ОТЧЕТ ФАТФ

Виртуальные активы

Признаки

отмывания денег и финансирования террористов

Сентябрь 2020

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) – это независимая межправительственная организация, разрабатывающая и популяризирующая свои принципы для защиты всемирной финансовой системы от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ являются общепризнанными международными стандартами по противодействию отмыванию денег (ПОД) и финансированию терроризма (ФТ). Подробная информация о ФАТФ размещена на сайте: http://www.fatf-gafi.org.

Данный документ и/или любые включённые в него географические карты подготовлены без предубеждения и ущемления статуса или суверенитета над любой территорией, международных границ и разграничительных линий, а также названий любых территорий, городов или областей.

Неофициальный перевод подготовлен АНО МУМЦФМ

Ссылка на оригинальный документ:

FATF (2020), *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets,* FATF, Paris, France, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

Фотография на первой странице: © GettyImages

Содержание

Список сокращений

КПА	Криптовалюта повышенной анонимности
НПК	Надлежащая проверка клиента
УНФПП	Установленные нефинансовые предприятия и профессии
DNS	Регистраторы доменных имен
ФАТФ	Группа разработки финансовых мер борьбы с отмыванием денег
ФО	Финансовые организации
ICO	Первичное размещение криптомонет
KYC	Верификация клиента
ПОО	Правоохранительные органы
ОД	Отмывание денег
СПО	Сообщения о подозрительных операциях
ФТ	Финансирование терроризма
ПУВА	Провайдеры услуг в сфере виртуальных активов

Введение

1. Виртуальные активы (ВА) и связанные с ними услуги могут стимулировать финансовую инновацию и повышать эффективность. Однако их особенности открывают и новые возможности лицам, занимающимся отмыванием денег, финансирующим террористов и другим преступникам, для отмывания преступных доходов и финансирования своей преступной деятельности. Возможность совершать быстрые трансграничные операции позволяет преступникам не только приобретать, перемещать и хранить активы в цифровом виде, часто за пределами регулируемой финансовой системы, но и скрывать отправителя и получателя средств, и затруднять своевременное выявление подозрительной деятельности сообщающими лицами. Эти факторы создают дополнительные препятствия для выявления и расследования преступной деятельности национальными органами власти.

2. В октябре 2018 года Группа финансовых мер борьбы с отмыванием денег (ФАТФ) актуализировала свои стандарты, уточнив их применение к деятельности в сфере ВА и к провайдерам услуг в сфере виртуальных активов (ПУВА), чтобы, в том числе, оказать помощь странам и территориям в снижении рисков отмывания денег (ОД) и финансирования террористов (ФТ), создаваемых деятельностью в сфере ВА, а также в защите целостности глобальной финансовой системы. В июне 2019 года ФАТФ приняла Пояснительную записку к Рекомендации 15, преследуя цель уточнить применение требований ФАТФ к деятельности и операциям с ВА и к ПУВА, в том числе в отношении передачи сообщений о подозрительных операциях.

3. ФАТФ подготовила настоящий краткий отчет о признаках ОД/ФТ, имеющих отношение к ВА, чтобы оказать помощь сообщающим лицам, включая финансовые организации (ФО), установленные нефинансовые предприятия и профессии (УНФПП), и ПУВА. Однако классификация этих признаков выполнена, исходя из особенностей выявления возможных случаев ОД и ФТ с использованием ВА, и передачи сообщений об этом. Настоящий отчет призван также помочь применению сообщающими лицами риск-ориентированного подхода к выполнению ими требований по надлежащей проверке клиентов (НПК). Согласно этим требованиям сообщающее лицо обязано знать, кто является его клиентом и бенефициарным владельцем, понимать характер и цели деловых отношений, а также иметь правильное представление об источнике средств клиента.

4. Оперативные учреждения, включая подразделения финансовой разведки (ПФР), правоохранительные органы (ПОО), а также работники прокуратуры могут использовать настоящий отчет в качестве справочно-информационного материала при анализе сообщений о подозрительных операциях (СПО), а также в целях совершенствования процессов выявления, расследования и конфискации ВА, имеющих отношение к противоправному применению.

5. С другой стороны, регуляторы финансовых организаций, УНФПП и ПУВА могут использовать эти признаки при подготовке СПО, и в мониторинге соблюдения сообщающими лицами требований режима ПОД/ФТ. Если сообщающее лицо располагает информацией, указывающей на наличие одного или нескольких признаков, не находящих объяснения с точки зрения бизнеса клиента, или если клиент дает противоречивые объяснения, но сообщающее лицо, несмотря на это, не передает СПО, либо не пытается добиться ясности в отношении операции, компетентные органы могут рассмотреть возможность проведения с сообщающим лицом последующих мероприятий с учетом его сферы деятельности.

Методология и источники, использованные при подготовке перечня признаков

6. При подборе включенных в настоящий отчет признаков использовались более сотни практических примеров, предоставленных странами и территориями в период с 2017 по 2020 год, материалы *Конфиденциального доклада ФАТФ о финансовых расследованиях в области виртуальных активов* (июнь 2019 года), опубликованного документа под названием *Отчет ФАТФ Виртуальные валюты. Ключевые определения виртуальных валют и потенциальные риски ПОД/ФТ* (июнь 2014 года), а также сведения о противоправном применении ВА, имеющиеся в открытом доступе.

Тенденции использования ВА для целей ОД/ФТ

Большинство преступлений в сфере ВА составили предикатные преступления и преступления ОД. Тем не менее, преступники использовали ВА и для уклонения от финансовых санкций и для сбора средств на поддержку терроризма.

Виды преступлений, о которых сообщают страны и территории, включают ОД, продажу контролируемых веществ и других запрещенных предметов (включая огнестрельное оружие), мошенничество, уклонение от уплаты налогов, компьютерные преступления (например, кибератаки с целью кражи), эксплуатацию детей, торговлю людьми, уклонение от санкций и ФТ. Наиболее распространенным среди них видом противоправного использования является незаконный оборот контролируемых веществ, когда они либо непосредственно продаются за ВА, либо ВА используется для наслоения в процессе ОД. Вторая по масштабам сфера преступного использования связана с мошенническими действиями, аферами, вымогательством и применением программ–вымогателей выкупа. В последнее время использовать ВА в качестве средства перевода, сбора и наслоения доходов начали профессиональные сети ОД.

Источник: Практические примеры, представленные странами и территориями в период с 2017 по 2020 год

Читателю этого отчета на заметку

7. Эти признаки характерны исключительно для ВА и для связанной с ними финансовой деятельности, и никоим образом не являются единственно возможными. Связанная с ВА подозрительная деятельность может также иметь те же проявления, что и деятельность по ОД/ФТ с использованием фиатной валюты и других видов активов. Поэтому сообщающие лица должны учитывать риски, создаваемые их клиентами, продуктами и операциями, а также наличие традиционных показателей риска. Признаки подозрительных операций всегда следует рассматривать в контексте.

8. Допускается самостоятельная разработка признаков, подобных перечисленным ниже. Они могут разрабатываться либо объединяться с информацией, полученной от оперативных учреждений, которая, в свою очередь, может быть доработана в рамках государственно-частного партнерства в циклическом эволюционном процессе, учитывающем риск и контекст, присущие конкретной стране или территории, категорию клиента или самого сообщающего лица. Наличие признака само по себе не обязательно является основанием для подозрений в ОД или ФТ, однако оно может послужить толчком для дальнейшего анализа и мониторинга. В конечном счете, может оказаться, что клиент, при объяснении наличия конкретного признака предоставит обоснование деловых или экономических целей сделки.

9. Компетентным органам, ФО, УНФПП и ПУВА при решении вопроса о возможной подозрительной деятельности следует помнить о том, что одни признаки могут чаще прослеживаться при ведении общего мониторинга операций, в то время как другие могут наблюдаться в ходе анализа конкретных операций. Наблюдение одного или нескольких признаков зависит от вида хозяйственной деятельности, продуктов и услуг, которые предлагает организация или ПУВА, а также от того, как они взаимодействуют со своими клиентами. Сообщающее лицо может с большей вероятностью заподозрить ОД или ФТ при наличии одного или нескольких признаков при практическом либо полном отсутствии указаний на законную цель экономической или предпринимательской деятельности.[1] Эти признаки не должны быть единственным фактором, определяющим необходимость передачи СПО. Сообщающим лицами следует рассматривать возможность передачи СПО при условии, если они знают, подозревают, либо имеют разумные основания предполагать, что было совершено преступление ОД/ФТ.

Признаки

10. Следующие далее разделы содержат подборку признаков подозрительной деятельности в сфере ВА или возможных попыток уклониться от разоблачения правоохранительными органами. Эти признаки были заимствованы из более чем сотни практических примеров, собранных с 2017 года по всей глобальной сети ФАТФ, а также из обзоров литературы и из исследований открытых источников. Как уже отмечалось, наличие одного признака не обязательно указывает на преступную деятельность. Часто подозрение на возможную преступную деятельность вызывает именно наличие нескольких признаков в операции, не имеющей логичного обоснования с точки зрения бизнеса. Наличие признаков должно служить толчком к проведению дальнейшего мониторинга, анализа и, в соответствующих случаях, к передаче сообщения.

Признаки, относящиеся к операциям

11. ВА пока не нашли широкого распространения среди населения, однако ими воспользовались преступники. Хотя использование ВА в целях ОД впервые стало известным более десяти лет назад, в настоящее время ВА получают все более широкое распространение в преступной деятельности. Данный набор признаков демонстрирует, что признаки, традиционно относящиеся к операциям с использованием обычных средств платежа, остаются актуальными и при выявлении возможной незаконной деятельности в сфере ВА.

Размеры и частота операций

- Структурирование операций с ВА (например, операций обмена или перевода), осуществляемое аналогично структурированию операций с наличными, путем разбиения на небольшие суммы либо на суммы, не превышающие пороговых значений, установленных для обязательной регистрации операций или для передачи сообщений.
- Проведение нескольких операций на большую сумму:
  - ✓ в короткие сроки, например в пределах 24-часового периода;
  - ✓ с регулярным сдвигом во времени, после чего операции на продолжительное время прекращаются. Эта картина особо распространена в случаях применения программ-вымогателей; или
  - ✓ на вновь открытый либо на ранее спящий счет.

1 Поскольку ряд признаков может относиться как к случаям ОД, так и ФТ, например, в при сборе средств, при финансировании иностранных боевиков-террористов (ИБТ) и покупке оружия (например, в даркнете) с использованием ВА, читателю рекомендуется читать совместно с Конфиденциальным отчетом ФАТФ о выявлении финансирования терроризма: соответствующие показатели риска (июнь 2016 года) (ограниченный доступ только для членов ФАТФ).

- Перевод ВА в пожарном порядке сразу в адрес нескольких ПУВА, особенно ПУВА, зарегистрированных либо оперирующих в другой стране или территории, в которой:
  - ✓ отсутствует взаимосвязь с местом жительства либо местом ведения бизнеса клиента; или
  - ✓ регулирование ПОД/ФТ отсутствует либо осуществляется недостаточно жестко.
- Внесение ВА депозитом на биржу, а затем нередко немедленный:
  - ✓ вывод ВА с биржи без проведения каких-либо операций обмена на другой ВА. Такой шаг представляется излишним, ведь он лишь ведёт к неоправданным расходам на комиссионные;
  - ✓ обмен ВА на ВА нескольких других видов, что опять же влечет за собой дополнительные комиссии за транзакции, но не имеет логичного обоснования с точки зрения бизнеса (например, диверсификация портфеля); или
  - ✓ перевод ВА из ПУВА непосредственно в личный кошелёк. По сути это превращает биржу или ПУВА в миксер ОД.
- Получение средств, предположительно украденных либо полученных в результате мошенничества:
  - ✓ депонирование средств с адресов ВА, на которых, как было установлено ранее, находились украденные средства, или с адресов, привязанных к держателям украденных средств.

Пример 1. Многократные немедленные переводы большого количества ВА в зарубежные ПУВА

Местный ПУВА представил СПО после возникновения у него подозрений в связи с покупкой крупных сумм ВА различными физическими лицами и их последующей немедленной передачей ПУВА в зарубежной стране. В некоторых случаях эти лица имели один и тот же адрес проживания, а большинство адресов ВА были доступны с одного и того же IP-адреса, что указывало
на возможное использование денежных мулов профессиональными отмывателями денег.

Кроме того, до покупки ВА мулами было организовано несколько наслоений фиатных средств. Чтобы скрыть происхождение средств, наличные деньги сначала депонировались на различные счета в различных ФО по всей стране. Затем эти средства переводились на различные счета, открытые на имя юридических лиц, зарегистрированных в данной стране. Электронные платежи поступали на счета небольшими суммами. После этого средства, прежде чем они попадали на счета мулов, открытые в местных ПУВА, переводились на другую группу счетов. На эти деньги немедленно приобретались ВА и переводились иностранным ПУВА. В этом примере фигурируют более 150 человек, которые перевели в общей сложности около 108352900 долларов США (или 11960 BTC) на несколько счетов ВА, принадлежащих двум зарубежным ПУВА.

Источник: Южная Африка

Пример 2. Несколько ВА и несколько переводов в зарубежные ПУВА

Местная биржа ВА сообщила, что у жертв фишинга были украдены примерно 400 миллионов южнокорейских вон (301170 евро). В конечном итоге их обменяли на ВА на этапе наслоения. Причиной передачи сообщения о подозрительной операции были несколько крупных переводов в один кошелек зарубежному ПУВА. Похищенные средства в фиатной валюте сначала обменивались на ВА трех видов, а затем депонировались в кошелек ВА подозреваемого лица в местном ПУВА. После этого подозреваемый попытался скрыть источник средств, переведя средства еще 55 раз через 48 отдельных счетов в нескольких местных ПУВА, а затем на другой заграничный кошелек ВА.

Источник: Южная Корея

Признаки, относящиеся к рисунку операций

12. Как и в предыдущем разделе, представленные ниже признаки иллюстрируют, как по нестандартному, странному или необычному рисунку операций можно выявить использование ВА для ОД/ФТ.

Операции новых пользователей

- Внесение крупного первоначального депозита при установлении новых отношений с ПУВА, при этом сумма средств не соответствует профилю клиента.
- Внесение всей суммы крупного первоначального депозита при установлении новых отношений с ПУВА в первый же день открытия счета. В тот же или на следующий день клиент начинает торговать всей суммой или её большой частью, либо на следующий день снимает всю сумму. Поскольку большинство ВА имеют операционный лимит по депозитам, отмывание крупных сумм может также осуществляться через внебиржевую торговлю.[2]
- Новый пользователь пытается торговать всей суммой ВА на балансе, либо снимает ВА и пытается перечислить с платформы весь остаток.

Пример 3. Первоначальный депозит не соответствует профилю клиента

Наличие следующих подозрительных признаков побудило ФО (банк) подать СПО, что стало причиной расследования ОД:

- операции, не соответствующие профилю владельца счета: в первые два дня после открытия лицевого счета для молодого по возрасту физического лица на счет поступали депозиты коммерческого характера в крупных размерах от различных юридических лиц;
- картина транзакций: внесенные средства немедленно переводились на счета нескольких ПУВА (в один день) для покупки ВА (биткоинов);

2 Внебиржевая торговля - торговля через брокерско-дилерскую сеть ценными бумагами с компаниями, которые не котируются на официальной бирже.

- профиль клиента — один участник операции был известен банку как фигурант дела о мошенничестве. Банк также предоставил властям IP-адреса, использованные для оказания услуг интернет-банкинга.

Расследование показало, что владелец личного счета был денежным мулом, завербованным преступниками на платформе социальных сетей, якобы для того, чтобы получать платежи за товары, продаваемые в интернете. Однако на самом деле эти средства перечислялись другими компаниями-жертвами, и не являлись платежами за товары. Депонированные средства дробными платежами немедленно переводились с личного банковского счета на другой счет, принадлежащий акционерному обществу в Чешской Республике, и обменивались на ВА (биткоин) в ряде местных ПУВА. Затем эти ВА немедленно снимались со счета. Помимо передачи СПО банк приостановил подозрительные переводы, что впоследствии позволило арестовать средства.

Местный ПУВА также заметил странности в полученных средствах и предоставил полезную информацию в помощь расследованию. Эта информация включала: обстоятельства, при которых были приобретены ВА; данные о транзакциях и другие сведения, полученные по линии НПК: адрес кошелька, копию представленного для покупки удостоверения личности, и имя предполагаемого покупателя. Это дало возможность властям запросить дополнительную информацию у банков (например, справки о состоянии счета).

Источник: Чешская республика

Операции, имеющие отношение ко всем пользователям

- Транзакции в нескольких ВА или с несколькими счетами, без логичного обоснования с точки зрения бизнеса.
- Частые переводы в течение определенного периода времени (например, день, неделя, месяц и т. д.) на один и тот же счет ВА:
  - ✓ несколькими лицами;
  - ✓ с одного и того же IP-адреса одним или несколькими лицами; или
  - ✓ на крупные суммы.
- Входящие операции с многих не связанных между собой кошельков на относительно небольшую сумму (накопление средств) с последующим переводом на другой кошелек или обменом всей суммы на фиатную валюту. Такие операции по нескольким связанным накопительным счетам могут сначала выполняться с ВА вместо фиатной валюты.
- Обмен ВА на фиатную валюту с потенциальным убытком (например, когда колеблется курс ВА, или невзирая на завышенные по сравнению со стандартами отрасли комиссионные сборы, в особенности когда сделки не имеют логичного обоснования с точки зрения бизнеса).
- Конвертация большого количества фиатной валюты в ВА или большого количества одного вида ВА в другие виды ВА без логичного обоснования с точки зрения бизнеса.

Пример 4. Повторные переводы

Местная ФО (фирма, занимающаяся ценными бумагами) передала СПО о несанкционированных переводах между счетами ВА своего брокера и иностранного гражданина. Фирма сообщила об этой деятельности после того, как установила, что этот иностранный гражданин намеревался совершить переводы на общую сумму 4,8 миллиона долларов США (двумя отдельными операциями с интервалом в шесть минут в один и тот же день), и подал брокеру заявку на открытие торгового счета на следующий рабочий день. Кошелек находился за пределами Каймановых островов. Данные этого СПО позволили провести успешный обмен информацией с иностранными ПФР. Онлайн-платформа в зарубежной стране смогла заморозить счет подозреваемого до завершения преступления, и большая часть средств была возвращена жертве.

Источник: Каймановы острова

Признаки, относящиеся к анонимности

13. Этот набор признаков опирается на системные характеристики и уязвимости, обусловленные технологией ВА. Приведенные ниже технологические приёмы повышают анонимность и создают дополнительные препятствия для выявления преступной деятельности правоохранительными органами. Эти факторы делают ВА привлекательными для преступников, которые хотят замаскировать или складировать свои средства. Тем не менее, само по себе наличие этих признаков в чьей-то деятельности автоматически не предполагает наличия незаконной сделки. Например, использование аппаратного или бумажного кошелька может быть законным способом защиты от краж. Опять же, наличие этих показателей следует рассматривать в контексте других характеристик клиента и взаимоотношений, или логичного обоснования с точки зрения бизнеса.

- Транзакции клиента с несколькими видами ВА, невзирая на чрезмерные транзакционные сборы, и особенно с ВА повышенной анонимности, такими как криптовалюта повышенной анонимности (КПА, англ.: anonymity-enhanced cryptocurrency - AEC) или конфиденциальные криптомонеты.
- Перевод ВА с открытым прозрачным блокчейном, такого как биткоин, на централизованную биржу, с последующим немедленным обменом его на AEC или на конфиденциальные криптомонеты.
- Клиенты, выполняющие функции незарегистрированного/ нелицензированного ПУВА на веб-сайтах пирингового (peer-to-peer - P2P) обмена, особенно если есть опасения, что клиент обрабатывает большое количество переводов ВА по поручению своего клиента, и взимает со своего клиента более высокие, по сравнению с другими биржами, комиссии за перевод. Использование банковских счетов для проведения этих P2P-транзакций.
- Аномальная транзакционная активность (уровень и объем) по обналичиванию ВА на биржах из кошельков P2P-платформ, без логичного обоснования с точки зрения бизнеса.
- ВА переводится на кошельки или с кошельков, которые ранее демонстрировали картину деятельности с использованием ПУВА, работающих с сервисами миксинга или P2P-платформами.

- Операции с использованием сервисов миксинга, свидетельствующие о намерении скрыть поток незаконных средств между известными адресами кошельков и маркетплейсами даркнета.
- Средства, внесенные либо снятые с адреса или кошелька ВА с непосредственно или косвенно обозначенными связями с известными подозрительными источниками, включая маркетплейсы даркнета, сервисы миксинга, сомнительные сайты гемблинга, незаконную деятельность (например, применение программ-вымогателей) и/или с сообщениями о кражах.
- Использование децентрализованных, некастодиальных аппаратных кошельков, или бумажных кошельков для перемещения ВА через границы.
- На платформу ПУВА входят пользователи, которые зарегистрировали свои доменные имена в Интернете через прокси-серверы или с помощью регистраторов доменных имен (DNS), скрывающих владельцев доменных имен.
- Входящие на платформу ПУВА пользователи используют IP-адрес, относящийся к даркнету или иному подобному программному обеспечению для закрытой связи, включая шифрованную электронную почту и VPN. Транзакции между партнерами с использованием различных средств анонимной шифрованной связи (например, форумы, чаты, мобильные приложения, онлайн-игры и т. д.) в обход ПУВА.
- Большое количество внешне не связанных между собой кошельков ВА, управляемых с одного IP-адреса (или MAC-адреса). Сюда может входить использование подставных кошельков, зарегистрированных на разных пользователей с целью сокрытия их связи между собой.
- Использование ВА с ненадлежащим документированием их технического исполнения, либо ВА, возможно связанных с аферами и другими инструментами реализации мошеннических схем, таких как финансовые пирамиды (Ponzi schemes).
- Получение средств от или отправка средств в ПУВА, в которых процедуры НПК или верификации клиентов (know-your-customer - KYC) явно недостаточны либо вообще отсутствуют.
- Использование киосков и криптобанкоматов:
  - ✓ невзирая на более высокие комиссионные для таких операций, и включая подобные устройства, обычно используемые мулами и жертвами афер; или
  - ✓ в районах высокого риска, обусловленного повышенной криминогенностью.

Само по себе использование криптобанкомата/киоска не является признаком подозрительности. Тем не менее, использование этих технических средств может быть таким признаком, если аппарат установлен в районе высокого риска либо использовался для неоднократных небольших транзакций (либо при наличии других дополнительных факторов).

Пример 5. Использование IP-адреса, связанного с маркетплейсом в даркнете AlphaBay

AlphaBay, крупнейший криминальный рынок даркнета, ликвидированный властями в 2017 году, на протяжении двух лет использовался сотнями тысяч людей для покупки и продажи запрещенных наркотиков, похищенных и поддельных удостоверений личности и устройств доступа, контрафактных товаров, вредоносных программ и других компьютерных хакерских инструментов, огнестрельного оружия и токсичных химикатов. Сайт представлял собой скрытый сервис в сети TOR, позволяющей скрыть местоположение своих базовых серверов, а также личности своих администраторов, модераторов и пользователей. Продавцы на AlphaBay пользовались ВА различных видов. У них насчитывалось около 200000 пользователей, 40000 поставщиков, 250000 листингов. В период с 2015 по 2017 год было проведено сделок с ВА на более чем 1 миллиард долларов США.

В июле 2017 года правительство США при содействии иностранных партнеров уничтожило серверы, на которых размещался рынок AlphaBay, арестовало администратора, и по ордеру на арест, выданному в Восточном округе Калифорнии, изъяло физические и виртуальные активы самого маркетплейса, а также активы, представлявшие собой незаконные доходы от преступного предприятия AlphaBay. После отслеживания операций по переводу ВА из AlphaBay на другие ВА-счета, и идентификации банковских счетов и других материальных активов, контролируемых предполагаемым администратором маркетплейса, федеральные агенты получили ордера на их арест.

Источник: Соединенные Штаты

Пример 6. Использование миксинга - Helix

ПУВА Helix в даркнете оказывал платную услугу миксинга, на протяжении трех лет помогая клиентам скрывать источники и владельцев ВА. Предположительно Helix перевел более 350000 биткоинов, стоимость которых на момент перевода превышала 300 миллионов долларов США. Оператор открыто рекламировал данную услугу как способ сокрытия сделок в даркнете от правоохранительных органов. В феврале 2020 г. лицу, управлявшему Helix, были предъявлены уголовные обвинения, в том числе в сговоре с целью ОД и ведении бизнеса денежных переводов, не имея на то лицензии.

Helix сотрудничал с AlphaBay до ареста этого маркетплейса в даркнете правоохранительными органами в 2017 году.

Источник: Соединенные Штаты

Пример 7. Использование децентрализованного кошелька

Данный пример демонстрирует использование децентрализованного кошелька преступниками для сокрытия источника преступных средств, полученных от незаконного оборота наркотиков. В этом примере преступники осуществили большое количество продаж наркотиков в интернете. Покупку они просили оплачивать не только фиатной валютой, но и ВА (биткоином, ЭКСМО кодами, ЭКСМО чеками).

Преступные средства, полученные в фиатной валюте, конвертировались в ВА с помощью анонимного счета на онлайновой трейдинговой блокчейн-платформе. Затем эти средства в форме ВА конвертировались в обменнике обратно в фиатную валюту, и переводились назад на личные банковские карточные счета преступников. Что касается преступных средств, полученных в виде ВА, то они сначала переводились на принадлежащие преступникам децентрализованные биткоин-кошельки, а затем - на биткоин-кошельки на различных биржах. Это повышает сложность поиска и отслеживания средств. Аналогичным образом, отмытые средства (в ВА) конвертировались обратно в фиат, и затем зачислялись на банковские карточные счета преступника. Преступник был признан виновным и приговорен судом к семи годам лишения свободы и штрафу.

Источник: Российская Федерация

Признаки, относящиеся к отправителям и получателям

14. Этот набор признаков имеет отношение к профилю и необычному поведению отправителя или получателя преступных средств.

Отклонения, наблюдаемые в процессе открытия счета

- Открытие нескольких счетов под разными именами для обхода ограничений ПУВА на торговлю и снятие средств.
- Транзакции с ненадежных IP-адресов, IP-адресов в странах или территориях, находящихся под санкциями или IP-адресов, ранее помеченных в качестве подозрительных.
- Частые попытки открыть счет в одном и том же ПУВА с одного и того же IP-адреса.
- Мерчант или корпоративный пользователь зарегистрировал свой домен в Интернете в стране или территории, отличной от страны его регистрации в качестве юридического лица, или в стране с недостаточно строгой процедурой регистрации доменов.

Отклонения, наблюдаемые в процессе НПК

- Неполные либо недостаточные данные, клиент отклоняет просьбы представить документы KYC или не отвечает на вопросы об источнике средств.
- Отправитель либо получатель не обладает достаточными знаниями либо предоставляет искаженную информацию об операции, источнике средств или отношениях с контрагентом.
- Клиент в ходе процедуры принятия на обслуживание представил поддельные документы или поддельные фотографии и/или удостоверения личности.

Пример 8. Клиент отказывается предоставить данные об источнике средств

ФО (банк) передала СПО в отношении счета одной местной компании. На счете хранились средства, полученные от продажи купонов, на которые можно было приобрести некий продукт (в данном случае биопластик). Средства, часть которых представляли собой ВА, вносили как физические, так и юридические лица. Несмотря на последовавшие просьбы банка, представители владельца счета не предоставили информацию о происхождении средств. Последующий анализ, проведенный властями, показал, что средства, переданные компанией, обнаружили связи с субъектами, имевшими отношение к организованной преступности и к одному мошенническому проекту.

Источник: Италия

Профиль

- Клиент предоставляет идентификационные или учетные реквизиты (например, нестандартный IP-адрес или флэш-куки) другого счета.
- Расхождения между IP-адресами, привязанными к профилю клиента, и IP-адресами, с которых инициируются транзакции.
- Адрес ВА клиента фигурирует на открытых форумах, связанных с незаконной деятельностью.
- Клиент известен правоохранительным органам в связи с его преступным прошлым, по открытой информации.

Пример 9. Профиль клиента не соответствует обычной торговле на крупные суммы ВА

ПУВА (обменник) и ФО (платежная организация) передали в ПФР СПО относительно торговли ВА на большую сумму сразу после открытия счета в обменнике. В частности, владелец счета осуществлял различные сделки купли-продажи ВА на сумму более 180000 евро, что не соответствовало профилю владельца счета (включая его род занятий и размер заработной платы).

Анализ показал, что ВА затем использовались для (i) операций на рынке даркнета; (ii) беттинга в онлайне; (iii) операций с ПУВА, которые не соблюдали требований ПОД/ФТ, или относительно которых ранее проводились расследования ОД на сумму в миллионы долларов; (iv) проведения операций на платформах пиринговых транзакций с ВА; и (v) "миксинга". Владелец счета также использовал различные средства (в частности, денежные переводы, онлайн-банкинг и предоплаченные карты) для вывода в этот период соответствующей суммы средств со своего счета. Полученные владельцем счета средства, как оказалось, поступали от сети физических лиц, которые покупали ВА (биткоин) за наличные и находились в различных странах или территориях Азии и Европы (включая Италию).

Средства поступали как денежными переводами, так и по банковской системе. Он также получал средства на свои предоплаченные карты от лиц в Африке и на Ближнем Востоке, которые, в свою очередь, собирали средства у сограждан, находящихся в Италии и за рубежом. Эти средства затем использовались для онлайнового гемблинга и для трансграничных переводов, а также снимались наличными в банкоматах в Италии.

Источник: Италия

Профиль возможного денежного мула или жертвы аферы

- Судя по всему, отправитель не знаком с технологией ВА и онлайновыми кастодиальными криптокошельками. Эти люди могут быть денежными мулами, завербованными профессиональными отмывателями денег, или превращенными в мулов жертвами мошенников, которых обманом привлекают к переводу преступных доходов, и которые не имеют понятия об их происхождении.
- Клиент, возраст которого значительно превышает средний возраст пользователей платформы, открывает счет и участвует в большом количестве транзакций. Возникает предположение о его возможном использовании в качестве денежного мула ВА или о том, что он является жертвой финансовой эксплуатации пожилых людей.
- Клиент является финансово уязвимым лицом. Таких граждан часто используют в своих целях наркоторговцы.
- Клиент покупает крупную сумму ВА, не соответствующую размерам его состояния либо его финансовому профилю. Это может служить указанием на отмывание денег, на денежного мула либо на жертву аферы.

Пример 10. Жертвы мошенничества становятся мулами

В этих инвестиционных аферах иностранные граждане связывались с пенсионерами и вообще пожилыми людьми по телефону, электронной почте или через социальные сети, и предлагали им инвестиционные возможности в биткоине или других ВА с обещанием огромной прибыли из-за растущей популярности ВА и их роста в цене. Сначала с банковского счета жертвы, с кредитной карты или с помощью других средств на различные платежные сервисы переводились небольшие суммы (во многих случаях не более 250 евро), которые затем оказались в руках преступников. Кроме того, жертвам поручали обменять фиатную валюту на биткоин в биткоинамате и отправить средства в адрес, указанный преступниками.

Жертвы были не сильно подкованы технически, и обычно не разбирались в технологии ВА и в тех инструментах, в которые они фактически делали инвестиции. Преступники также просили жертв установить на своем компьютере приложение для удаленной работы, якобы для корректного перевода средств на определенные счета. Это компрометировало устройства жертв, поскольку давало возможность преступникам осуществлять несанкционированные денежные переводы без ведома жертвы до тех пор, пока она не замечала исчезновение денег со счета. В некоторых случаях преступники фабриковали статьи, в которых известные звёзды, богатые бизнесмены или дикторы новостей пропагандировали инвестиции в ВА, тем самым формируя у жертв чувство доверия к "инвестициям" и их легитимности.

Источник: Финляндия

Иные виды необычного поведения

- Клиент с высокой частотой меняет свои идентификационные данные, включая адреса электронной почты, IP-адреса и финансовую информацию, что также может указывать на завладение данными счета клиента.
- Клиент на протяжении одного дня неоднократно пытается войти в один или несколько ПУВА с разных IP-адресов.
- Информация в полях сообщений ВА указывает на операции, связанные с незаконной деятельностью либо покупкой товаров, таких как запрещенные наркотики или похищенные данные кредитных карт.
- Клиент неоднократно проводит операции с определённым кругом физических лиц, получая при этом значительную прибыль или убытки. Такое поведение может указывать на возможное завладение данными счета и на попытку снятия остатка средств на счетах жертв посредством торговли или применения схемы ОД для сокрытия потоков средств с помощью инфраструктуры ПУВА.

Признаки, относящиеся к источнику средств или капитала

15. Предоставленные странами и территориями практические примеры демонстрируют, что использование ВА часто связано с преступной деятельностью, такой как незаконный оборот наркотиков и психотропных веществ, мошенничество, кражи и вымогательство (включая киберпреступления). Ниже приведены общие признаки, имеющие отношение к источнику средств или капитала, связанному с такой преступной деятельностью:
    - Совершение операций с адресами ВА или банковскими картами, связанными с известными аферами мошенничества, вымогательством или применением программ-вымогателей, с маркетплейсами даркнета и другими незаконными веб-сайтами, с адресами, находящимися под санкциями.
    - Операции с ВА по переводу средств на сервисы или с сервисов онлайн-гемблинга.
    - Использование одной или нескольких кредитных и/или дебетовых карт, привязанных к кошельку ВА, для снятия крупных сумм фиатной валюты (crypto-to-plastic), или когда средства для покупки ВА снимаются с денежных депозитов на кредитные карты.
    - На хищение средств может указывать значительное превышение обычного уровня суммой депозита, сделанного на счет или на адрес ВА, при неизвестном источнике средств, с последующей конвертацией в фиатную валюту.
    - Отсутствие прозрачности либо недостаточность информации о происхождении средств и их собственниках, например, использующих подставные компании, или средств, внесенных в рамках первичного размещения криптомонет (ICO), при возможном отсутствии персональных данных инвесторов, или входящие переводы из онлайновых платежных систем по кредитным/предоплаченным картам с последующим немедленным снятием средств.
    - Средства клиента поступают напрямую из сторонних сервисов миксинга или с миксеров, встроенных в кошельки.
    - Основная часть объема клиентского капитала формируется за счет инвестиций в ВА, в IC0, или в мошеннические ICO и т.д.
    - Капитал клиента в непропорциональных объемах извлекается из ВА, поступивших от сторонних ПУВА, в которых отсутствуют механизмы регулирования ПОД/ФТ.

Пример 11. Использование подставных компаний - Deep Dot Web

В мае 2019 года американские правоохранительные органы по постановлению суда арестовали веб-сайт DeepDotWeb (DDW). Предполагаемым владельцам и операторам DDW были предъявлены обвинения в сговоре с целью ОД на миллионы долларов. Это были откаты за перенаправление физических лиц с сайта DDW на рынки даркнета. Предполагаемые владельцы и операторы DDW получали за реферальные ссылки откатные платежи, представлявшие собой комиссии с выручки от продажи запрещённых товаров, таких как фентанил и героин, приобретенных частными лицами, оказавшимися на маркетплейсе даркнета благодаря ссылкам, размещенным на сайте DDW.

Эти откаты выплачивались в ВА, и поступали в биткоин-кошелек, контролируемый сайтом DDW. Чтобы скрыть характер и источник преступных доходов, размер которых составил более 15 миллионов долларов США, владельцы и операторы сайта переводили преступные откаты со своего биткоин-кошелька DDW на другие биткоин-кошельки, а также на контролируемые ими банковские счета, открытые на подставные компании. Обвиняемые использовали эти подставные компании для перемещения своих преступных доходов и осуществления другой деятельности, относящейся к DDW. За пять лет веб-сайт в виде откатных платежей с рынков даркнета получил около 8155 биткоинов на общую сумму около 8 миллионов долларов США по курсу биткоина на моменты отдельных транзакций. Биткоины серией более чем в 40000 депозитов переводились на контролируемый обвиняемыми биткоин-кошелек DDW, а затем путем проведения более чем 2700 транзакций выводились в различные адреса. Сумма биткоинов на момент снятия средств с биткоин-кошелька DDW составила около 15 миллионов долларов США.

Источник: Соединенные Штаты

Пример 12. Использование нескольких бирж ВА, предоплаченных карт и поддельных удостоверений личности при НПК

Обвиняемые по этому делу предположительно занимались ОД совместно с киберпреступниками, которые взломали биржу ВА, и украли ВА на сумму 250 миллионов долларов США. Двое обвиняемых предположительно отмыли похищенные ВА в сумме около 91 миллиона долларов, плюс ещё 9,5 миллиона долларов от другой кибератаки.

После этого с похищенными ВА были совершены в автоматическом режиме несколько сотен операций, и ВА были пропущены через несколько бирж ВА. В ряде случаев, чтобы обойти процедуры KYC на биржах ВА, преступники использовали поддельные фотографии и поддельные удостоверения личности. В конечном счете около 35 миллионов долларов США этих преступных средств были выведены на счета иностранных банков, а также использованы для покупки предоплаченных карт, которые можно было обменять на ВА. Обвиняемые использовали как независимые, так и связанные счета, и оказывали клиентам услуги перевода ВА, в частности, за отдельную плату конвертировали ВА в фиатную валюту. Обвиняемые также вели бизнес в США, но никогда не регистрировались в Сети по борьбе с финансовыми преступлениями (Financial Crimes Enforcement Network - FinCEN).

Источник: Соединенные Штаты

Признаки, относящиеся к географическим рискам

16. Акцент в данном наборе признаков сделан на том, как преступники, перемещая свои незаконные средства, использовали различия в нормативной базе стран и территорий, находившихся на разных этапах внедрения пересмотренных стандартов ФАТФ по ВА и ПУВА.[3] Как следует из предоставленных странами практических примеров, преступники использовали пробелы в режимах ПОД/ФТ в части ВА и ПУВА, перемещая свои незаконные средства в ПУВА, находящиеся либо оперирующие в странах или территориях, в которых нормы регулирования в области ПОД/ФТ в отношении ВА и ПУВА были минимальными либо вовсе отсутствовали. В этих странах мог отсутствовать режим регистрации/ лицензирования, или на ВА и ПУВА могли не распространяться требования передачи СПО, или отсутствовал полный спектр превентивных мер, как того требуют стандарты ФАТФ. В настоящем отчете не ставится цель определить перечень "высокорисковых" стран и территорий. Тем не менее, сообщающим лицам предлагается при анализе географических рисков принять к сведению нижеследующие признаки. Эти риски относятся к странам и территориям, в которых находится отправитель транзакции, получатель транзакции, а также к транзитным странам и территориям. Признаки также относятся к рискам, связанным с инициатором транзакции или получателем средств, возможно имеющим отношение к стране или территории высокого риска. Кроме того, их можно применить к гражданству клиента, его месту жительства и месту работы.

- Средства клиента происходят с биржи либо отправляются на биржу, которая не зарегистрирована в стране или территории, где находится этот клиент или биржа.
- Клиент использует биржу ВА или зарубежный сервис перевода денег или ценностей (MVTS), находящийся в высокорисковой стране или территории, где отсутствуют или, насколько известно, установлены неадекватные нормативные требования ПОД/ФТ, включая неадекватные меры НПК и KYC, к работающим с ВА структурам.
- Клиент направляет средства ПУВА, работающему в стране или территории, в которой отсутствует регулирование ВА, либо не внедрены механизмы регулирования ПОД/ФТ.
- Клиент организует новые офисы либо перемещает офисы в страны или территории, в которых ВА не регулируются, либо которые не внедрили нормативные акты, регулирующие ВА, или организует новые офисы в странах или территориях в отсутствие четкого обоснования этого шага с точки зрения бизнеса.

3 В июле 2020 года ФАТФ опубликовала "12-месячный обзор пересмотренных стандартов ФАТФ в отношении виртуальных активов и провайдеров услуг в сфере виртуальных активов". Раздел 2 этого отчета описывает ход внедрения пересмотренных стандартов за время с июня 2019 года.

Пример 13. Биткоин-дилер, занимающийся без лицензии деятельностью по переводу денег (трансграничные элементы)

В апреле 2019 года подсудимый получил два года тюрьмы за занятие без лицензии бизнесом по переводу денег. Более чем тысяче клиентов в США он продал ВА (биткоин) на сотни тысяч долларов. Было также принято решение о конфискации у подсудимого прибыли в размере 823357 долларов США.

Подсудимый рекламировал свои услуги на веб-сайтах, предназначенных для пользователей ВА, с некоторыми клиентами встречался лично, чтобы принять наличные деньги в обмен на ВА. Другие клиенты платили ему через банкоматы по всей стране или пользуясь услугами операторов денежных переводов. За свои услуги подсудимый получал пятипроцентное вознаграждение по действующему обменному курсу. Сначала он приобретал биткоины на американской бирже, но, как только его деятельность начала вызывать подозрения и его счет был закрыт, подсудимый переключился на биржу в Азии. На этой бирже подсудимый в период с марта 2015 года по апрель 2017 года, совершив сотни отдельных транзакций, купил биткоинов на 3,29 миллиона долларов США. Подсудимый также признал, что свои американские наличные деньги, предназначавшиеся для обмена, он хранил у дилера драгоценных металлов в сопредельной с США стране. Он также признал, что в период с конца 2016 года по начало 2018 года он и другие лица ввезли в США в общей сложности более 1 миллиона долларов США частями в размере чуть меньше порога отчетности в 10000 долларов США.

Источник: Соединенные Штаты Америки

ПУВА переводит свою деятельность в страну с неадекватными нормами ПОД/ФТ

В преддверии имплементации в 2017 году в азиатской стране "А" политических мер по запрету деятельности ПУВА, один ПУВА (биржа), учрежденный в стране "А", перевел свою деятельность в страну "Б" в том же регионе. В 2018 году после знаковых взломов ряда крупных ПУВА (бирж) страна "Б" ужесточила свой нормативно-правовой режим ПОД/ФТ в отношении ВА. В марте 2018 года ПУВА объявил о своих намерениях перенести свою штаб-квартиру в страну "В" в Европе (на тот момент эта европейская страна еще не ввела полномасштабный режим ПОД/ФТ в отношении ВА и ПУВА). Позднее, в ноябре 2018 года, страна "В" ввела определенные нормы в отношении ПУВА, а в феврале 2020 года она подтвердила невыдачу разрешения на работу фигурирующего в данном примере ПУВА. В опубликованных позднее в 2020 году сообщениях указывалось, что ПУВА уже перенес свою регистрацию и статус юридического лица в страну "Г" в Африке.

Источник: Открытая информация

Заключение

17. Настоящий Отчет составлен на основе материалов, полученных от членов ФАТФ по всей глобальной сети. Он призван стать практическим пособием как для государственного, так и для частного сектора в поиске, выявлении и, в конечном счете, предупреждении преступной деятельности по ОД и ФТ с применением ВА.

18. Фигурирующие в настоящем Отчете признаки специфичны для особенностей и уязвимостей, присущих конкретно ВА. Они не являются исчерпывающими и не годятся для применения в любой ситуации. Эти признаки нередко являются лишь одним из многих элементов, составляющих более широкую общую картину потенциального риска ОД или ФТ. Важно, чтобы эти признаки (или любой отдельный признак) не рассматривались изолированно. Они должны быть увязаны с информацией, полученной от соответствующих органов власти.

19. Риск-ориентированный подход, осуществляемый на основе регулярного и активного двустороннего диалога государственного и частного секторов, несомненно, повысит отдачу от настоящего Отчета. Вот почему компетентным органам рекомендуется распространить настоящий Отчёт среди сообщающих лиц, и проводить с ними партнерские встречи и информационно-пропагандистские мероприятия в целях оказания содействия осмыслению ими настоящего Отчета.

20. Поскольку представленные признаки постоянно изменяются, их лучше всего использовать совместно с другой контекстуальной информацией национальных правоохранительных органов и открытых источников. Наиболее характерные для данной страны или территории признаки и сведения частному сектору могут предоставлять также и компетентные органы. При подготовке их рекомендаций соответствующим сообщающим лицам можно, к примеру, использовать информацию настоящего Отчета. Однако настоящий Отчет не подлежит использованию в качестве инструмента регулирования для целей комплаенса или надзорных проверок, или в качестве контрольного перечня при осуществлении надзора над организациями частного сектора, поскольку не все показатели одинаково применимы ко всем странам и территориям и ко всем организациям.

Ссылки

ФАТФ (Июнь 2014), ОТЧЁТ ФАТФ Ключевые определения и потенциальные риски в сфере ПОД/ФТ

ФАТФ (Июнь 2019), Руководство ФАТФ по применению риск-ориентированного подхода к виртуальным активам и провайдерам услуг виртуальных активов

ФАТФ (Июнь 2020), 12-месячный обзор пересмотренных стандартов ФАТФ в отношении виртуальных активов и провайдеров услуг в сфере виртуальных активов

Отчёты только для членов ФАТФ

ФАТФ (Июнь 2016), Конфиденциальный Отчет ФАТФ о выявлении показателей риска финансирования террористов

ФАТФ (Июнь 2019), Конфиденциальный Отчет ФАТФ о финансовых расследованиях в отношении виртуальных активов

http://www.fatf-gafi.org

Сентябрь 2020

Виртуальные активы - Признаки отмывания денег и финансирования террористов

Виртуальные активы и связанные с ними услуги могут стимулировать финансовую инновацию, однако их особенности создают и новые возможности для лиц, занимающихся отмыванием денег, финансирующих террористов и других преступников, по отмыванию преступных доходов и финансированию своей преступной деятельности.

ФАТФ подготовила данный короткий отчет о признаках подозрительной деятельности с виртуальными активами в помощь сообщающим лицам, включая финансовые организации, установленные нефинансовые предприятия и профессии, и провайдеров услуг в сфере виртуальных активов, в выявлении и передаче сообщений о возможной деятельности по отмыванию денег и финансированию терроризма с использованием виртуальных активов.