в рамках своих блокчейнов. Они являются фундаментом для выполнения транзакций и взаимодействия пользователей внутри сети. В отличие от монет, токены могут выполнять более специализированные функции, такие как представление активов, прав на участие в проектах или доступ к определенным услугам.

Стейблкоины

Стейблкоины – это тип криптовалюты, стоимость которой закреплена за стоимостью другого актива, такого как фиатные деньги, драгоценные металлы или ценные бумаги, в соотношении один к одному. Эти токены помогают трейдерам быстро переводить активы в стабильную валюту в периоды рыночной волатильности. Крипто графики стейблкоинов отражают их стабильность, поэтому у предпринимателей есть возможность вести взаиморасчеты с устойчивым курсом без участия банков. В отличие от фиатных валют, стейблкоины можно быстро и выгодно отправлять и получать в любой точке мира. USDT и USDC – самые популярные стейблкоины. Капитализация одного лишь USDT равна 98 млрд долларов США.

Токены безопасности

Security-токены служат цифровым представлением традиционных финансовых инструментов в блокчейне, таких, как доли в компании, акции и облигации. Эти токены фактически выступают в роли ценных бумаг в цифровом формате. Их выпуск подчиняется строгому регулированию, обеспечивая соответствие законодательству о ценных бумагах, что повышает доверие и безопасность для инвесторов. Благодаря использованию блокчейн-технологий, управление этими активами становится более прозрачным и эффективным, минимизируя бюрократию и предоставляя инвесторам улучшенный доступ к глобальным рынкам и повышенную ликвидность инвестиций. Процесс первичного предложения этих токенов, называется Security Token Offering (STO).

Служебные токены

Служебные или Utilit-токены предоставляют пользователям доступ к определенным услугам или функциям внутри блокчейн-проекта или платформы. В отличие от токенов безопасности, которые функционируют как инвестиционные инструменты и предоставляют права на долю в прибыли или управлении, служебные токены несут в себе практическую ценность, позволяя взаимодействовать с сервисами или приложениями.

Применение служебных токенов может охватывать различные аспекты, включая оплату доступа к сетевым ресурсам, использование специфических функций платформы – например, голосование или запуск смарт-контрактов – а также служить внутренней валютой для осуществления транзакций в пределах экосистемы. Служебные токены стимулируют экономическую активность внутри проекта, способствуя его поддержке и развитию. Один из примеров служебного токена – Filecoin (FIL), используется для покупки места для хранения данных или вознаграждения за предоставление доступного дискового пространства.

Токены управления

Токены управления предоставляют их владельцам уникальную возможность активно участвовать в управлении блокчейн-проектами. Это включает в себя право голоса при принятии ключевых решений, внос предложений по развитию и модификации проектов, а также участие в обсуждении новых инициатив. Такой механизм позволяет создать полностью децентрализованные и самоуправляемые экосистемы, где решения принимаются коллективно, а не централизованно.

Токены управления находят особенно широкое применение в сферах децентрализованных финансов и игровых платформах, известных как GameFi.

NFT (non-fungible token), или невзаимозаменяемый токен – это уникальный цифровой актив, созданный на основе технологии блокчейн. Отличительной чертой NFT является его уникальность. В отличие от взаимозаменяемых токенов, таких, как биткоин или эфириум, его, невозможно разделить и продать по частям. NFT создают через смарт-контракты на различных блокчейн-платформах, включая Ethereum, Solana, NEAR, Polkadot и многие другие. Каждая NFT содержит не только блокчейн информацию, но и метаданные: медиафайл, описание, Content ID и json. Это делает невозможным дублирование или подделку токена.

Приватные монеты

Приватные монеты, такие как Monero (XMR), предназначены для обеспечения анонимности и конфиденциальности транзакций. Monero использует сложные криптографические методы, включая подписи кольца и скрытые адреса, чтобы скрыть идентификаторы отправителя и получателя, а

также суммы транзакций. Это делает Monero идеальным выбором для пользователей, которые ценят приватность своих финансовых операций выше всего. В отличие от многих других криптовалют, где транзакции могут быть отслежены и просмотрены публично, Monero обеспечивает высокий уровень анонимности, делая практически невозможным отслеживание потоков средств внутри сети.

Цифровые валюты центрального банка (CBDC)

Цифровые валюты центрального банка представляют собой цифровой аналог фиатных валют, выпускаемый и регулируемый центральными банками стран. В отличие от децентрализованных криптовалют, CBDCs находятся под полным контролем национальных финансовых институтов, что обеспечивает их стабильность и официальное признание как законного платежного средства. Эти валюты предлагают преимущества, включая улучшение эффективности платежных систем и борьбу с отмыванием денег.

Примеры CBDC, такие, как цифровой юань в Китае и цифровой евро от Европейского Центрального Банка, демонстрируют стремление интегрировать цифровые валюты в существующую финансовую инфраструктуру, обеспечивая надежность, безопасность и удобство использования. В отличие от криптовалют, цифровые валюты центрального банка обладают стабильностью, поддерживаемой государством, и предоставляют регуляторам возможность для эффективного надзора и контроля транзакций, что делает их менее подверженными рыночным колебаниям и повышает доверие инвесторов.

Монеты и токены децентрализованных финансов (DeFi)

Чтобы понять, как работает DeFi, важно осознать, что DeFi монета – это не просто криптовалюта или токен для спекуляций. Это ключ к активному участию в экосистемах децентрализованных финансов, которые включают в себя децентрализованные биржи, такие как WhiteSwap, пулы лик-

видности, стейкинг, фарминг, кредитование и NFT. Эти инструменты предоставляют пользователям уникальные возможности для управления своими активами без необходимости обращаться в традиционные финансовые институты. Задумываясь о том, сколько видов криптовалют в мире, можно оценить масштабы и динамику развития блокчейн-технологий [13].

Глава 2. Современные тенденции и вызовы в сфере финансирования терроризма с использованием цифровых технологий

2.1 Роль криптовалют в отмывании доходов и финансировании терроризма

Развитие криптовалют, таких как Bitcoin, Ethereum и другие, открыло новые возможности для финансирования различных видов деятельности, включая терроризм. Децентрализованная природа криптовалют, анонимность транзакций и отсутствие центрального контроля создают благоприятную среду для террористических организаций, которые могут использовать их для сбора средств, перевода денег и финансирования своих операций [15].

1. Особенности криптовалют, способствующие финансированию терроризма:

– Анонимность: Транзакции с криптовалютами могут быть анонимными, затрудняя отслеживание движения средств.

– Децентрализация: Отсутствие центрального контрольного органа делает криптовалюты менее восприимчивыми к контролю со стороны государств.

– Скорость и удобство: Криптовалюты позволяют быстро и легко переводить деньги по всему миру, минуя традиционную банковскую систему.

– Низкие комиссии: по сравнению с традиционными банковскими переводами, комиссии за операции с криптовалютами значительно ниже [16].

2. Способы использования криптовалют для финансирования терроризма:

– Сбор средств: Террористические организации используют криптовалюты для сбора пожертвований от сторонников.

– Переводы средств: Криптовалюты позволяют террористам быстро и незаметно переводить деньги между своими членами и подразделениями.

– Финансирование операций: Криптовалюты могут использоваться для покупки оружия, взрывчатых веществ и других ресурсов, необходимых для проведения терактов.

– Отмывание денег: Криптовалюты могут использоваться для маскировки происхождения незаконно полученных средств [17].

3. Проблемы борьбы с использованием криптовалют для доходов и финансирования терроризма:

– Отсутствие единого законодательства: не существует единого международного законодательства, регулирующего использование криптовалют, что затрудняет борьбу с их незаконным применением.

– Сложности отслеживания: Анонимность и децентрализация криптовалют делают отслеживание и блокировку транзакций сложной задачей.

– Недостаток ресурсов: Правоохранительные органы и финансовые регуляторы могут испытывать нехватку ресурсов и expertise для борьбы с финансовыми преступлениями, связанными с криптовалютами [18].

4. Решения и меры по противодействию:

– Усиление международного сотрудничества: необходимо разработать международные стандарты и законодательство, регулирующие использование криптовалют и способствующие обмену информацией между правоохранительными органами.

– Разработка инструментов отслеживания: необходимо разрабатывать новые инструменты и технологии, позволяющие отслеживать и блокировать незаконные транзакции с криптовалютами.

– Повышение осведомленности: необходимо повышать осведомленность общественности о рисках, связанных с использованием криптовалют для финансирования терроризма.

– Взаимодействие с криптосообществом: необходимо налаживать сотрудничество с криптосообществом, привлекая его к борьбе с незаконным использованием криптовалют [19].

2.2 Методы отслеживания транзакций с использованием криптовалют

Децентрализованная природа криптовалют, анонимность транзакций и отсутствие центрального контроля создают определенные сложности для отслеживания и анализа их использования. Однако развитие технологий и исследований в этой области позволило создать ряд методов, которые могут помочь в борьбе с незаконным использованием криптовалют, включая отмывание денег, финансирование терроризма и другие финансовые преступления [20].

1. Особенности блокчейна, влияющие на отслеживание транзакций:

– **Прозрачность:** Все транзакции в блокчейне публичны и доступны для просмотра.

– **Неизменяемость:** Информация, записанная в блокчейн, не может быть изменена или удалена.

– **Псевдонимность:** хотя адреса в блокчейне публичны, они не всегда связаны с конкретными лицами [21].

2. Методы отслеживания и анализа транзакций:

– **Анализ графов транзакций:** Изучение связей между адресами в блокчейне с помощью алгоритмов, позволяющих выявлять кластеры и модели активности.

– **Анализ потоков средств:** Отслеживание движения средств между различными адресами, позволяющее определить, где происходят операции по отмыванию денег или финансированию терроризма.

– **Анализ поведения пользователей:** Изучение паттернов активности пользователей, например частоты транзакций, размера транзакций и типа используемых криптовалют.

– **Анализ метаданных:** Изучение информации, связанной с транзакциями, такой как время транзакции, IP-адрес, использованные криптобиржи и другие сервисы.

– **Анализ контрактов:** Изучение смарт-контрактов, используемых в блокчейне, для выявления потенциальных рисков и злоупотреблений [22].

3. Инструменты и технологии для отслеживания:

– **Blockchain Explorer:** Сервисы, позволяющие просматривать информацию о транзакциях в блокчейне.

– **Аналитические платформы:** Платформы, предоставляющие инструменты для анализа транзакций, включая визуализацию графов, кластеризацию и поиск аномалий.

– **Инструменты отслеживания:** Специальные инструменты, которые могут помочь в отслеживании конкретных адресов или транзакций.

– **Машинное обучение:** Применение алгоритмов машинного обучения для анализа больших объемов данных и выявления подозрительных транзакций.

4. Вызовы и ограничения:

– **Сложность анализа:** Объем данных в блокчейне может быть очень большим, а анализ может быть сложным и трудоемким.

– **Псевдонимность:** Трудности в установлении связи между адресами и реальными людьми.

– **Развитие криптотехнологий:** постоянно появляются новые криптовалюты и технологии, что требует постоянного совершенствования методов отслеживания [23].

Отслеживание и анализ транзакций с использованием криптовалют является важной задачей для борьбы с преступлениями. Развитие технологий и алгоритмов открывает новые возможности для выявления и пресечения незаконных действий.

2.3 Законодательство Республики Казахстан и международные стандарты, регулирующие использование криптовалют в контексте противодействия финансированию терроризма

На данном этапе Республикой Казахстан принят ряд организационных и правовых мер по имплементации международных стандартов по регулированию деятельности оборота цифровых активов.

С момента присоединения Казахстана, в 2011 году, к Евразийской группе по противодействию легализации преступных доходов и финансированию терроризма (далее – ЕАГ), являющийся региональным органом по типу Группы разработки финансовых мер борьбы с отмыванием денег (далее – ФАТФ), страной проводилась работа по внедрению международных институтов, а также рекомендаций по вопросам противодействия ОД/ФТ, результатам которого стало успешное завершение процедуры взаимной оценки по противодействию отмыванию преступных доходов и финансированию терроризма, которую страна проходила в течение последних двух лет [24].

Так, в отечественном законодательстве впервые термин «цифровой актив» был закреплен в июне 2020 года [25], а уже в феврале 2023 года официально опубликован Закон «О цифровых активах в Республике Казахстан» [26].

Следует отметить, что согласно Закону Республики Казахстан «Об информатизации» (п. 55-1 ст. 1), «цифровой актив» определяется как имущество, созданное в электронно-цифровой форме с применением средств криптографии и

компьютерных вычислений, не являющееся финансовым инструментом, а также электронно-цифровая форма удостоверения имущественных прав. Также в данном законе (ст. 31-1) установлено, что цифровой актив не является средством платежа. Одним из видов цифрового актива является «цифровой токен», определенный как цифровое средство учета, обмена и удостоверения имущественных прав [27].

Основным же нормативно-правовым актом, регулирующим сферу противодействия ОД/ФТ в Казахстане, является Закон Республики Казахстан «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 1 июля 2016 года [28]. Нормативный акт устанавливает комплекс мер, которые должны осуществляться для предотвращения ОД/ФТ, включая:

– идентификацию и оценку рисков ОД/ФТ;

– должную осмотрительность клиентов;

– мониторинг финансовых операций;

– отчетность об операциях, подлежащих финансовому мониторингу;

– сотрудничество с правоохранительными и другими государственными органами;

– международное сотрудничество.

Следует отметить, что Законом о ПОД/ФТ к субъектам финансового мониторинга также отнесены лица, осуществляющие деятельность по выпуску цифровых активов, организации торгов ими, а также предоставлению услуг по обмену цифровых активов на деньги, ценности и иное имущество.

В рамках установленной правовой основы в Казахстане используются различные правовые инструменты для противодействия ОД/ФТ:

– идентификация и оценка рисков ОД/ФТ: субъекты финансового мониторинга обязаны проводить идентификацию и оценку рисков ОД/ФТ в отношении своих клиентов и операций;

– должная осмотрительность клиентов: субъекты финансового мониторинга обязаны проводить должную осмотрительность клиентов, в том числе изучать происхождение их средств;

– мониторинг финансовых операций: субъекты финансового мониторинга обязаны осуществлять мониторинг финансовых операций своих клиентов с целью выявления подозрительных сделок;

– отчетность об операциях, подлежащих финансовому мониторингу: субъекты финансового мониторинга обязаны представлять в Агентство по финансовому мониторингу (АФМ) отчеты об операциях, подпадающих под определение операций, подлежащих финансовому мониторингу;

– сотрудничество с правоохранительными и другими государственными органами: субъекты финансового мониторинга обязаны сотрудничать с правоохранительными и другими государственными органами в рамках расследований, связанных с ОД/ФТ;

– международное сотрудничество: Казахстан сотрудничает с другими странами в сфере противодействия ОД/ФТ в рамках международных организаций и двусторонних соглашений.

К законодательным актам, устанавливающим основные принципы противодействия терроризму и экстремизму, правовые и организационные основы профилактики терроризму и экстремизму относятся Законы РК:

– О противодействии терроризму [29];

– О противодействии экстремизму [30];

Закон РК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» регулирует процедуры международного взаимодействия уполномоченных органов в сфере противодействия легализации и отмыванию доходов, полученных преступным

путем, и финансированию терроризма, включая розыск и возврат преступных активов. Также содержит нововведения для защиты некоммерческого сектора от использования их в целях финансирования терроризма. Требования применяются к некоммерческим организациям и религиозным объединениям, которые запрашивают добровольные финансовые и другие пожертвования.

Международный опыт

Международной группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ), одним из членов которой с 2011 г. является Республика Казахстан, были подготовлены Специальные Рекомендации по предотвращению финансирования терроризма (далее – Рекомендации). В них предусматривается, что каждой стране следует установить уголовную ответственность за финансирование терроризма, террористических актов и террористических организаций. В соответствии с п. VII Рекомендаций «странам следует обязать финансовые учреждения, в том числе организации, занимающиеся переводом денежных средств, получать точные и достоверные сведения о клиенте (имя, адрес и номер счета) и включать их в состав операции по переводу активов или связанных с указанной операцией передаваемых сообщений, с учетом того, что данные сведения должны сопровождать операцию с указанными средствами на всех этапах» [31].

В последние годы криптовалюты стали популярным инструментом для финансирования различных видов деятельности, включая терроризм. Децентрализованная природа криптовалют, анонимность транзакций и отсутствие центрального контроля создают благоприятную среду для террористических организаций, которые могут использовать их для сбора средств, перевода денег и финансирования своих операций. Это вызвало необходимость разработки международного законодательства, направленного на противодействие финансированию терроризма с использованием криптовалюты.

1. Международные правовые документы:

– Конвенция ООН о борьбе с финансированием терроризма (1999): является основным международным правовым инструментом, устанавливающим обязательства государств по борьбе с финансированием терроризма [32].

– Резолюция Совета Безопасности ООН 1373 (2001): устанавливает обязательства государств по борьбе с финансированием терроризма, в том числе с использованием криптовалют [33].

– Рекомендации ФАТФ (2019): предоставляют руководящие принципы для государств по борьбе с отмыванием денег и финансированием терроризма, включая меры по противодействию использованию криптовалют [31].

2. Проблемы правового регулирования:

Отсутствие единого подхода: отсутствует единый международный стандарт для регулирования криптовалют, что затрудняет создание единой системы противодействия финансированию терроризма с их использованием.

Сложности с идентификацией: Анонимность транзакций с криптовалютами делает сложным идентификацию отправителей и получателей средств.

Отсутствие централизованного контроля: Децентрализация блокчейн-технологии затрудняет контроль и регулирование транзакций.

Развитие новых технологий: Постоянное появление новых криптовалют и технологий представляет вызов для правоприменения [34].

3. Основные подходы к правовому регулированию:

«Знай своего клиента» (KYC): Обязательство криптобирж и других сервисов идентифицировать клиентов и проверять их информацию.

«Проверь свою транзакцию» (KYT): Обязательство криптобирж и других сервисов отслеживать транзакции и выявлять подозрительную активность [35].

Создание специальных подразделений: Создание специализированных подразделений в правоохранительных органах для борьбы с отмывание доходов и финансированием терроризма с использованием криптовалют.

Сотрудничество с криптосообществом: Развитие сотрудничества с криптосообществом для обмена информацией и разработки совместных решений [36].

4. Перспективы развития международного законодательства:

Развитие международных стандартов: необходимо разработать единые международные стандарты для регулирования криптовалют и создания единой системы противодействия финансированию терроризма.

Усиление международного сотрудничества: необходимо усилить международное сотрудничество между государствами для обмена информацией и совместных расследований.

Развитие новых технологий: необходимо разрабатывать новые технологии для отслеживания и анализа транзакций с криптовалютами.

Повышение осведомленности: необходимо повышать осведомленность общественности о рисках, связанных с использованием криптовалют для финансирования терроризма [37].

Международное законодательство в области противодействия финансированию терроризма с использованием криптовалюты находится на этапе формирования. Необходимо продолжать разрабатывать эффективные механизмы контроля и регулирования криптовалют, усиливать международное сотрудничество и повышать осведомленность общественности о рисках, связанных с использованием криптовалют для финансирования терроризма.

Тема 3. Инструменты при расследовании отмывания доходов и финансирования терроризма с использованием криптовалют

3.1 Инструменты анализа транзакций с криптовалютами

Решения для блокчейн-анализа предоставляют полный набор инструментов для мониторинга транзакций, оценки рисков и расследований. Основная идея состоит в том, чтобы связать адреса в блокчейне с реальными личностями или организациями и предоставить инструменты для анализа транзакций в блокчейне.

Ниже перечислены основные функции инструментов для блокчейн-анализа.

Классификация адресов – одним из основных применений ПО для анализа блокчейнов является связывание блокчейн-адресов с реальными личностями или организациями. Без этого все остальные данные не будут иметь смысла, поэтому инструменты такого рода применяют множество различных методов для идентификации реальных акторов в блокчейне**.**

Мониторинг транзакций и анализ рисков – блокчейн-анализ позволяет контролировать каждую транзакцию, имеющую отношение к вашему бизнесу, и оценивать риски исходя из происхождения средств, денежного потока и истории кошельков отправителя или получателя.

Инструменты для исследований и анализа – предоставляют средства визуализации для проведения собственных исследований транзакций и блокчейн-адресов.

Технология анализа блокчейна: под капотом Разобравшись с основными функциями продуктов для блокчейн-анализа, давайте теперь рассмотрим, каким образом эти продукты достигают этой функциональности.

Классификация и идентификация – для определения реальной идентичности блокчейн-адресов, инструменты анализа блокчейнов используют такие методы, как алгоритмы кластеризации, веб-скрейпинг, мониторинг баз данных о мошенничествах и пылевые атаки. Кластеризация – это наиболее распространенный способ, с помощью которого ПО для анализа идентифицирует таких акторов, как биржи, платежные системы, кошельки и т.д.

Анализ рисков осуществляется путем создания специализированных моделей рисков и машинного обучения их с тем, чтобы в результате они рассчитывали коэффициент риска для каждой блокчейн-транзакции. Модели риска основываются на множестве параметров, таких как сумма транзакции, происхождение средств и история денежных потоков.

Инструменты для исследований и анализа представляют собой графический интерфейс для составления графов транзакций с целью обнаружения связей между ними.

Варианты применения и преимущества блокчейн-анализа

Наиболее важным примером применения блокчейн-анализа является регуляторная сфера. Криптобизнесы и прочие финансовые организации используют блокчейн-анализ для снижения рисков и соответствия регуляторным требованиям.

Наблюдение и расследования

Программное обеспечение для анализа блокчейнов играет решающую роль в уголовных расследованиях, связанных с криптовалютами. Это позволяет правоохранительным органам отслеживать движение средств и идентифицировать преступников. Например, преступник использует некий сервис для конвертации криптоактивов в фиатные деньги. С помощью инструментов для анализа блокчейна можно определить используемый криптосервис, и если в нем реализована строгая политика KYC, это даст возможность идентифицировать реального преступника.

Лучшее ПО и инструменты для анализа блокчейна

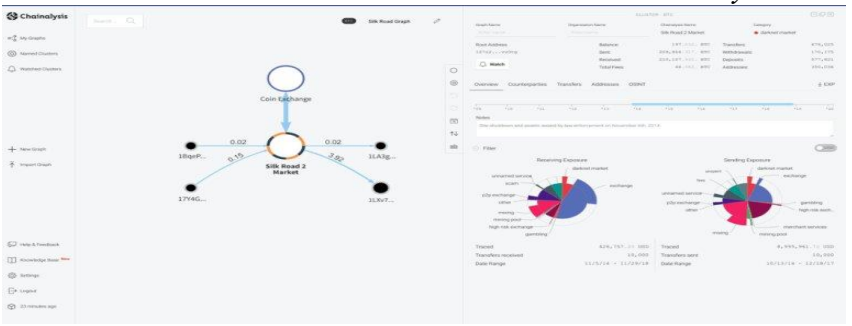
Chainalysis Chainalysis – одна из ведущих компаний в области блокчейн-анализа, которая предоставляет ПО для обеспечения правового соответствия и проведения собственных исследований банкам, криптобизнесам и государственным учреждениям. Она предлагает множество инструментов для мониторинга транзакций, оценки рисков и визуализации данных.

Chainalysis KYT (Know Your Transaction) определяет рискованные криптовалютные транзакции, ассоциируемые с даркнет-маркетами, мошенническими схемами и адресами, находящимися под санкциями. Программа предоставляет простой в использовании интерфейс для анализа транзакций и связей между ними.

Reactor помогает визуализировать денежный поток для любого адреса в блокчейне Bitcoin или Ethereum. Программа также предоставляет информацию о реальной идентичности блокчейн-адресов, что имеет решающее значение для расследований, связанных с криптовалютами.

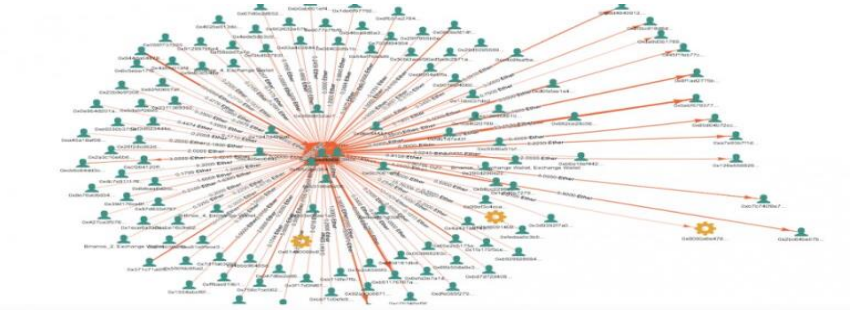
Chainalysis Kryptos предоставляет полные профили для более чем 1800 криптовалютных компаний на основе данных KYC. Это эталонный отраслевой справочник по криптовалютным сервисам и их ончейн-активности (см.Рисунок №2).

Рисунок №2



Coinpath Coinpath – это продукт Bitquery, которая предоставляет API-интерфейсы для отслеживания денежных потоков в блокчейне. С помощью API от Coinpath можно создавать свои инструменты для мониторинга транзакций и визуализации данных, помогающие в расследовании таких преступлений, как, например, отмывание денег через биткойны. В настоящее время поддерживается более 20 блокчейнов и тысяч токенов на основе Ethereum (см.Рисунок №3).

Рисунок №3



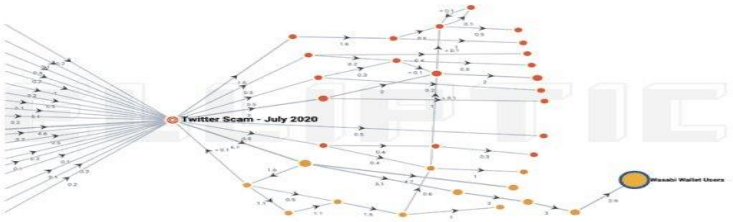
Elliptic

Продуктами Elliptic пользуются крупные криптобиржи и финансовые организации во всем мире. Компания предоставляет множество решений для обеспечения правового соответствия криптовалютных проектов и исследования и анализа блокчейн-данных. Вот некоторые из доступных продуктов Elliptic:

– **Elliptic Lens** обеспечивает компаниям уровень понимания блокчейн-данных, необходимый для защиты бизнеса компании и интересов ее клиентов. Lens используют команды, занимающиеся борьбой с мошенническими схемами и обеспечением правового соответствия, а также операционные подразделения компаний. Этот инструмент дает представление о том, кто стоит за каждым из адресов, а также о денежном потоке кошельков.

– **Elliptic Navigator** – мощные возможности этого инструмента в отношении отслеживания и настраиваемые правила регулирования рисков обеспечивают последовательное и точное понимание источника и конечного пункта назначения средств для более чем 100 криптоактивов (см.Рисунок №4).

Рисунок №4



AnChain.

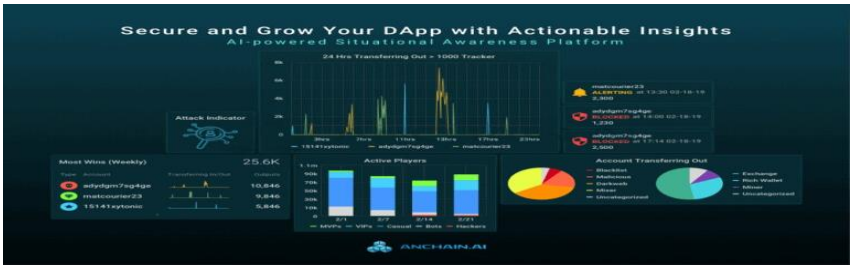
AI Основанная в 2018 году, компания AnChain предоставляет набор продуктов на основе искусственного интеллекта для обеспечения правового соответствия и проведения собственных исследований и анализа в области криптовалют. Продукты AnChain включают в себя:

Blockchain Ecosystem Intelligence API (BEM API) – это источник информации о реальной идентичности владельцев адресов в блокчейне и инструмент для анализа рисков, связанных с криптовалютными транзакциями.

Compliance. Investigation. Security Operation (CISO) – это инструмент для визуализации данных с целью собственного анализа блокчейн-транзакций и адресов с закрепленной за ними реальной идентичностью.

Smart Contract Auditing Sandbox (CAS) – это изолированная программная среда для анализа исходного кода миллионов смарт-контрактов Ethereum и оценки безопасности любых смарт-контрактов, написанных на Solidity (см.Рисунок №5).

Рисунок №5



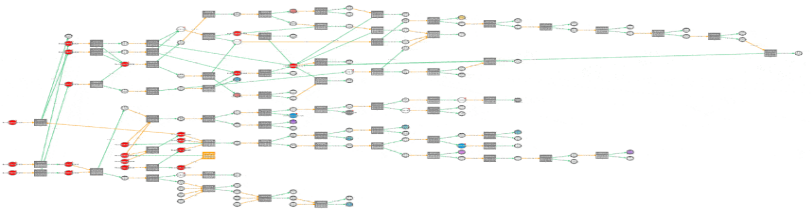
CipherTrace CipherTrace предоставляет поставщикам услуг в сфере виртуальных активов полный комплект инструментов для контроля рисков и обеспечения правового соответствия. Продукты компании поддерживают более 800 токенов и помогают обнаружить факты отмывания денег посредством криптовалют, проводить расследования и осуществлять регуляторный надзор за правовым соответствием бизнесов, работающих с виртуальными активами. В число продуктов ChiperTrace входят:

Armada – определяет высокорисковые платежи между банками и поставщиками услуг в сфере виртуальных активов и выявляет риски, связанные с сотнями подобных провайдеров услуг и другими компаниями криптосферы, используя глубокий анализ их практик KYC и AML.

Sentry – помогает расследовать деятельность по отмыванию денег посредством криптовалют на основе анализа как открытых, так и закрытых данных, а также использует патентованные алгоритмы кластеризации для быстрого агрегирования и выявления корреляции между различными показателями, а затем предоставляет пользователям полезную для практического применения атрибуцию.

Inspector – инструмент поиска и визуализации для исследования криптовалютных транзакций (см.Рисунок №6).

Рисунок №6



Crystal Blockchain

Crystal Blockchain – это продукт Bitfury, предоставляющий различным биржам и банкам API-интерфейсы для отслеживания денежных потоков в блокчейнах и другие веб-инструменты. Предусмотрены три варианта лицензии в зависимости от вариантов использования.

Crystal Expert – облачное решение для исследования блокчейна Биткойна, разработанное для нужд малого бизнеса в сфере криптовалют.

Crystal API обеспечивает полностью автоматизированный мониторинг транзакций и разработан для использования в финансовых организациях с большим объемом транзакций, таких как биржи, платежные системы или сервисы для трейдинга.

Crystal Pro предоставляет возможность выделенного хостинга для банков и других крупных финансовых учреждений с целью расширения их возможностей для защиты данных (см.Рисунок №7).

Рисунок №7

Uppsala Security

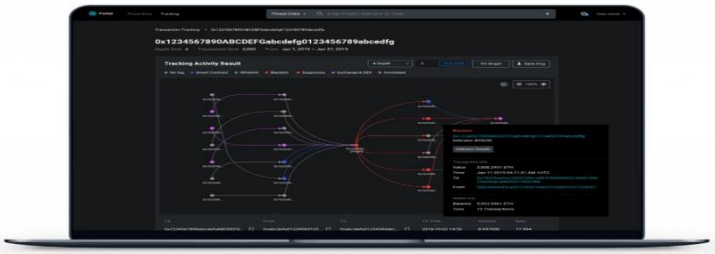
Uppsala Security предоставляет решения по управлению рисками для AML, правового соответствия и кибербез-

опасности в сфере криптовалют. Основанная в январе 2018 года, Uppsala Security построила первую краудсорсинговую платформу для разведки угроз безопасности, известную как Sentinel Protocol. Продукты Uppsala Security включают:

Crypto Analysis Risk Assessment (CARA) – использует технологии машинного обучения для классификации уровней риска криптоадресов, основываясь на поведенческих шаблонах как вредоносных, так и обычных пользовательских кошельков.

Crypto Analysis Transaction Visualization (CATV) – это криминалистическое решение для сферы виртуальных активов, которое отслеживает как входящие, так и исходящие транзакции проверяемого кошелька. Этот инструмент предоставляет визуальный интерфейс для анализа потоков токенов и типов кошельков, с которыми взаимодействует исследуемый кошелек, помогая определить подозрительные отклонения от паттернов поведения обычных пользователей (см.Рисунок №8).

Рисунок №8



Coinfirm

Coinfirm основана в 2016 году, под руководством бывших ведущих AML-специалистов из Royal Bank of Scotland. Компания предоставляет множество решений для AML и правового соответствия. Производимое компанией ПО позволяет также быстро передавать, регистрировать и отчитываться обо всех данных, необходимых для соответствия т.н. Travel Rule (обновление к рекомендациям FATF,

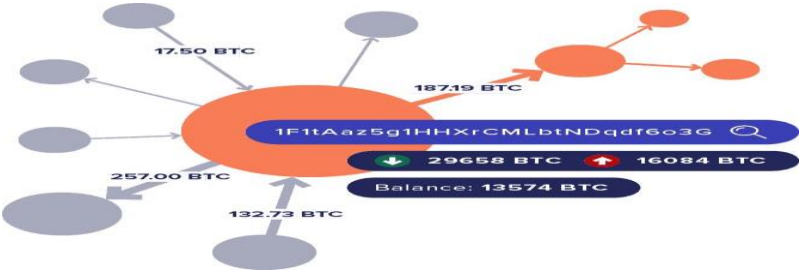
касающееся международных и внутренних электронных переводов) и требованиям, перечисленных в нормативах FATF.

В число продуктов Coinfirm входят:

Coinfirm's AML platform – помогает криптобизнесам осуществлять в реальном времени мониторинг адресов и транзакций.

Travel rule solution от Coinfirm предоставляет провайдерам услуг в сфере виртуальных активов инструменты для идентификации, анализа рисков и сопровождения конкретных случаев, обеспечивая для компаний соответствие рекомендациям FATF (см.Рисунок №9).

Рисунок №9



Solidus Labs

Solidus Labs – это автоматизированный центр для наблюдения за рынком и мониторинга рисков, разработанный специально для работы с цифровыми активами. Это решение позволяет управлять всеми рисками правового соответствия из одной программной среды и помогает минимизировать риски и затраты клиентов.

В число продуктов Solidus входят:

– Решения по наблюдению за рынком и мониторингу транзакций помогают идентифицировать фиктивную торговлю и спуфинг, а также характерные для крипторынков угрозы, такие как межрыночные манипуляции.

– Решения для управления рисками и сопровождения отдельных случаев помогает клиентам избежать многих угроз и операционных проблем и управлять соответствием

регуляторным требованиям посредством единого интуитивно понятного интерфейса, созданного специально для работы с криптоактивами (см.Рисунок №10).

Рисунок №10

В отличие от традиционных финансов, технология блокчейн позволяет реализовывать технологические инновации с неограниченным пользовательским доступом к продуктам и услугам. Наличие открытых данных позволяет производителям создавать передовые программы для отслеживания и анализа этих данных. Это также и единственный способ эффективно выявлять преступную активность, связанную с криптовалютами. Без таких инструментов и правоохранительные органы, и криптобизнес, были бы практически слепы [38].

3.2 Анализ блокчейна для установления следов финансирования терроризма: возможности и ограничения

Блокчейн-технология, лежащая в основе криптовалют, предоставляет уникальную возможность для отслеживания и анализа финансовых операций. Прозрачность и неизменяемость блокчейна, хотя и привлекательны для обеспечения безопасности и прозрачности, также создают сложности для террористических организаций, которые пытаются использовать криптовалюты для финансирования своей деятельности [39].

1. Возможности анализа блокчейна:

Прозрачность транзакций: Все транзакции в блокчейне публичны и доступны для просмотра. Это позволяет отслеживать движение средств от источника до получателя.

Неизменяемость данных: Информация, записанная в блокчейн, не может быть изменена или удалена. Это обеспечивает достоверность данных и позволяет восстановить цепочку транзакций.

Анализ графов транзакций: Использование инструментов анализа графов позволяет визуализировать связи между адресами в блокчейне, выявлять паттерны активности и кластеры, связанные с подозрительными операциями.

Анализ потоков средств: Отслеживание движения средств между различными адресами позволяет определить источник финансирования, получателей и маршруты, которые используются для маскировки операций.

Анализ метаданных: Изучение метаданных, связанных с транзакциями, таких как время, IP-адрес, криптобиржа, может предоставить дополнительную информацию для выявления подозрительной активности [40].

2. Ограничения анализа блокчейна:

Псевдонимность: хотя транзакции в блокчейне публичны, адреса не всегда связаны с реальными лицами. Это затрудняет идентификацию участников операций.

Сложность анализа: Объем данных в блокчейне может быть огромным, что требует значительных вычислительных ресурсов и специализированных инструментов для анализа.

Отсутствие централизованной информации: Отсутствие централизованного реестра криптоактивов затрудняет сбор и анализ данных из разных источников.

Динамичное развитие: постоянно появляются новые криптовалюты и технологии, что требует постоянного обновления инструментов и методов анализа [41].

3. Примеры использования анализа блокчейна:

Выявление анонимных кошельков: Анализ графов транзакций позволяет выявлять анонимные кошельки, которые могут быть использованы для отмывания денег или финансирования терроризма.

Отслеживание перемещения средств: Анализ потоков средств позволяет отслеживать перемещение средств от источника до получателя, выявляя промежуточные кошельки и транзакции.

Идентификация подозрительных транзакций: Анализ поведения пользователей и метаданных позволяет идентифицировать подозрительные транзакции, которые могут быть связаны с финансированием терроризма.

Анализ смарт-контрактов: Анализ смарт-контрактов позволяет выявлять потенциальные риски и злоупотребления, связанные с финансированием терроризма [42].

Анализ блокчейна является мощным инструментом для борьбы с финансированием терроризма. Он позволяет отслеживать движение средств, выявлять подозрительную активность и предотвращать незаконные операции. Однако, необходимо помнить о его ограничениях, таких как псевдонимность и сложность анализа. Развитие технологий, а также сотрудничество с криптосообществом и правоохранительными органами позволит повысить эффективность использования анализа блокчейна для борьбы с финансированием терроризма [43].

3.3 Методы оперативного сбора информации при обнаружении фактов финансирования терроризма через криптовалюты

Один из распространенных способов сбора средств для реализации целей террористической деятельности – обращение к близким родственникам и друзьям членов террористической организации. Поэтому нужно устанавливать в обязательном порядке круг родственников и друзей каждого субъ-

екта террористической организации для отслеживания денежных потоков. В настоящее время финансовая и материально-техническая поддержка террористических группировок и отдельных террористов формируется за счет средств из внешних (за пределами юрисдикции) и внутренних источников. При проведении финансовых расследований в случае наличия фактов финансирования от родственников и знакомых необходимо собирать и анализировать движения денежных средств родственников террористов и их близких (знакомых), как находящихся на территории страны, так и за ее пределами. При наличии у подозреваемых лиц денежных средств на банковских счетах и картах необходимо получать сведения о движении средств на них. В ряде случаев лица, оказывающие содействие террористам, совершают переводы с использованием карт, зарегистрированных в других странах либо с использованием различных платежных систем в качестве средства, обеспечивающего частичную конфиденциальность, либо для облегчения совершения платежа. В таких случаях лицам, проводящим финансовые расследования следует получать информацию из национальных либо зарубежных платежных систем о проводимых транзакциях подозреваемыми, а также использованных ими финансовых инструментах.

Наиболее сложным в этом случае является отслеживание совершенных транзакций в виртуальных валютах. В этом случае финансовые расследования должны преследовать цель не только установить данные о наличии криптокошельков у лица, переводившего средства на нужды террористов, но и совместно с зарубежными коллегами получить данные об используемых террористами и их пособниками криптокошельках, счетах в банках, электронных кошельках, аффилированных юридических лицах и т.д. Исследование одновременно с ФР в ходе предварительного следствия мобильных устройств, компьютерной техники подозреваемых, связанных с ними лиц, позволяет обнаружить наличие аккаун-

тов социальных сетях в Интернете и почтовых сервисах, а сопоставление имеющейся в них информации с финансовыми данным – отследить, какие финансовые источники и ресурсы использовались для сбора средств. Сбор средств может также осуществляться через подконтрольные юридические лица либо НКО. В этом случае необходимо тщательное исследование финансовых операций таких субъектов в совокупности с иными данными (время их регистрации, декларируемый вид деятельности, фактическое осуществление предпринимательской активности и т.д.) [44].

Глава 4. Рекомендации по эффективному противодействию финансированию терроризма в условиях цифрового развития преступности

4.1 Обучение сотрудников полиции о распознавании признаков возможного финансирования терроризма с использованием криптовалют

Легализация преступных доходов и финансирование терроризма – угрозы мирового порядка, представляющие опасность для международной финансовой системы и экономики каждого государства. Данные явления неразрывно связаны и с другими преступлениями: коррупция, незаконный оборот наркотиков, торговля людьми, мошенничество, кражи. В условиях реально существующих террористических угроз, оффшоризации капиталов и появления все новых схем отмывания доходов неизбежно встает вопрос о компетентности сотрудников организаций, работающих с денежными средствами и иным имуществом, которое может быть использовано для ОД/ФТ, их информированности и подготовленности к недопущению, выявлению и предотвращению незаконных финансовых потоков, используемых в том числе и для террористической деятельности [45].

Обучение и образовательные программы должны быть стандартизированы для правоохранительных органов. Базовое обучение должно быть предусмотрено уже на начальном уровне, а специализированное обучение отдельных сотрудников должно проводиться как на начальном уровне, так и в течение всей карьеры сотрудника. Вместе с тем такое специализированное обучение сотрудников будет различаться в зависимости от задач, которые стоят перед следователем по финансовым преступлениям и финансовым аналитиком. Сотрудники, которые выбрали для себя эту сферу деятельности, должны быть обеспечены возможностями карьерного роста и конкурентной заработной платой. Базовые навыки проведения финансового расследования должны включаться в программу подготовки сотрудников полиции начального уровня и опытных следователей [46].

Решить проблему только на уровне государства невозможно, поскольку именно организации, осуществляющие операции с денежными средствами или иным имуществом (перечень определен в Законе «О ПОД/ФТ», далее организации), работают с гражданами, проводят финансовые операции и сделки, на местах принимают решение о подтверждении или отказе в перемещении денежных средств внутри страны и за ее пределами. Реагирование и принятие мер в этом случае должно быть не только оперативным, но и опережающим преступный замысел, поскольку на стадии интеграции, когда «грязные» деньги «вводятся» в легальный экономический оборот и под «правомерным видом» «растворяются» в экономике того или иного государства, отследить цепочку, а тем более вернуть преступно добытые «отмытые» средства бывает крайне сложно.

В этих условиях государство призывает на помощь организации и, помогая им, формирует национальную систему ПОД/ФТ, одним из элементов которой является подготовка кадров, создает необходимую для этого законодательную базу. По своей сути государство выработало и предложило как

для себя и своих органов, так и для организаций – методологию борьбы с ОД/ФТ, закрепив это в своде законов и подзаконных актов.

Цель подготовки и обучения кадров – получение необходимых знаний для соблюдения действующего законодательства РК и внутренних документов организации в области ПОД/ФТ, а также содействие формированию и совершенствованию систем внутреннего контроля организаций. Но, конечно, само по себе только получение знаний не может быть основной целью, так как «теория без практики мертва». Поэтому в качестве основной цели выступает повышение подготовки, компетентности и профессионализма кадров на основе полученных ими в процессе обучения знаний, и как результат – 13 способность принимать меры по противодействию отмыванию денег и финансированию терроризма. Все это объединяет стратегическая цель – обеспечение экономической безопасности нашей страны.

Для достижения указанных целей, а также для обеспечения экономической безопасности Указом Президента РК создана Академия финансовой борьбы с отмыванием (AML Academy), которая обучает сотрудников правоохранительных органов вопросам проведения параллельных финансовых расследований, а также дел связанных с использованием цифровых активов [47].

Основными задачами Академии являются:

– обучение, подготовка и повышение квалификации с проведением сертификации на системной основе всех участников национальной системы ПОД/ФТ/ФРОМУ: лица, предоставляющие информацию, информацию в уполномоченный орган по финансовому мониторингу в соответствии с Законом Республики Казахстан о ПОД/ФТ, должностные лица и поставщики агентств, государственные органы, а также руководители руководящих/специальных государственных органов и судей, занимающихся расследованиями и соблюдением уголовных дел в сфере ПОД/ФТ/ФРОМУ, и другие

официальные лица (при заключении соответствующих договоров)

– совершенствование и дальнейшее развитие деятельности дополнительного образования в сфере ПОД/ФТ/ФРОМУ

– проведение научных, прикладных, аналитических и ИТ-исследований, оценочных мероприятий, методических разработок в целях развития национальных систем ПОД/ФТ/ФРОМУ [48].

4.2 Международное сотрудничество для обмена информацией и координации действий при противодействии финансированию терроризма с использованием криптовалют

Развитие цифровых технологий, инноваций в области обработки и передачи данных и Интернета привело к созданию гиперсвязанного мира, в котором доступ к информации, обмен ею и ее получение происходят практически мгновенно. По состоянию на 2022 год почти 70 процентов населения мира пользуется Интернетом [49], из которых более 93 процентов – это пользователи социальных сетей [50]. По оценкам, в 2022 году в мире будет создано более 97 зеттабайт информации. В то время как подобные технологические достижения способствуют преобразованию общества во имя всеобщего блага, террористы используют эти технологии в своих злонамеренных целях. Применение новых технологий в террористических целях ставит перед государствами-членами серьезные задачи по борьбе с терроризмом, в частности по противодействию использованию технологий, обеспечивающих анонимность и возможность координировать и действовать удаленно.

С другой стороны, новые технологии открывают широкие возможности для укрепления потенциала контртеррористических и правоохранительных органов. Например, с их

помощью правоохранительные органы могут выполнять большие объемы работы с меньшими затратами, принимать своевременные решения в ускоренном порядке, генерировать новые знания и проводить подрывные операции удаленно. Противодействие использованию террористами новых технологий зависит от понимания механизмов такого использования, разработки эффективной правовой базы и мер реагирования на уровне политики, а также наращивания оперативного потенциала для противодействия применению таких технологий в террористических целях, включая привлечение и использование новых технологий.

Новые технологии открывают перед правоохранительными органами безграничные возможности для эффективного противодействия терроризму с соблюдением положений международного права прав человека. Правоохранительные органы могут применять новые технологии для выявления, расследования, судебного преследования и разрешения дел о террористической деятельности новыми и более эффективными способами. Использование оперативной информации из открытых источников обеспечивает быстрый сбор данных об интересующих объектах, что может повысить эффективность правоохранительной деятельности. Передовые технологии анализа данных и искусственного интеллекта (ИИ) позволяют обрабатывать и анализировать огромные объемы информации, благодаря чему правоохранительные органы имеют возможность выявлять закономерности, обнаруживать потенциальные угрозы и принимать превентивные меры реагирования на террористическую деятельность. Новейшие системы наблюдения, включая распознавание лиц и биометрические технологии, помогают идентифицировать и отслеживать перемещения подозреваемых, повышая эффективность расследований, предотвращая потенциальные атаки и привлекая террористов к ответственности. Кроме того, с помощью инструментов цифровой криминалистики можно получать важные доказательства путем извлечения данных из

электронных устройств, что позволяет правоохранительным органам выявлять скрытые связи, разрушать террористические сети и привлекать террористов к ответственности. Использование новых технологий может способствовать более эффективному распределению ограниченных ресурсов правоохранительных органов. При этом крайне важно, чтобы эти технологии использовались с учетом этических норм и при строгом соблюдении права на неприкосновенность частной жизни, прав человека и принципа верховенства права. Необходимо обеспечить прозрачность и подотчетность действий и их результатов, чтобы гарантировать ответственное использование новых технологий и предотвратить потенциальное злоупотребление этими мощными инструментами. Кроме того, рекомендуется внедрить комплексные программы обучения, для того чтобы сотрудники правоохранительных органов могли овладеть необходимыми навыками с целью эффективного применения новых технологий в рамках правовых и этических норм. Ответственно подходя к использованию новых технологий, правоохранительные органы могут значительно расширить свои усилия по борьбе с терроризмом и обеспечить безопасность и защиту населения [51].

Одним из ключевых международных институтов в сфере борьбы с отмыванием доходов, полученных незаконным путем, и финансированием терроризма на сегодняшний день является Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ), созданная по инициативе Глав государств и Правительств Большой семерки в 1989 году.

Итогом работы стал опубликованный доклад «Сорок рекомендаций» ФАТФ в 1990 году, позже пересмотренный и дополненный «IX Специальными рекомендациями». В феврале 2012 года приняты обновленные Рекомендации ФАТФ – Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения.

В настоящее время в мире существует 8 Региональных групп по типу ФАТФ (РГТФ), одной из которых является Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ). ЕАГ создана в 2004 году и объединила страны Евразийского региона: Беларусь, Индию, Казахстан, Китай, Кыргызстан, Россию, Таджикистан, Туркменистан и Узбекистан. С 2011 года группа имеет статус межправительственной организации. ЕАГ призвана сыграть важную роль в вопросах снижения угрозы международного терроризма и обеспечения прозрачности, надежности и безопасности финансовых систем государств региона и их дальнейшей интеграции в международную инфраструктуру противодействия отмыванию денег и финансированию терроризма.

В рамках международной институциональной системы противодействия отмыванию денег и финансированию терроризма в 1995 году учреждена организация неофициального формата – Группа подразделений финансовой разведки «Эгмонт».

Цель Группы «Эгмонт» – обеспечить площадку для эффективного взаимодействия ПФР во всем мире в целях борьбы с отмыванием денег и финансированием терроризма, а также для содействия в реализации внутренних программ по ПОД/ФТ.

Агентство РК по финансовому мониторингу принят в Группу «Эгмонт» в июле 2011 года [52].

Вместе с тем, следует отметить, из отчета взаимной оценки Республики Казахстан о международном сотрудничестве, результаты работы в области ПОД/ФТ:

1. Международное сотрудничество, включая оказание взаимной правовой помощи, в целом осуществляется конструктивно и своевременно. ГП, являясь центральным органом (наряду с ВС) и координатором этой деятельности, обеспечивает учет запросов и их своевременное исполнение. Для их передачи используются защищенные электронные каналы

связи. Опрос Глобальной сети ФАТФ характеризует качество оказания ВПП с положительной стороны. Вместе с тем обратная связь о пользе предоставленных в рамках исполнения запросов ВПП сведений не запрашивается на системной основе.

2. В подавляющем большинстве случаев все компетентные органы обращаются к механизмам ВПП, когда по делу имеется сведения о транснациональном характере преступления. Статистическая информация свидетельствует о том, что компетентные органы уверенно прибегают к механизмам ВПП и в целом запрашиваемая помощь соответствует профилю риска страны.

3. ПО/СГО страны успешно устанавливают, арестовывают и конфискуют активы за рубежом, чему в том числе способствует реализация в Республике Казахстан с 2016г. проекта «Возврат похищенных активов». Используются альтернативные форматы международного сотрудничества, в том числе CARIN, ARIN AP, ARIN-WCA, INTERPOL FOCAL POINT и другие.

4. Власти Республики Казахстан в целом эффективно сотрудничают в сфере выдачи преступников и большинство соответствующих входящих запросов удовлетворяется. В тех случаях, когда лицо скрылось от правоохранительных органов, власти страны принимают меры к установлению его местонахождения и выдачи, либо принимает усилия к привлечению таких лиц к ответственности, в том числе через направление поручений об осуществлении уголовного преследования и иные соответствующие механизмы.

5. Правоохранительные органы эффективно сотрудничают и обмениваются информацией в рамках иных форм на различных международных площадках. Такое сотрудничество приводит к конкретным практическим результатам.

6. Международный информационный обмен по линии АФМ реализуется на системной основе, совместно с широким кругом контрагентов и его характер соответствует наци-

ональным рискам ОД/ФТ. Представители АФМ продемонстрировали широкий круг инструментов международного сотрудничества, которые могут покрыть не только потребности самой финансовой разведки, но и других правоохранительных органов. В то же время представляется недостаточной интенсивность спонтанных информаций зарубежным партнерам, в том числе в тех случаях, когда соответствующие имеющиеся в распоряжении АФМ сведения передаются компетентным органам внутри страны.

7. Международное взаимодействие надзорных органов за ФУ и УНФПП основывается на международных соглашениях, каких-либо нормативных препятствий для обмена соответствующей информацией не имеется. Уровень международного взаимодействия в надзоре соответствует потребностям регуляторов и возможным рискам на данном этапе.

8. Все компетентные органы обеспечивают качественное исполнение запросов иностранных государств о бенефициарных владельцах по каналам ВПП и используя иные формы международного сотрудничества. Существует практика предоставления дополнительных сведений (не связанных с запросом), которые могут быть полезны для финансового расследования [53].

4.3 Профилактика использования криптовалют для финансирования террористических организаций

В последние годы криптовалюты стали привлекательным инструментом для финансирования терроризма, обеспечивая анонимность, скорость и глобальный доступ. Республика Казахстан, стремясь стать мировым центром криптоиндустрии, сталкивается с вызовами, связанными с использованием криптовалют в незаконных целях, включая финансирование терроризма.

Особенности использования криптовалют в финансировании терроризма:

Анонимность: Криптовалютные операции не требуют предоставления личной информации, что затрудняет отслеживание финансовых потоков.

Децентрализация: Криптовалюты не контролируются центральным банком или правительством, что делает их привлекательными для организаций, желающих избежать государственного контроля.

Скорость и доступность: Криптовалютные транзакции осуществляются быстро и доступны в любой точке мира, что позволяет террористам быстро переводить средства и обходить ограничения.

Существующие меры противодействия в Казахстане:

Закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [28] регулирует борьбу с отмыванием денег и финансированием терроризма, но нуждается в совершенствовании в части применения к криптовалютам.

Концепции развития финансового мониторинга на 2022–2026 годы [54] включает меры по укреплению межведомственного сотрудничества, но не хватает специализированных мер по борьбе с использованием криптовалют.

Финансовая разведка Казахстана осуществляет мониторинг финансовых операций, но пока не обладает достаточным опытом и инструментами для эффективного отслеживания криптовалютных транзакций.

Заключение

Профилактика использования криптовалют в отмывании доходов и финансировании терроризма является сложной, но необходимой задачей. Казахстан должен активно действовать, совершенствуя законодательство, укрепляя правоохранительные органы, развивая международное сотрудничество и повышая уровень осведомленности. Своевременные и эффективные меры позволят минимизировать риски использования криптовалют в террористической деятельности и обеспечить стабильность и безопасность в Республике Казахстан.

Республика Казахстан стремится стать мировым центром криптоиндустрии, что приводит к росту числа криптовалютных бирж, обменников и сервисов, создавая благоприятные условия для отмывания денег и финансирования терроризма.

Существующее законодательство о противодействии ОД/ФТ требует обновления и адаптации к особенностям криптовалютных операций, чтобы эффективно пресекать их использование преступниками.

Нехватка специалистов по кибербезопасности и криптовалютам, недостаток финансирования, а также слабая координация между различными ведомствами создают сложности в борьбе с использованием цифровых технологий в ОД/ФТ.

Увеличение числа онлайн-мошенничеств, кражи данных и хакерских атак создает дополнительные угрозы для финансовой системы Казахстана и затрудняет отслеживание финансовых потоков, связанных с ОД/ФТ.

Рекомендации для сотрудников правоохранительных органов:

1. Повышение квалификации:

– обучение сотрудников правоохранительных органов по работе с криптовалютами, кибербезопасностью и анали-

зом финансовых транзакций, в т.ч. с использование цифровых активов (криптовалют).

2. Совершенствование законодательства:

– криминализация деяний за создание и организацию криптомиксеров в незаконных целях, включая отмывание доходов и финансирование терроризма.

3. Усиление международного сотрудничества:

– Активное участие в международных организациях, таких как ЕАГ, FATF и INTERPOL, для обмена информацией и опытом в противодействии ОД/ФТ, в том числе с использованием криптовалют.

4. Развитие новых инструментов:

– применение технологий анализа больших данных для выявления подозрительных финансовых операций, связанных с криптовалютами.

– использование технологий искусственного интеллекта для автоматизации процессов мониторинга финансовых транзакций, в том числе блокчейн и выявления подозрительных операций.

5. Повышение осведомленности:

– проведение информационных кампаний, направленных на повышение осведомленности населения о рисках использования криптовалют в незаконных целях, в том числе в отмывании доходов и финансировании терроризма.

Вместе с тем, правоохранительным органам государства следует обратить внимание на возможности технологий искусственного интеллекта, который будет играть все более важную роль в противодействии преступному отмыванию денег и доходов. Преимущества технологий, такие как скорость, точность, объективность и автоматизация, позволят повысить эффективность противодействия этому явлению. Однако необходимо учитывать вызовы и ограничения, связанные с их использованием, и разрабатывать четкие нормативные рамки для его ответственного применения. По мере развития искусственного интеллекта и его интеграции с дру-

гими технологиями ожидается, что он продолжит играть решающую роль в противодействии преступной легализации (отмывания) доходов и обеспечении национальной безопасности. Однако следует помнить, что эти технологии не заменяют, а дополняют системы, направленные на улучшение результатов и упрощение обеспечения мер по противодействию киберпреступности.

Наряду с этим необходимо проводить повышение квалификации специалистов по работе с технологиями искусственного интеллекта. Этот вопрос требует комплексного подхода, сочетающего в себе обучение и самообразование, практический опыт, сертификацию и аккредитацию, сотрудничество и обмен знаниями.

Для этих целей необходимо внести предложения по дополнению Концепции развития искусственного интеллекта на 2024-2029 годы с включением правоохранительных органов по вопросам использования технологий искусственного интеллекта в сфере противодействия не только отмывания доходов/финансирования терроризма, но и киберпреступности в целом.

С помощью ответственного и эффективного использования искусственного интеллекта мы можем создать более надежную и безопасную финансовую систему и противодействовать преступности, подпитываемой легализацией (отмыванием) денег.

Данные методические рекомендации помогут сотрудникам правоохранительных органов в Казахстане эффективно противодействовать отмыванию доходов и финансированию терроризма в условиях цифрового развития преступности и обеспечить безопасность страны.

Список использованных источников

1. Рисс В.И. К вопросу о коллективных валютах или частных деньгах // Экономика, управление, и право: инновационное решение проблем. – 2017. – С. 21-23.
2. Хажиахметова Е.Ш. Криптовалюта - деньги XXI века // Новая наука: от идеи к результату. — Агентство международных исследований, 2016. – №11-2. – С. 177-179.
3. Crypto Currency Архивная копия от 31 августа 2014 на Wayback Machine, Forbes, 20-04-2011 (вариант русского перевода статьи), интернет – ресурс: https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#1d70e499353e (дата обращения 03.09.20224г.).
4. Пещеров А.И. Понятие и место криптовалюты в системе денежных средств / А.И. Пещеров // Юридическая мысль. – 2016. – №3(95). – С. 130–138. – EDN XDNUSH.
5. *Luke Fortney*. Blockchain Explained (англ.). Интернет – ресурс: Investopedia. https://www.investopedia.com/terms/b/blockchain.asp (дата обращения: 12.09.2024г.).
6. Marco Iansiti and Karim R. Lakhani. The Truth About Blockchain (англ.) // Harvard Business Review: magazine. – 2017. – No. January – February 2017 issue. – P. 118-127. Интернет – ресурс: https://hbr.org/2017/01/the-truth-about-blockchain (дата обращения: 12.09.2024г.).
7. Satoshi, 2008, – С. 3. Интернет – ресурс: https://www.bitcoin.org/bitcoin.pdf (дата обращения: 12.09.2024г.).
8. Genesis Block, Block 0 (англ.). Интернет – ресурс: https://bitcoin.org/en/glossary/genesis-block (дата обращения: 12.09.2024г.).
9. Finding 2016 Blocks Интернет – ресурс: https://davehudson.io/blog/2014-06-15-0000 (дата обращения: 12.09.2024г.).

10. Bitcoin Block Explorer – сайт, позволяющий просматривать цепочку блоков Интернет – ресурс: https://www.blockexplorer.com/ (дата обращения: 12.09.2024г.).

11. Joshua Kopstein (2013-12-12). «The Mission to Decentralize the Internet». The New Yorker Интернет – ресурс: https://www.newyorker.com/tech/annals-of-technology/the-mission-to-decentralize-the-internet (дата обращения: 12.09.2024г.).

12. Vitalik Buterin. On Public and Private Blockchains Интернет – ресурс: https://www.coindesk.com/markets/2015/08/07/vitalik-buterin-on-public-and-private-blockchains/ (дата обращения: 12.09.2024г.).

13. Какие существуют виды криптовалют и в чем их отличия? Интернет – ресурс: https://blog.whitebit.com/what-are-the-different-types-of-cryptocurrency/ (дата обращения: 12.09.2024г.).

14. «Криптовалюты: возможности и риски для финансовой системы» / Под ред. А.А. Игнатьева, С.В. Соловьева. – М.: Изд-во МГУ, 2020.

15. «The Use of Cryptocurrencies by Terrorist Organizations» / P.A. Tsalidis, P.V. Vouzis. – Global Crime, 2021, vol. 22, no. 4.

16. «Fighting Terrorist Financing Through Cryptocurrencies: A Global Perspective»/ J.M. Galea. - International Journal of Security and Terrorism, 2020, vol. 17, no. 3.

17. «Cryptocurrencies and Terrorism Financing: A Review of the Literature» / M.A. Khan. – Journal of Money Laundering Control, 2020, vol. 23, no. 2.

18. «Cryptocurrencies and Money Laundering: A New Era of Financial Crime» / S.A. Awan. – Journal of Financial Crime, 2021, vol. 28, no. 5.

19. «Blockchain Security: A Comprehensive Guide to Understanding and Protecting Blockchains» / by P.K. Saxena. – Apress, 2021.

20. «Cryptocurrency and Anti-Money Laundering: A Practical Guide to Compliance» / by D.P. Singh. – Springer, 2022.

21. «Financial Crime and Cryptocurrency: A Guide to Detecting and Combating Financial Crime in the Digital Age» / by A.L. Lewis. - Wiley, 2021.

22. «Blockchain Forensics: A Practical Guide to Investigating and Analyzing Blockchain Data» / by M.A. Al-Bassam. – CRC Press, 2020.

23. «The Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World» / by D. Tapscott, A. Tapscott. – Portfolio, 2016.

24. https://eurasiangroup.org/ru/mutual-evaluation-report-of-the-republic-of-kazakhstan-has-been-published-on-the-eag-website.

25. https://adilet.zan.kz/rus/docs/K940001000

26. https://adilet.zan.kz/rus/docs/Z2300000193

27. https://adilet.zan.kz/rus/docs/Z2200000141/info

28. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: закон Республики Казахстан от 13 мая 2020 года №325-VI [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=37484323 (дата обращения: 18.10.2024).

29. О противодействии терроризму: закон Республики Казахстан от 13 июля 1999 г. №416 [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/ docs/Z990000416_ (дата обращения: 18.10.2021).

30. О противодействии экстремизму: закон Республики Казахстан от 18 февр. 2005г. №31 [Электронный ресурс] –

Режим доступа: https://adilet.zan.kz/rus/ docs/Z050000031_ (дата обращения: 18.10.2021).

31. Специальные Рекомендации по предотвращению финансирования терроризма [Электронный ресурс] // URL: http://eurasiangroup.org/files/FATF_docs/9_special_recomendations_rus.pdf (дата рецепции материала 08.08.2018);

32. Конвенция ООН о борьбе с финансированием терроризма (1999).

33. Резолюция Совета Безопасности ООН 1373 (2001).

34. «The Use of Cryptocurrencies by Terrorist Organizations» / P.A. Tsalidis, P.V. Vouzis. – Global Crime, 2021, vol. 22, no. 4.

35. «Fighting Terrorist Financing Through Cryptocurrencies: A Global Perspective»/ J.M. Galea. – International Journal of Security and Terrorism, 2020, vol. 17, no. 3.

36. «Cryptocurrencies and Terrorism Financing: A Review of the Literature» / M.A. Khan. – Journal of Money Laundering Control, 2020, vol. 23, no. 2.

37. "Cryptocurrencies and Money Laundering: A New Era of Financial Crime" / S.A. Awan. - Journal of Financial Crime, 2021, vol. 28, no. 5.

38. Лучшие инструменты для блокчейн-анализа и как они работают Интернет – ресурс: https://investfuture.ru/articles/id/luchshie-instrumenty-dlya-blokcheyn-analiza-i-kak-oni-rabotayut © (дата обращения: 14.09.2024г.)

39. «Blockchain Security: A Comprehensive Guide to Understanding and Protecting Blockchains» / by P.K. Saxena. – Apress, 2021.

40. «Cryptocurrency and Anti-Money Laundering: A Practical Guide to Compliance» / by D.P. Singh. – Springer, 2022.

41. «Financial Crime and Cryptocurrency: A Guide to Detecting and Combating Financial Crime in the Digital Age» / by A.L. Lewis. – Wiley, 2021.

42. «Blockchain Forensics: A Practical Guide to Investigating and Analyzing Blockchain Data» / by M.A. Al-Bassam. – CRC Press, 2020.

43. «The Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World» / by D. Tapscott, A. Tapscott. – Portfolio, 2016.

44. Методические рекомендации ЕАГ по организации и проведению финансовых расследований в сфере ПОД/ФТ, интернет – ресурс: https://eurasiangroup.org/files/uploads/files/Public_typology_reports/FI_Guidence_rus.pdf (дата обращения: 16.09.2024г.).

45. Общая характеристика системы обучения и подготовки кадров в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (под/фт) в России / редкол.: Каратаев М.В. (отв. ред) [и др.] – Москва. – 25 стр.

46. РУКОВОДСТВО ФАТФ ПО ФИНАНСОВЫМ РАССЛЕДОВАНИЯМ: ОПЕРАТИВНЫЕ ВОПРОСЫ Июнь 2012г., Интернет – ресурс: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/reports/Operational%20Issues%20Financial%20Investigations%20Guidance%20_%20RUSSIAN.pdf (дата обращения 16.09.2024г.).

47. Указ Президента Республики Казахстан от 20 февраля 2021 года № 515 О некоторых вопросах Агентства Республики Казахстан по финансовому мониторингу // Интернет – ресурс: https://adilet.zan.kz/rus/docs/U2100000515 (дата обращения: 16.09.2024г.).

48. AML ACADEMY // Интернет – ресурс: https://www.amlacademy.kz/about (дата обращения: 17.09.2024г.).

49. Отчет МСЭ о глобальной возможности установления соединений за 2022 год, URL: https://www.itu.int/itu-d/reports/statistics/ global-connectivity-report-2022/index/

50. Инфографика Data Never Sleeps от компании Domo, Data Never Sleeps 10.0 | Domo

51. Кибербезопасность и новые технологии // Интернет- ресурс: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/law_enforcement_capabilities_framework_for_new_technologies_in_countering_terrorism_finalout_web_ru.pdf (дата обращения: 16.09.2024г.).

52. Международное сотрудничество //интернет – ресурс: https://www.gov.kz/memleket/entities/afm/activities/813?lang=ru (дата обращения: 17.09.2024г.).

53. ОТЧЕТ взаимной оценки Республики Казахстан // 2023 // интернет – ресурс: https://eurasiangroup.org/files/uploads/files/ME_(2023)_1_rus_rev1_2.pdf (дата обращения: 14.09.2024г.).

54. Указ Президента Республики Казахстан от 6 октября 2022 года № 1038 «Об утверждении Концепции развития финансового мониторинга на 2022-2026 годы» // Интернет – ресурс: https://adilet.zan.kz/rus/docs/U2200001038 (дата обращения: 19.09.2024г.).

СОДЕРЖАНИЕ

Верстка:
Туренова Б.Ю.

Отдел организации научно-исследовательской и редакционно-издательской
работы Алматинской академии МВД Республики Казахстан
имени М. Есбулатова 050060 Алматы, ул. Утепова, 29

Подписано в печать 31 октября 2024 г.
Формат 60х84 1/16 Бум. тип. №1. Печать на ризографе. Уч.-изд. л. 2,3.
Тираж 50 экз.