UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Июнь 2014

Издание подготовлено при финансовой поддержке Бюро по международной правоохранительной деятельности и наркотикам Госдепартамента США. Изложенные в нем мнения, выводы и рекомендации принадлежат авторам и не обязательно совпадают со взглядами Государственного департамента США.

* * *

Настоящее издание официально не редактировалось. Титульный фотоснимок: Антуанетта Петрова.

1 Введение

Являясь гарантом Конвенций ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ, против транснациональной организованной преступности и против коррупции, Управление ООН по наркотикам и преступности (УНП ООН) обладает значительными сравнительными преимуществами для оказания помощи в сфере борьбы с отмыванием денег и в вопросах конфискации активов. Мандат УНП ООН в этих областях был усилен резолюцией ЭКОСОС №2004/29, в которой четко определено, что УНП ООН следует «продолжать свою работу в сфере борьбы с отмыванием денег при наличии внебюджетных ресурсов и в сотрудничестве с соответствующими региональными и международными организациями, участвующих в деятельности по имплементации соответствующих международных инструментов и стандартов по борьбе с отмыванием денег путем предоставления по просьбе государств-участниц обучения, консультативной и долгосрочной технической помощи».

В 2012 г. по запросу Секретариата ГУАМ и при финансовой поддержке Бюро по международной правоохранительной деятельности и наркотикам Госдепартамента США Региональное представительство в Центральной Азии Управления ООН по наркотикам и преступности приступило к реализации проекта «Укрепление потенциала стран-участниц ГУАМ в сфере сотрудничества на национальном и региональном уровнях в вопросах противодействия отмыванию денег, а также ареста и конфискации доходов, полученных преступным путем». Проект нацелен на поощрение регионального подхода в борьбе с отмыванием денег в станах ГУАМ (Грузия, Украина, Азербайджан и Молдова) и одновременно с этим на укрепление межведомственного сотрудничества этих стран на национальном уровне.

Целью данного пособия, подготовленного в рамках вышеупомянутого проекта, является предоставление следователям и прокурорам практической информации по выявлению, расследованию, уголовному преследованию отмывания денег, совершенного посредством виртуальных валют, а также по аресту таких валют.

2 Выражение признательности

Авторы хотели бы выразить благодарность всем, кто внес свой вклад, делился советами и предоставлял отзывы при подготовке настоящего пособия.

Пособие было разработано под техническим руководством Глобальной программы по борьбе с отмыванием денег, преступных доходов и финансированием терроризма (GPML) и Глобальной программы по борьбе с киберпреступностью, УНП ООН.

Экспертная работа проведена консультантами УНП ООН Дэвидом О'Райли, Георгием Джохадзе и Евгением Уманцем.

Свой вклад также внесли представители стран-участниц ГУАМ.

3 Содержание

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Модуль 1
Знакомство с виртуальными валютами

1 Краткое изложение

Цель данного модуля – представить общий обзор истории возникновения и концепций электронных денег и виртуальных валют. Содержащаяся в этом модуле информация представляет собой важный справочный материал, являющийся основой для всех последующих модулей.

Для понимания генезиса виртуальных валют в этом модуле приводиться краткая историческая ретроспектива, в том числе описываются некоторые из самых известных примеров виртуальных валют и виртуальных валютных бирж. Кроме того, дается толкование ключевых терминов, использующихся в последующих модулях, и приводятся другие важные правовые определения. Установление четких понятий помогает правильно определить границы исследования, а также предотвратить недопонимание и путаницу. Далее следует описание некоторых из наиболее распространенных типов электронных денег и виртуальных валют, включая категоризацию виртуальных валют.

С точки зрения следствия очень важно понимать взаимосвязи между электронными деньгами, виртуальными валютами и традиционной финансовой системой. В данном модуле обсуждаются некоторые из наиболее типичных взаимосвязей, а также дается характеристика текущего правового регулирования виртуальных валют. Модуль дополнен рядом практических примеров. При этом особое внимание уделяется bitcoin как виртуальной валюте, характеризующейся большой популярностью и специфическими трудностями, связанными с используемой в ней технологией.

2 Цели обучения

По окончанию данного модуля Вы будете:

- Знать ключевые термины в области электронных денег и виртуальных валют.
- Знать основные виды электронных денег и виртуальных валют.
- Понимать интерфейс между виртуальными валютами и традиционной финансовой системой.
- Знать о текущем состоянии правового регулирования электронных денег и виртуальных валют.
- Познакомитесь с bitcoin как примером криптовалют, а также принципами его функционирования.

3 История виртуальных валют

Концепция виртуальной валюты не является новинкой, о чем свидетельствуют многочисленные примеры появившихся и уже исчезнувших за последнее десятилетие виртуальных валют. В этом разделе дается краткий обзор некоторых из самых известных виртуальных валют и бирж виртуальных валют.

Одной из первых популярных виртуальных валют была E-Gold. Появившаяся в 1996 году[1], E-Gold позволяла пользователям открывать счета в единицах, выраженных в граммах золота (или других драгоценных металлах), с возможностью совершать мгновенные переводы на другие счета E-Gold. Как сообщается, в 2005 году число пользователей E-Gold достигло 2,5 млн. человек, а ежедневный оборот составил 6,3 млн. дол. США. В 2007 году судом присяжных США руководители E-Gold былы признаны виновными в отмывании денег, преступном сговоре и ведении нелицензионной деятельности по переводу денег, что в конечном итоге привело к ликвидации E-Gold[2, 3]. E-Gold спровоцировала появление целого ряда подобных систем, таких как адрес e-Bullion.com, Pecunix.com и др.

Созданная в 1998 году и демонстрирующая впечатляющую динамику роста, WebMoney на момент подготовки данного пособия насчитывала почти 25 млн. пользователей[4]. WebMoney предоставляет своим пользователям возможность контролировать имущественные права на ценности (активы), которые хранятся другими участниками системы (известными как гаранты)[5].

Созданная в 2006 году и просуществовавшая до 2013 года, Liberty Reserve позволяла пользователям регистрироваться и переводить другим пользователям активы, требуя для этого только имя, адрес электронной почты и дату рождения. При этом никакие мероприятия по проверке личности пользователей не проводились. В 2013 году Министерство юстиции США официально обвинило Liberty Reserve в ведении незарегистрированной деятельности по переводу денег и отмывании преступных доходов на сумму более $6 млрд.[6].

Сеть Bitcoin является децентрализованной пиринговой платежной системой, не имеющей центрального органа или посредников,

---

[1] «Федералы обвиняют E-Gold в пособничестве кибер-преступникам», NBC News, Май 2007. (Источник: http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-e-gold-of-helping-cybercrooks)

[2] «Фирма, оперирующая интернет валютой, признается виновной в отмывании денег», The Industry Standard, Июль 2008. (Источник: http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering)

[3] http://en.wikipedia.org/wiki/E-gold

[4] http://www.wmtransfer.com/eng/about/statistics/index.shtml, статистика WebMoney состоянием на апрель 2014.

[5] http://en.wikipedia.org/wiki/WebMoney

[6] «‘Банк черного рынка’ обвиняется в отмывании преступных доходов на $6 млрд.», ABC News, Май 2013. (Источник: http://abcnews.go.com/US/black-market-bank-accused-laundering-6b-criminal-proceeds/story?id=19275887)

функционирование которой обеспечивается ее же пользователями. В 2009 году Сатоши Накамото опубликовал первую спецификацию Bitcoin вместе с описанием концепции криптографической защиты для списка рассылки[7]. С этого времени ценность bitcoin резко возросла, начиная с примерно 0,3 дол. США в 2011 году, достигнув 1135 дол. США в 2013 году[8]. Принципы работы сети Bitcoin подробно рассматриваются в примере, приведенном далее.

4 Определения терминов

Дать определение терминам важно для предотвращения непреднамеренной путаницы. Это особенно важно в области виртуальных валют, где существуют многочисленные близкие по значению часто употребляемые термины, такие как электронные деньги[9], виртуальная валюта[10, 11, 12, 13, 14,15] и криптовалюта[16]. Эти термины, иногда частично совпадающие, иногда противоречащие друг другу, отличаются и по содержанию, и по предмету. На самом деле вопрос о том, соответствуют ли определения виртуальной валюты и электронной валюты определению валюты или их все же следует рассматривать как товар, в настоящее время еще дискутируется[17, 18, 19].

---

[7] https://bitcoin.org/en/faq
[8] http://bitcoincharts.com/
[9] http://ec.europa.eu/internal_market/payments/emoney/index_en.htm
[10] http://en.wikipedia.org/wiki/Virtual_currency
[11] «Руководство: Применение Положения FinCEN для лиц, управляющих, осуществляющих обмен или использующих виртуальные валюты», Руководство FinCEN FIN-2013-G001, Март 2013. (Источник: http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html)
[12] «ЕБА предупреждает пользователей виртуальных валют», Европейская Банковская Администрация, Декабрь 2013. (Источник: http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies)
[13] «Схемы с использованием виртуальных валют», Европейский Центральный Банк, Октябрь 2012. (Источник: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf)
[14] «Виртуальные Экономика и Валюты – Дополнительное руководство Службы внутренних доходов США поможет снизить риски несоблюдения налогового законодательства», Управление правительственной отчетности США, Май 2013. (Источник: http://www.gao.gov/assets/660/654620.pdf)
[15] «Переосмысление электронных валют», Yankee Group, Май 2013. (Источник: http://info.tapjoy.com/wp-content/uploads/sites/4/2013/05/RedefiningVirtualCurrency_WhitePaper-1MAY2013-v1.pdf)
[16] http://www.investopedia.com/terms/c/cryptocurrency.asp
[17] «Bitcoin будет рассматриваться в Финляндии как товар, не сумев пройти проверку на деньги», Bloomberg, Январь 2014. (Источник: http://www.bloomberg.com/news/2014-01-19/bitcoin-becomes-commodity-in-finland-after-failing-currency-test.html)
[18] Извещение Службы внутренних доходов 2014-21. (Источник: http://www.irs.gov/pub/irs-drop/n-14-21.pdf)
[19] «Bitcoin становиться предметом искусства после отказа Швеции от креативной валюты», Bloomberg, Январь 2014. (Источник: http://www.bloomberg.com/news/2014-01-21/bitcoin-becomes-art-as-swedish-taxman-rejects-creative-currency.html)

Для целей данного пособия будут использоваться определения терминов и классификация виртуальных валют, предложенная ФАТФ [20]. Эти определения приведены в следующих главах.

4.1 Определения ФАТФ

4.1.1 Виртуальная валюта

«Виртуальная валюта представляет собой цифровое выражение стоимости, которым можно торговать в цифровой форме и которое функционирует в качестве (1) средства обмена; и/или (2) расчётной денежной единицы; и/или (3) средства хранения стоимости, но не обладает статусом законного платёжного средства ни в одной юрисдикции».

Для целей этого определения под «цифровым выражением» понимается выражение чего-либо в виде цифровых данных. Физический объект, например, флэш-накопитель или bitcoin может содержать цифровое выражение виртуальной валюты, но, в конечном счете, такая виртуальная валюта как таковая функционирует только тогда, когда она цифровым способом, через Интернет, связана с системой виртуальной валюты.

Принципиальным моментом в термине «цифровое выражение» является то, что значение имеют сами цифровые данные, т.е. виртуальная валюта, а не носитель, на котором они хранятся. Цифровое выражение виртуальной валюты можно пересылать, копировать или переместить на другой носитель, при этом ценность виртуальной валюты обуславливается ее цифровым выражением.

Виртуальную валюту следует отличать от фиатных валют (они же «реальные валюты», «реальные деньги» или «национальные валюты»), которыми являются деньги в монетной и бумажной форме страны, признающей их законным платежным средством. Фиатные деньги обращаются, принимаются и используются в качестве средства расчетов в эмитирующей их стране.

4.1.2 Электронные деньги / е-деньги

«Ее [виртуальную валюту] следует отличать от электронных денег, которые являются цифровым выражением фиатной валюты и используются для электронного перевода стоимости, выраженной в фиатной валюте. Электронные деньги представляют собой механизм цифрового перевода фиатной валюты, т.е. они используются для электронного перевода валюты, обладающей статусом законного платежного средства».

[20] Отчет ФАТФ «Виртуальные валюты – ключевые определения и потенциальные риски в сфере ПОД/ФТ», ФАТФ/ОЭСР, Июнь 2014. (Источник: http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html)

Виртуальные валюты не имеют статуса законного средства платежа в какой-либо юрисдикции. Гипотетически и практически возможно создать цифровое выражение фиатной валюты. Но, согласно определению, это не будет являться виртуальной валютой. В связи с этим для обозначения цифрового выражения фиатной валюты используется термин «электронные деньги».

4.1.3 Цифровая валюта

«Цифровая валюта может выступать цифровым выражением как виртуальной валюты (нефиатной валюты), так и электронных денег (фиатной валюты) ...»

Используя понятие цифрового выражения стоимости, приходится сталкиваться со специфическими сложностями. Некоторые из них присущи виртуальным валютам, некоторые – электронным деньгам. Например, в случае с виртуальными валютами возникают определенные вопросы, связанные с конвертацией фиатной валюты в виртуальную. Это едва ли является вопросом для электронных денег, которые по определению уже являются формой фиатной валюты.

Тем не менее, возможны ситуации, когда не имеет значение, является ли цифровое выражение стоимости законным платежным средством в какой-нибудь стране. К примеру, проблему «двойной траты» необходимо решать в любом случае. Двойная трата – это ситуация, когда цифровое выражение стоимости используется (тратится) более одного раза. Очевидно, что это является серьезной проблемой для любой системы перевода стоимости и не зависит от того, являются цифровые данные фиатными или нефиатными валютами.

Термин цифровая валюта охватывает оба приведенных выше понятия, и таким образом, предоставляет собой термин, подразумевающий как фиатные, так и не фиатные валюты.

5 Классификация виртуальных валют

Предложенная ниже классификация заимствована у ФАТФ[21], согласно которой виртуальные валюты классифицируются в зависимости от того:

1. Могут ли они конвертироваться в фиатные валюты и обратно (конвертируемые или неконвертируемые).

2. Существует ли центральный администратор виртуальной валюты (централизованные или распределенные).

Более подробно эта классификация, а также некоторые другие связанные с этим вопросы рассматриваются в последующих главах. Безусловно, существуют также и другие классификации[22].

5.1 Конвертируемые и неконвертируемые виртуальные валюты

«Конвертируемая (или открытая) виртуальная валюта обладает эквивалентной стоимостью в реальной валюте и может обмениваться на реальную валюту и обратно. Примерами конвертируемой виртуальной валюты являются: Bitcoin; e-Gold (более несуществующая), Liberty Reserve (более несуществующая), Second Life Linden Dollars и WebMoney».

«Неконвертируемая (или закрытая) виртуальная валюта предназначена для использования в конкретных виртуальных сферах или мирах, таких, как глобальные многопользовательские онлайновые ролевые игры (MMORPG) или Amazon, и которая по правилам, регулирующим её использование, не может быть обменена на фиатную валюту. Примерами неконвертируемой виртуальной валюты являются: Project Entropia Dollars[23]; Q Coins; и World of Warcraft Gold».

Суть первой классификации виртуальных валют состоит в том, могут ли они быть конвертированы в фиатные валюты и обратно. Виртуальная валюта, которую можно обменять на фиатную, называется конвертируемой или открытой виртуальной валютой. Виртуальная валюта, которую нельзя обменять на фиатную, называется неконвертируемой или закрытой виртуальной валютой.

---

[21] Отчет ФАТФ «Виртуальные валюты – ключевые определения и потенциальные риски в сфере ПОД/ФТ», ФАТФ/ОЭСР, Июнь 2014. (Источник: http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html)

[22] «Схемы с использованием виртуальных валют», Европейский Центральный Банк, Октябрь 2012. (Источник: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf)

[23] Несмотря на предложенное ФАТФ определение, следует отметить, что доллары Project Entropia на самом деле могут быть обменены на фиатные деньги. Следовательно, они являются конвертируемой валютой (https://account.entropiauniverse.com/account/withdrawals/index.xml?).

Но, как отмечается в отчете ФАТФ, нельзя исключать возникновение неофициального, вторичного «черного» рынка, на котором неконвертируемую и используемую только в пределах определенной виртуальной среды валюту можно обменять на фиатную или иную виртуальную валюту[24]. По этой причине классификация виртуальных валют на конвертируемые и неконвертируемые имеет для правоохранительных и следственных целей весьма ограниченную ценность. И напротив, классификация в зависимости от того, являются ли виртуальные валюты централизованными или децентрализованными, представляется как та, что имеет большую практическую ценность. Это классификация рассматривается в следующей главе.

5.2 Централизованные и децентрализованные виртуальные валюты

Вторая классификация виртуальных валют заключается в том, имеет ли система виртуальной валюты центрального администратора. Виртуальная валюта, имеющая центрального администратора, называется централизованной. Виртуальная валюта, не имеющая центрального администратора, называется децентрализованной.

Все неконвертируемые виртуальные валюты являются централизованными: по определению они эмитируются центральным администратором, который устанавливает правила, ограничивающие их конвертацию. В отличие от неконвертируемых виртуальных валют, конвертируемые виртуальные валюты подразделяются на два подтипа: централизованные и децентрализованные.

«В системах централизованных виртуальных валют имеется единый администратор, т.е. третья сторона, которая контролирует систему. Администратор эмитирует валюту, устанавливает правила её использования, ведёт централизованный реестр платежей и имеет право изымать валюту из обращения. Обменный курс конвертируемой виртуальной валюты может быть либо плавающим, т.е. определяться рыночным предложением и спросом на виртуальную валюту, либо фиксированным, т.е. привязанным администратором к заданной величине в фиатной валюте или в других ценностях, используемых в «реальном мире», таких, как золото или валютная корзина. В настоящее время в подавляющем большинстве платежных операций в виртуальной валюте используются именно централизованные виртуальные валюты. Примерами таких валют являются: E-Gold (более несуществующая), Liberty Reserve dollars/euros (более несуществующая), Second Life Linden Dollars, PerfectMoney, WM-units WebMoney и World of Warcraft Gold.

Третьей стороной в контексте данной классификации является физическое или юридическое лицо, которое участвует в операции, но не является ее стороной и не связано с двумя другими участниками операции. Другими

[24] «Виртуальная валюта требует новых жестких правил», China View, Февраль 2012. (Источник: http://news.xinhuanet.com/english/2007-02/12/content_5730970.htm)

словами, третье лицо выступает нейтральной стороной между участниками сделки или финансовой транзакции.

«Децентрализованные виртуальные валюты (также называемые криптовалютами) являются распределенными, основанными на математических принципах пиринговыми виртуальными валютами с открытым исходным кодом, у которых нет центрального администратора и отсутствует централизованный контроль или надзор. Примерами являются: Bitcoin, LiteCoin и Ripple».

Наиболее ярким примером децентрализованной виртуальной валюты является bitcoin, хотя существуют и другие. В основе функционирования децентрализованных виртуальных валют лежит пиринговая сеть, посредством которой осуществляется управление транзакциями. Информация о передаче прав собственности распространяется через сеть способом, обеспечивающим по прошествию короткого периода времени, в течение которого происходит подтверждение транзакций, безопасность и целостность передачи стоимости.

Пример: Linden Dollars

Second Life представляет собой виртуальный мир в реальном времени, разработанный компанией Linden Lab.[25] Пользователи взаимодействуют с Second Life через установленное на компьютере приложение, которое позволяет им подключаться и исследовать виртуальный мир. В этом виртуальном мире есть своя внутренняя экономика и внутренняя валюта, известная как Linden Dollars. Linden Dollars могут использоваться для покупки, продажи, аренды или торговли землей, товарами или услугами с другими пользователями.

Исходя из приведенной в разделе 5 классификации, Linden Dollars являются конвертируемой централизованной виртуальной валютой, что и будет продемонстрировано далее.

Конвертируемая виртуальная валюта

Linden Dollars можно приобрести как в виртуальном мире Second Life, так и на онлайновой обменной площадке LindX[26] или через другие обменники виртуальных валют.

Linden Dollars можно приобрести через обменник Linden при помощи кредитной карты или PayPal[27]. В других обменниках возможны и другие способы оплаты, такие как банковские переводы[28] или

25 http://secondlife.com/whatis/
26 http://community.secondlife.com/t5/English-Knowledge-Base/Buying-and-selling-Linden-dollars/ta-p/700107
27 http://community.secondlife.com/t5/English-Knowledge-Base/Billing/ta-p/700037#Section_.3
28 https://www.virwox.com/help.php

посредством bitcoin[29], [30]. На бирже виртуальных валют Linden Dollars могут обмениваться на другие виртуальные или фиатные валюты.

Централизованная виртуальная валюта

Linden Lab устанавливает условия использования Linden Dollars и является администратором для этой виртуальной валюты. В пользовательском соглашении Linden Lab указывает, что ее доллары не являются реальной валютой или другим финансовым инструментом, не имеют реальной стоимости и не могут обращаться вне виртуального мира Linden Lab[31]. В практике имеется ряд показательных случаев, когда решения Linden Labs относительно политики обращения ее виртуальной валюты оказывали существенное влияние на стоимость Linden Dollars[32].

Пример: World of Warcraft Gold

World of Warcraft является глобальной многопользовательской онлайновой ролевой игрой (MMORPG), созданной компанией Blizzard Entertainment[33]. Игроки управляют героем, который исследует мир, сражается с монстрами, ведет поиски и прочее. Игроки, используя виртуальное золото, могут приобрести различные виртуальные товары. Золото можно заработать в игре, выполняя квесты, но есть и другие способы.

Согласно предложенной в разделе 5 классификации золото World of Warcraft является неконвертируемой централизованной виртуальной валютой, что и будет продемонстрировано далее.

Неконвертируемая виртуальная валюта

В связи с тем, что третьи лица нередко предлагают возможности по покупке Gold of World of Warcraft, которое зачастую украдено со взломанных эккаунтов пользователей или получено иным способом, нарушающим политику его использования, компания Blizzard Entertainment активно агитирует пользователей World Of Warcraft отказываться от покупки золота у третьих лиц[34], [35]. Компания проводит мероприятия по повышению осведомленности пользователей и применяет санкции в отношении тех пользователей, кто использует золото, приобретенное у третьих лиц. Такие санкции

29 http://www.crossworldsxchange.com/buy_L$_bitcoins.htm
30 https://en.bitcoin.it/wiki/VirWoX
31 http://lindenlab.com/tos. В частности, Раздел_4.5 и 9.2.
32 http://en.wikipedia.org/wiki/Economy_of_Second_Life#Acts_of_Linden
33 http://us.battle.net/wow/en/
34 http://eu.battle.net/wow/en/shop/anti-gold/
35 http://us.battle.net/wow/en/blog/3768752

могут предусматривать полное отключение от виртуального мира World Of Warcraft[36].

Но, несмотря на эти меры, неофициальная, вторичная торговля золотом World Of Warcraft существует и активно развивается[37]. Как отмечалось в главе 5.1, факт существования вторичной торговли золотом World Of Warcraft означает то, что это золото *де-факто* является конвертируемой виртуальной валютой. Хотя, в соответствии с определением ФАТФ, это золото относится к категории неконвертируемых виртуальных валют.

Централизованная виртуальная валюта

Blizzard Entertainment устанавливает условия использования золота World Of Warcraft и выступает администратором этой виртуальной валюты[38]. В частности, соглашаясь с условиями использования:

«Вы соглашаетесь с тем, что Вы не имеете прав собственности на любой такой контент, в том числе, не ограничиваясь виртуальными товарами или валютой, которые аккумулируются или приобретаются в ходе игры, или на любые другие атрибуты, связанные с любой учетной записью. Blizzard не признает никакие намеренные операции с виртуальной собственностью, совершенные вне игры, или намеренную продажу, дарение или торговлю в «реальном мире» всего, что появляется или приобретается в игре. Соответственно, Вы не можете продавать виртуальные предметы игры или виртуальные валюту за «реальные» деньги или обменивать эти предметы или валюту на ценности вне игры.» [39]

[36] http://us.battle.net/en/security/theft#gold
[37] http://www.wikihow.com/Safely-Buy-Gold-in-World-of-Warcraft
[38] http://us.blizzard.com/en-us/company/legal/wow_tou.html
[39] http://us.blizzard.com/en-us/company/legal/wow_tou.html(Раздел 8)

6 Интерфейс между виртуальными валютами и традиционной финансовой системой

Для целей данного пособия важно понимать, какой интерфейс существует между виртуальными валютами и традиционной финансовой системой.

Как уже упоминалось ранее, существуют вторичные рынки неконвертируемых виртуальных валют. Основным источником неконвертируемой валюты является центральный администратор виртуальной валюты. Вторичные рынки неконвертируемых валют, такие как Интернет-аукционы, могут принимать различные способы оплаты (источники финансирования), в том числе конвертируемые виртуальные валюты.

Внимание данного раздела, однако, сконцентрировано на первичной покупке конвертируемых виртуальных валют. Иными словами, на способах конвертации фиатных валют, товаров, услуги или других форм ценности в виртуальные валюты.

6.1 Биржи виртуальных валют

Торги конвертируемыми виртуальными валютами обычно происходят на биржах виртуальных валют, предлагающие разный валютный курс для разных валют. Для оплаты биржевых услуг используется сочетание фиксированной платы и комиссионного процента. Дополнительная плата может взиматься за депонирование и/или снятие средств со счета в виртуальной валюте. Существуют различные источники и способы перевода средств биржам виртуальных валют и, среди прочего:

- Другие виртуальные валюты[40], [41], [42].
- Банковский перевод[43], [44], [45]
- Денежный перевод[46]
- Платежная карта[47]
- Наличные[48], [49]
- PayPal[50]

Существуют и другие инновационные модели, которые не обязательно предполагают возможность свободной покупки-продажи виртуальной валюты, а скорее просто облегчают покупку виртуальной валюты

[40] https://firstmetaexchange.com/home
[41] https://www.virwox.com/?stage=1
[42] http://howtobuybitcoins.info/
[43] https://www.bitstamp.net/help/how-to-buy/
[44] http://portal.bitcoinschile.cl/
[45] https://www.bitcoin.de/
[46] https://www.coinmama.com/
[47] http://btc-dealer.com/
[48] http://www.tradebitcoin.com/
[49] https://localbitcoins.com/
[50] https://www.virwox.com/?stage=1

нетрадиционными способами. Одним из таких примеров является покупка bitcoin по SMS[51].

Учитывая относительную неурегулированность рынка виртуальных валют, существует риск того, что биржи виртуальных валют не идентифицируют должным образом источник происхождения наличных денежных средств или другие источники финансирования, использующиеся для покупки виртуальных валют[52]. Совсем недавно несколько стран объявили о своих планах урегулировать деятельность посредников виртуальных валют, таких как биржи виртуальных валют, с целю снижения рисков отмывания денег[53], [54], [55].

6.2 Финансовые учреждения

Как уже упоминалось в главе 6.1, банковский счет может использоваться для приобретения виртуальной валюты или для зачисления фиатных денег, полученных от реализации виртуальных валют. Это значит, что все типичные меры регулирования и надзора, используемые в отношении банковских счетов, будут применяться и в данном случае. Однако, как указывается в некоторых источниках, использование денежных мулов для отмывания преступных доходов в сети Интернет с помощью различных методов и средств, в том числе посредством виртуальных валют, представляет собой серьезную угрозу[56], [57].

Кроме того с целью хранения и/или перевода фиатной валюты сами по себе биржи виртуальных валют также взаимодействуют с финансовой системой.

---

[51] http://sms.btc-sm.com/

[52] Отчет ФАТФ «Виртуальные валюты – ключевые определения и потенциальные риски в сфере ПОД/ФТ», стр.9, ФАТФ/ОЭСР, Июнь 2014 (Источник: http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html)

[53] «Сингапур намерен регулировать биржи виртуальных валют», BBC News, Март 2014. (Источник: http://www.bbc.co.uk/news/business-26556523)

[54] «Нью-йоркский регулятор планирует регулировать биржу Bitcoin», BBC News, Март 2014. (Источник: http://www.bbc.co.uk/news/technology-26538378)

[55] «Конвертируемые виртуальные валюты (как Bitcoin) подпадают под положения законодательства США о противодействии отмыванию денег», Digital Passing, Март 2013. (Источник: http://www.digitalpassing.com/2013/03/22/convertible-virtual-currency-bitcoin-money-laundering-rules/)

[56] «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», Международного проекта Совета Европы по борьбе с киберпреступностью и МАНИВЕЛ, Март 2012. (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

[57] «Отмывание денег посредством новых способов платежей», ФАТФ-ГАФИ, Октябрь 2010. (Источник: http://www.fatf-gafi.org/media/fatf/documents/reports/ML using New Payment Methods.pdf)

Юридические и регулятивные последствия этого факта демонстрируют пока еще свое становление [58], [59], [60].

6.3 Наличные деньги / банкоматы

Использование наличных денежных средств всегда было привлекательным для целей отмывания преступных доходов. А значит, интерфейс между виртуальными валютами и наличными деньгами заслуживает пристального внимания.

Осведомленность о виртуальных валютах и их популярность в последние годы существенно возросла, особенно с появлением Bitcoin. С ростом популярности этой виртуальной валюты появились и новые модели, которые предлагают возможности, ранее не доступные с другими виртуальными валютами. Например, в ряде стран существуют Bitcoin-банкоматы[61]. Такие банкоматы делают возможным покупку и продажу bitcoin за наличные[62], [63].

Обмен виртуальных валют на наличные деньги возможен и при личном контакте[64], [65].

6.4 Платежные карты

За последнее десятилетие динамика использования платежных, в частности, дебетовых и предоплаченных карт во всем мире ежегодно демонстрировала в процентом выражении двузначные цифры. [66] Предоплаченные карты предоставляют собой альтернативу различным традиционным банковским продуктам и услугам, таким как дебетовые или кредитные карты, или дорожные чеки. [67] Платежные карты могут использоваться как для проведения оплаты, так и для получения оплаты от третьих лиц, в схемах трансграничных денежных переводов и т.д.

---

[58] «Жаман Мидзухо в США, Канада судится из-за потерь bitcoin на Mt.Gox», Reuters, Март 2014. (Источник: http://www.reuters.com/article/2014/03/16/us-bitcoin-mtgox-mizuho-idUSBREA2E01V20140316)

[59] «В судебную тяжбу по делу Mt.Gox в США и Канаде вовлечен японский Mizuho Bank, обвиняемый в мошенничестве", Arstechnica, Март 2014. (Источник: http://arstechnica.com/tech-policy/2014/03/mtgox-class-action-suits-in-us-and-canada-allege-fraud-drag-in-japans-mizuho-bank/)

[60] «Китай запрещает финансовым компаниям проводить сделки с bitcoin», Bloomberg News, Декабрь 2013. (Источник: http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html)

[61] http://bitcoinatmmap.com/

[62] https://bitcoinatm.com/

[63] https://robocoinkiosk.com/

[64] http://www.tradebitcoin.com/

[65] https://localbitcoins.com/

[66] «Расширение возможностей дебетовых и предоплаченных карт», Euromonitor International, Февраль 2013. (Источник: http://www.euromonitor.com/expanding-opportunities-in-debit-and-pre-paid-card-products/report)

[67] «Отчет о новых способах платежей», ФАТФ-ГАФИ, 2006. (Источник: http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf)

Предоплаченные карты могут использоваться абсолютно анонимно. На практике некоторые эмитенты привлекают потенциальных клиентов именно анонимными предоплаченными картами с отсутствием или высоким лимитом по сумме и количеству операций[68].

6.5 Провайдеры денежных переводов

Предыдущее исследование по изучению криминальных денежных потоков в сети Интернете свидетельствует о том, что использование провайдеров денежных переводов является наиболее распространенной техникой отмывания криминальных денег, полученных вследствие совершения компьютерных преступлений.[69] Учитывая, что подавляющее количество переводов, совершенных через провайдеров денежных переводов, выплачиваются наличными, такие услуги представляют возможности по интеграции преступных доходов в легальную финансовую систему. При этом огромный объем операций с наличностью обеспечивает отличную маскировку для отмывания денег на стадии размещения. Зачастую финансовые услуги являются частью сложной схемы, где присутствует, как минимум, одна операция с наличными и участвует, по меньшей мере, один денежный мул.

Традиционная типология с участием провайдеров денежных переводов выглядит следующим образом:

1. Спам-рассылка ложных объявлений о трудоустройстве с последующей вербовкой заинтересовавшихся по телефону или другим способом, который не требует личной встречи. Предлагаемые вакансии часто якобы связаны с финансовой деятельностью или позиционируются как «работа на дому».

2. Деньги переводятся на банковский счет завербованного мула. Мул получает инструкции снять полученную сумму наличными и отправить их некому лицу, используя систему денежных переводов. За свои услуги мул получает комиссионное вознаграждение.

3. Провайдеры денежных переводов служат орудием и способом перемещения денежных средств.

В контексте данного исследования нет причины не предположить, что наличные деньги могут быть зачислены на счет мула (шаг 2), используя виртуальные валюты.

---

[68] «Отмывание денег посредством новых способов платежей», ФАТФ-ГАФИ, Октябрь 2010. (Источник: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf)

[69] Параграф 139, «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», Международного проекта Совета Европы по борьбе с киберпреступностью и МАНИВЕЛ, Март 2012 (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

6.6 Законные торговцы, принимающие виртуальную валюту

Другим проявлением роста популярности bitcoin является то, что все большее число торговцев принимают платежи в виртуальных валютах, прежде всего bitcoin. [70] , [71] , [72] Bitcoin является привлекательной альтернативой для торговцев по следующим причинам[73]:

1. После подтверждения сделки с bitcoin являются необратимыми, поэтому нет рисков возвратных платежей или других рисков мошенничества, которые существуют при использовании платежных карт.

2. Комиссия по операциям с bitcoin меньше комиссии по операциям с платежными картами.

Пропорционально росту количества торговцев, принимающих bitcoin, появилась и динамично развивается целая система услуг, нацеленная на оказание содействия бизнесу осуществлять торговлю, используя bitcoin[74].

7 Правовое регулирование

В этом разделе пособия будет сделана попытка разобраться в вопросах действующего в настоящее время правового регулирования виртуальных валют как на национальном, так международном уровнях.

7.1 Международные нормы и стандарты

В качестве вступительного слова справедливо заметить, что на сегодняшний момент не существует единых правил или стандартов, которые бы глобально применялись к виртуальной валюте как форме цифровой валюты. Относительная новизна этого феномена, а также совсем недавний рост до какого-либо значительного уровня и относительно незначительное влияние, не создавали до сих пор необходимых предпосылок для всеобъемлющего правового регулирования виртуальных валют.

Тем не менее, было бы нелогично предположить, что виртуальные валюты функционируют в полном правовом вакууме. Даже в отсутствие установленных правовых норм в этой области существует некий общий контекст, в котором обращаются электронные деньги и виртуальная валюта. Другим словам, бурное развитие электронной торговли, и, в частности, усилия на глобальном, региональном и национальном уровнях, направленные на содействие инновациям и эффективности финансовых операций, без сомнения, являются одними из основных инструментов, способствующие успешному становлению системы электронной торговли.

---

70 https://bitpay.com/directory#/
71 https://spendbitcoins.com/places/
72 http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/
73 https://www.bitcoin247.com/en/merchants
74 https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses

Но помимо этого необходимо также учитывать некоторые аспекты, имеющие отношение к потенциальному использованию виртуальных валют для целей отмывания денег, равно как и компьютерных преступлений, с которыми оно, как правило, связано (в случаях незаконной деятельности с использованием виртуальных валют).

7.1.1 Нормативно-правовое регулирование электронной торговли и ее применение к виртуальным валютам

Даже при том, что на сегодняшний день нет единого определения электронной торговли, в значительной степени она понимается как любая форма деловой сделки между физическими и юридическими лицами, которые используют технологию электронной связи вместо физического обмена товаров или услуг. [75] Появление и бурный рост электронной торговли в значительной степени обязан развитию Интернета как среды для общения между клиентами и бизнесом. По последним данным, объемы электронной торговли составляют почти 5% глобальных продаж. [76]

Отправной точкой правил электронной торговли является Типовой закон об электронной торговле 1996 года, разработанный и принятый Комиссией Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ). [77] И хотя этот акт и не является международным договором в традиционном понимании международного публичного права, этот документ широко используется для развития национальных законодательств в области электронной коммерции и, в сущности, служит международным стандартом, регулирующим электронную торговлю. Секретариат ЮНСИТРАЛ ведет реестр стран, в которых принят и вступил в силу закон об электронной торговле. На момент подготовки данного пособия такие законы были приняты в 54 странах. [78]

Типовой закон ЮНСИТРАЛ об электронной торговле устанавливает ряд понятий, играющих важную роль в понимании текущей правовой дискуссии о виртуальных валютах. Одним из таких понятий является принцип **технологической нейтральности**[79], или, в понятиях Типового закона, *медиа нейтральности*. [80] Переводя в контекст виртуальных валют,

---

[75] Директива 2000/31/ЕС Европейского парламента и Совета от 8 июня 2000 года «О некоторых правовых аспектах услуг информационного общества, в частности электронной торговли, на внутреннем рынке», статья 2 (f), (Источник: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML); Типовой закон ЮНСИТРАЛ об электронной торговле, Статья 1(b) (Источник: https://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

[76] «Мировые объемы продаж электронной торговли достигли $1 трлн. дол. США», BizReport (Источник: http://www.bizreport.com/2013/08/global-ecommerce-sales-top-us1-trillion.html)

[77] https://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

[78] https://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html

[79] Пояснительная записка к Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах (Источник: http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf).

[80] Типовой закон ЮНСИТРАЛ об электронной торговле (с Руководством по принятию),

этот принцип означает, что технологии, применяемые для осуществления операций с виртуальными валютами, могут использоваться как в законных, так и противозаконных целях, и что основная технология не считается незаконной *per se* только в силу возможного ее преступного использования. Этот аргумент особенно актуален в дискуссиях о возможном запрете использования виртуальных валют в качестве законных финансовых инструментов, что могло бы привести к отказу в законном использование этой технологии. Такие опасения по своему характеру не диссонируют с правовыми нормами, которые регулируют децентрализованный пиринговый обмен защищенными авторским правом материалами, а также вопросы использования для этих целей технических средств.[81] Большая часть прецедентного права поддерживает концепцию технологической нейтральности, соглашаясь с законным использованием технологии и перекладывая ответственность за ее незаконное использование на конечных пользователей.

И хотя основной целью Типового закона ЮНСИТРАЛ об электронной торговле, скорее всего, является гармонизация правил об электронной торговле, глобальной целью данного акта все же является содействие развитию электронной торговли и создание условий, способствующих ее росту. В этом контексте виртуальные валюты представляют собой интересную дилемму. С одной стороны, использование виртуальной валюты согласуется с общей целью содействия росту электронной коммерции, предлагая дополнительный способ осуществления финансовых операций, полезный для развития электронной торговли. С другой стороны, угрозы и проблемы, связанные с высокими рисками, которые присущие криптовалютам, а также угрозы совершения киберпреступлений в отношении этих валют могут служить демотивирующим фактором, о чем свидетельствует недавний скандальный случай с Mt. Gox[82].

Одним из наиболее важных аспектов регулирования электронной торговли в контексте виртуальных валют является **защита потребителей**. Речь идет о наборе норм, защищающих права потребителей и предоставляющие им право на товары и услуги приемлемого стандарта, а также защищают их от нечестных и несправедливых деловых практик. Например, в Директиве ЕС об электронной торговле [83] прямо устанавливается высокий уровень защиты прав потребителей в качестве основного фактора, способствующего свободному движению услуг информационного общества.[84] Учитывая широкий перечень вопросов,

(Источник: https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

[81] A&M Records, Inc. v. Napster, Inc. (Источник: http://onlinelaw.wustl.edu/case-study-am-records-inc-v-napster-inc/); MGM Studios, Inc. v. Grokster, Ltd. (Источник: http://en.wikipedia.org/wiki/MGM_Studios,_Inc._v._Grokster,_Ltd.), Pirate Bay (Источник: http://en.wikipedia.org/wiki/The_Pirate_Bay_trial), BitTorrent systems (Источник: http://en.wikipedia.org/wiki/Legal_issues_with_BitTorrent).

[82] http://en.wikipedia.org/wiki/Mt._Gox#Bankruptcy_and_shutdown

[83] Директива 2000/31/ЕС Европейского парламента и Совета от 8 июня 2000 года «О некоторых правовых аспектах услуг информационного общества, в частности, электронной торговли на внутреннем рынке» (Источник: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN.

[84] Директива 98/27/ЕС Европейского парламента и совета от 19 мая 1998 г.,

охватываемых современным законодательством о правах потребителей и о защите прав потребителей, более чем очевидно, что некоторые из особенностей криптовалют, таких как bitcoin, с присущим им невозвратным характером операций, несомненно, будет вызывать вопросы с точки зрения защиты прав потребителей. [85] Возможно, еще более актуальным примером является активное сближение сфер противодействия киберпреступности и защиты данных: организации по защите прав потребителей часто становятся основными партнерами в вопросах выявления и сообщения о компьютерных преступлениях [86] и, таким образом, могут являться важным источником информации для целей расследований, связанных с незаконным использованием виртуальных валют.

В то же время различные юридические акты, касающиеся электронных платежей и электронных денег, имеют, пожалуй, меньшее значение в контексте виртуальных валют. Дело в том, что как международные, так и региональные нормативные документы, регулирующие вопросы электронных денег и электронных платежей [87], в основном, придерживаются логики, что такие платежи осуществляются при помощи установленных финансовых механизмов через традиционные финансовые учреждения, использующие фиатные деньги. Но на самом деле виртуальные валюты, будь то централизованные, или децентрализованные, обращаются вне этих учреждений и механизмов за исключением, когда такое взаимодействие происходит при обмене виртуальных валют на фиатные и наоборот. Поэтому, несмотря на то, что некоторые аналогии, бесспорно, могут быть проведены чисто с юридической точки зрения, отличия в осуществлении транзакций и, прежде всего, разительное отличие в части применимых регулятивных норм не имеют большого значения для правового анализа и практического использования виртуальных валют.

7.1.2 Нормативно-правовые акты в сфере противодействия отмыванию денег и виртуальные валюты

Отмывание денег означает процесс, посредством которого преступники маскируют происхождение собственности и контроль над доходами от преступной деятельности, представляя такие доходы как имеющие законное происхождение. И хотя криминальные деньги могут быть

касающаяся защиты интересов потребителей (Источник: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31998L0027)

85 Право на отзыв в соответствии с Директивой 2011/83/EU о правах потребителей (Источник: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1)

86 http://www.ftc.gov/enforcement/consumer-sentinel-network

87 Типовой закон ЮНСИТРАЛ о международных кредитовых переводах (Источник: https://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf); Директива 2009/110/ЕС Европейского Парламента и Совета от 16 сентября 2009 г. об учреждении, деятельности и надзоре за деятельностью организаций, занимающихся электронными деньгами (Источник: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN)

успешно отмыты и без помощи финансового сектора, реальность такова, что ежегодно сотни миллиардов долларов, полученных преступным путем, отмываются через финансовые учреждения.[88] Характер продуктов и услуг, предлагаемых на рынке финансовых услуг (владение, контроль и управление денежными средствами и собственностью других лиц) означает, что финансовый сектор уязвим с точки зрения отмывания денег.

Существует обширная база международных инструментов и стандартов в сфере борьбы с отмыванием денег. Ее начало было положено Конвенцией Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ 1988 года, которая стала первым международно-правовым документом, определившим элементы преступления по отмыванию доходов, полученных в результате совершения перечисленных Конвенцией преступлений.[89] Аналогичный подход нашел свое отражение и в Конвенции Организации Объединенных Наций против транснациональной организованной преступности 2000 года[90] и в Конвенции Организации Объединенных Наций против коррупции 2003 года[91], которые дали дальнейшее развитие понятия отмывания доходов, полученных преступным путем, и установили конкретные требования и процедуры по борьбе с этим феноменом. Международная конвенция ООН о борьбе с финансированием терроризма предлагает более специализированный подход, устанавливая специальные механизмы по установлению, обнаружению и замораживанию или аресту орудий и доходов от связанных с финансированием терроризма преступлений.[92]

Обзор современных инструментов по борьбе с отмыванием денег не будет полным, не рассмотрев инструменты Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ). ФАТФ – межправительственный орган, созданный для разработки стандартов и содействия эффективному осуществлению правовых, нормативных и операционных мер по борьбе с отмыванием денег, финансированием терроризма и другими угрозами для целостности международной финансовой системы.[93] Рекомендации ФАТФ[94], охватывающие вопросы отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения,

---

88 «Что такое отмывание денег?», International Compliance Association (Источник: http://www.int-comp.org/what-is-money-laundering).

89 Статья 5 Конвенции Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (Источник: http://www.unodc.org/pdf/convention_1988_en.pdf)

90 Статьи 6 и 7 Конвенции Организации Объединенных Наций против транснациональной организованной преступности (Источник: http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC Convention/TOCebook-e.pdf)

91 Статьи 23, 52, 54 и 57 Конвенции Организации Объединенных Наций против коррупции (Источник: http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf)

92 Статья 8 Международной конвенции ООН о борьбе с финансированием терроризма (Источник: http://www.un.org/law/cod/finterr.htm).

93 http://www.fatf-gafi.org/pages/aboutus/

94 http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html

являются, в сущности, обязательными стандартами, исполнение которых контролируется ФАТФ.

Учитывая цель данного пособия и характер децентрализованных виртуальных валют, представляется очевидным, что использование виртуальных валют в качестве орудия отмывания денег или в целом как орудия криминальных денежных потоков в сети Интернет, вызывает вполне обоснованные опасения. В то же время необходимо понимать, что актуальные с точки зрения отмывания денег аспекты виртуальных валют в меньшей степени связаны с самой технологией (которая по-прежнему может представлять интерес по причинам повышенной конфиденциальности и сложности отслеживания, а также из-за криптографической защиты), а, скорее, связаны с отсутствием должного регулирования и контроля со стороны компетентных органов за операциями с использованием виртуальных валют. Поскольку операции с виртуальными валютами проводятся фактически вне установленных, и, таким образом, тщательно регулируемых традиционных финансовых механизмов, виртуальные валюты представляются весьма привлекательной опцией для преступников, занимающихся отмыванием денег. Некоторые специфические виды виртуальных валют, в основе которых лежат анонимность и криптографическая защита, как, например, bitcoin, имеют дополнительное преимущество в виде чрезвычайной сложности отслеживания и декодирования операций между пользователями таких систем. Таким образом, с точки зрения борьбы с отмыванием денег внимание должно быть сосредоточено не на самих виртуальных валютах, а на тесно связанных с ними международных стандартах, которые в той или иной мере направлены на предотвращение незаконного использования виртуальных валют для целей отмывания преступных доходов.

7.2 Уголовные преступления, связанные с виртуальными валютами

Виртуальные валюты в силу своей природы могут иметь отношение к целому ряду уголовных преступлений. И несмотря на то, что в центре внимания данного пособия находится отмывание денег, совершенное посредством виртуальных валют, представляется важным также кратко показать более широкий контекст, в котором такие преступления совершаются. При этом обращает на себя внимание и вызывает беспокойство наличие взаимосвязей преступлений с использованием виртуальных валют и компьютерных преступлений.

Прежде всего, как отмечалось ранее, виртуальные валюты все же попадают под действие ряда регулятивных норм. Нарушение этих норм в некоторых случаях может влечь за собой уголовное наказание. Например, владение или использование виртуальной валюты *per se* может в некоторых странах быть уголовно наказуемым деянием с формулировкой «незаконное владение нелицензированной валютой» или «осуществление деятельности по обмену нелицензированных денежных средств».

Виртуальные валюты сами по себе могут являться объектом уголовного преступления, как, например, в случае кражи виртуальной валюты или приобретения виртуальной валюты мошенническим способом. Такие действия также могут включать в качестве составной части преступления конвертацию виртуальной валюты в реальную валюту.

Кроме всего виртуальные валюты могут быть частью *modus operandi* отдельного преступления, например, в случае использования виртуальных валют для покупки запрещенных товаров, таких как оружие, наркотики или материалы, свидетельствующих о насилии над детьми, а также для оплаты услуг, предоставление которых в некоторых странах может особым образом регулироваться или криминализироваться (например, азартные игры). В этом смысле виртуальные валюты представляют собой *орудие* совершения преступления. Виртуальные валюты также могут быть предоставлены или получены с намерением использовать их в полном объеме или частично для совершения преступлений, установленных универсальными международно-правовыми документами по борьбе с терроризмом, или иным способом предназначаться для причинения смертельных или серьезных увечий гражданскому или любому другому лицу, не принимающего активного участия в военных действиях во время вооруженного конфликта, когда целью таких деяний по своей природе или контексту является запугивание населения или принуждение правительства, или международной организации к совершению или воздержанию от совершения какого-либо действия (преступления по финансированию терроризма).

Наконец, находясь в центре внимания данного пособия, уголовное преступление по отмыванию денег совершается, когда виртуальные валюты используются для конверсии или передачи имущества, если известно, что такое имущество представляет собой доходы от преступлений, в целях сокрытия или утаивания преступного источника имущества, или с целью помочь любому лицу, участвующему в совершении такого преступления или преступлений, уйти от ответственности за свои деяния, или для сокрытия или утаивания истинной природы, источника, местонахождения, способа распоряжения, перемещения, прав, включая права собственности, на имущество, зная, что такое имущество представляет собой доходы от преступлений.

Учитывая электронную природу виртуальных валют, почти во всех этих типах преступлений может существовать тесная связь с кибернетическими преступлениями. Сам по себе термин «киберпреступность» не имеет унифицированного определения, и, вероятно, его лучше всего рассматривать как совокупность действий или поведение, а не как отдельное деяние. Киберпреступность обычно воспринимается как понятие, которое обозначает преступления против компьютерных данных и систем, а именно: преступления против конфиденциальности, целостности и доступности данных и систем, а также преступления, совершенные с помощью компьютерных данных и систем, и преступления, связанные с содержанием данных, такие как компьютерное мошенничество, преступления по нарушению авторских прав или прав на

торговую марку, или рассылка и контроль рассылки спама. В последнем случае «традиционные» преступления, такие как подделка или производство, распространение или хранение детской порнографии, получают иную квалификацию и степень тяжести, если они совершаются с использованием компьютерных систем, так как технология позволяет и облегчает совершение и/или сокрытие таких преступлений, содействует более широкому распространению негативного эффекта этих деяний, и оказывает более тяжелое воздействие на жертвы независимо от того, в какой стране они находятся[95]. Но, в общем, разграничение может быть сделано путем выделения «основных» киберпреступлений, которые связанны с актами, направленных против компьютерных информационных систем или данных, из более широкой категории киберпреступлений, совершенных с помощью компьютерных систем или данных.

В последнее десятилетие наблюдается позитивная динамика имплементации в национальное законодательство международных и региональных инструментов, направленных на борьбу с киберпреступностью. К ним относятся как юридически обязывающие, так и юридически не обязывающие документы. Генезис, правовой статус, географический охват, предмет и механизмы, предусмотренные этими инструментами, сильно разнятся. Примерами региональных договоров могут быть, к примеру, Конвенция Совета Европы о компьютерных преступлениях, Соглашение о сотрудничестве государств – участников Содружества Независимых Государств (СНГ) в борьбе с преступлениями в сфере компьютерной информации, Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, или Конвенция о преступлениях в области информационных технологий Лиги арабских государств.[96] Все государства-участники ГУАМ представлены в Совете Европы и являются участниками Конвенции Совета Европы о компьютерных преступлениях.[97] Страны регулярно проходят проверку на предмет их соответствия положениям конвенции, которая

[95] Комплексное исследование по киберпреступности (проект, 2013), подготовленное УНП ООН для рассмотрения межправительственной экспертной группой по проведению всестороннего исследования проблем киберпреступности, в соответствии с методологией, согласованной в рамках этой экспертной группы (далее – Комплексное исследование УНП ООН по киберпреступности), стр. 11 и далее.

[96] Конвенция Совета Европы о компьютерных преступлениях (2001); Соглашение о сотрудничестве государств – участников Содружества Независимых Государств (СНГ) в борьбе с преступлениями в сфере компьютерной информации (2001); Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (2009); Конвенции о преступлениях в области информационных технологий Лиги арабских государств (2010). Для получения дополнительной информации о юридически обязывающих и необязывающих инструментах см. также Комплексное исследование УНП ООН по киберпреступности, стр. 63 и далее.

[97] Список государств-участников доступен: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

проводится Комитетом Конвенции Совета Европы по киберпреступности (T-CY).

Что касается уголовных преступлений, связанных с виртуальными валютами, то «основные» киберпреступления (как то неправомерный доступ к компьютерной системе) могут быть *вспомогательными* по отношению к таким преступлениям, как кража виртуальной валюты. Например, «хакерский» взлом личного кошелька с целью кражи bitcoin может квалифицироваться как кража, где киберпреступление является вспомогательным преступлением, облегчающее совершение основного. Преступления по неправомерному доступу также могут иметь отношение к отмыванию денег посредством виртуальных валют, например, когда счета третьих лиц используются для проведения операций без их на то согласия.

Более широкие формы киберпреступности, такие как компьютерное мошенничество, могут представлять собой основное преступление, для которого виртуальная валюта является объектом, например, когда виртуальная валюта получена обманным путем. Наконец, преступления, связанные с данными контента и другие формы киберпреступности, такие как совершенные с использованием компьютера акты хранения или распространения материалов жестокого обращения с детьми или продажа запрещенных наркотиков онлайн, могут либо быть предикатным преступлением по отношению к отмыванию денег посредством виртуальных валют (в случае продажи таких материалов), либо быть основным преступлением, для которого виртуальные валюты выступают орудием (в случае приобретения такого материала). Вряд ли найдется лучше пример потенциального использования криптовалют для торговли незаконными материалами, чем пример Silk Road. [98] Подводя итого вышесказанному, отметим, что возможные взаимосвязи между киберпреступлениями, «традиционными» преступлениями и виртуальными валютами множественны и потенциально сложны.

Важно также отметить, что ряд характеристик преступных деяний, обычно квалифицируемых как «киберпреступление», со следственной точки зрения являются сходными с характеристиками преступлений, совершенных с использованием виртуальных валют. Киберпреступлениям, к примеру, возможно более, нежели любой другой форме преступности, присущ транснациональный характер и вовлечение нескольких юрисдикций только добавляет сложности как для целей проведения расследования, так с точки зрения оказания взаимной правовой помощи. Кроме того незаконное использование, перехват или вмешательство в компьютерные системы или данные часто бывает трудно отследить и, таким образом, получение сообщений о совершении киберпреступлений остается одной из главных проблем. В дополнение к этому, как и все другие преступления, киберпреступления оставляют следы, большинство из которых – в электронной форме. Другими словами, это – электронные

[98] «ФБР закрыл состоящий на службе киберпреступникам сайт Silk Road», USA Today, (Источник: http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/)

доказательства. Нужно сказать, что существуют многочисленные правовые и технические трудности в обеспечении своевременной сохранности и анализе таких доказательств. Эти и другие особенности киберпреступлений, зачастую являющиеся предикатными или вспомогательными преступлениями по отношению незаконному использованию виртуальных валют, нередко требуют глубокого понимания соответствующих вопросов, как со стороны регуляторов, так и представителей системы уголовного правосудия.

7.3 Регулирование на национальном уровне

В отличие от международного контекста вопрос о регулировании использования виртуальных валют в той или иной степени был решен в нескольких странах, как правило, в рамках действующего законодательства, касающегося предоставления отчетности, регистрации, налогообложения и возможных злоупотреблений в целях отмывания денег. В то же время тестирование различных подходов к регулированию виртуальных валют в условиях ожидаемого роста операций с их использованием, а также осознания достижений в области развития технологий, приходится констатировать, что нынешние состояние регулирования виртуальных валют находятся все еще на начальном уровне. Следовательно, странами практикуются самые разные подходы к регулированию статуса виртуальных валют и разработке применимых к ним правил.

В виду растущей популярности электронной торговли **Соединенные Штаты Америки** являются активным участником дискуссий о виртуальных валютах. Используемый в настоящее время политиками и регуляторными органами подход состоит в том, чтобы разрешить функционирование виртуальных валют при условии применения установленных правил к определенным игрокам, действующих на рынке услуг виртуальных валют. В рамках этого подхода в марте 2013 года Комиссией по борьбе с финансовыми преступлениями (FinCEN) было опубликовано руководство FIN-2013-G001 [99], разъясняющее вопросы применения законодательства США к определенным категориям провайдеров услуг виртуальных валют (обменники, администраторы и т.д.), на которые теперь распространяются требований по регистрации, хранению документов и пр. на ровне с другими провайдерами финансовых услуг («ПФУ»). Это Руководство проводит четкую разграничительную линию между, с одной стороны, пользователями виртуальной валюты (не считаются ПФУ и, таким образом, на них не распространяются требования по регистрации и ведению документации), и администраторами и обменниками, с другой стороны, которые квалифицируются как ПФУ, так как их деятельность предполагает оказание услуг по «перемещению денег». Кроме того Служба внутренних доходов США (IRS) опубликовала Руководство 2014-21[100], в котором предоставила ответы на ряд вопросов

[99] http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
[100] http://www.irs.gov/pub/irs-drop/n-14-21.pdf?utm_source=3.31.2014+Tax+Alert&utm_campaign=3.31.14+Tax+Alert&utm_medium=email

касательно статуса виртуальных валют в США с точки зрения налогообложения. В Руководстве отмечается, что виртуальные валюты должны рассматриваться как товар и, таким образом, доходы, полученные от продажи таких товаров, должны облагаться налогом.

Соединенное Королевство прияло «на вооружение» подобный подход к рынку виртуальных валют (криптовалют, в частности), что следует из положений Налогового и Таможенного Бюллетеня 09/14 «Налоговый режим деятельности, связанной с bitcoin и другими подобными криптовалютами».[101] Признавая бурный характер развития рынка услуг, предоставляемых посредством децентрализованных виртуальных валют, и одновременно не признавая явно bitcoin как полноценную валюту, Бюллетень приравнивает bitcoin к средству оплаты, к которому применяются механизмы индивидуального (НДС, сумма которого отличается в зависимости от категории пользователей: майнеры, обменеики и пр.), и корпоративного налогообложения (подоходный налог и налог на прирост капитала, полученного от операций с bitcoin).

Китай отдал предпочтение иному подходу к регулированию рынка виртуальных валют, введя запрет на использование bitcoin и других криптовалют своими финансовыми и платежными учреждениями. В декабре 2013 года Народный банк Китая и пять связанных с ним министерств опубликовали циркуляр «Предотвращение рисков, связанных с Bitcoin»[102], обнародовав свою позицию относительно того, что bitcoin не является деньгами и не может быть использован как законное платежное средство для обмена на иностранную валюту, оплаты ипотеки, совершения других законных платежей, в том числе инвестиций или страхования. В то же время запрет не является абсолютным, поскольку виртуальные валюты все еще могут использоваться в Интернете в качестве товара на страх и риск пользователей. Однако, сайты, предоставляющие возможность торговли с использованием bitcoin, в соответствии с законом о борьбе с отмыванием денег, подлежат регистрации в регулирующих органах по вопросам телекоммуникаций.

Другой, хотя все такой же осторожный, подход используется властями **Канады**, в соответствии с которым bitcoin не является законным платежным средством в стране. Тем не менее, в отличие от Китая, канадские власти оставили для себя открытой возможность для пересмотра этого вопроса в будущем в зависимости от развития событий. Изучая возможности использования bitcoin и других виртуальных валют в интересах граждан Канады, канадские власти учитывают такие факторы, как финансовая стабильность, высокий риск, а также «удобство и простота использования, цена, надежность, безопасность и эффективные механизмы возмещения» [103] . Один из первых банкоматов (АТМ),

---

101 http://www.hmrc.gov.uk/briefs/vat/brief0914.htm

102 «Циркуляр Народного банка Китая и пяти связанных с ним министерств о "Предотвращении рисков, связанных с Bitcoin" (неофициальный перевод)», BTC China, (Источник: https://vip.btcchina.com/page/bocnotice2013).

103 «Что нужно знать о цифровой валюте», Налоговая служба Канады (Источник: http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-eng.html).

предоставляющий возможность обмена bitcoin на канадские доллары и наоборот, был установлен в Ванкувере в октябре 2013 года.[104] Помимо этого в Канаде существуют и другие возможности обмена и торговли bitcoin, что свидетельствует о растущей популярности криптовалют в стране.

Возможно, на нечто среднее между этими полярными подходами пал выбор в **Сингапуре**. Не ограничивая использование виртуальных валют в качестве возможного средства платежа в своей финансовой системе, Сингапур намеревается ужесточить требования к обменным площадкам и торгующих bitcoin автоматам с целью обязательной идентификации личности клиентов и обеспечения прозрачности сделок с bitcoin.[105]

[104] «Первый в мире банкомат Bitcoin открывается в Ванкувере, Канада», Mashable (Источник: http://mashable.com/2013/10/30/bitcoin-atm-2/)

[105] "Валютное Управление Сингапура будет регулировать посредников на рынке виртуальных валют с целью минимизации рисков отмывания денег и финансирования терроризма", Валютное Управление Сингапура (Источник: http://www.mas.gov.sg/news-and-publications/press-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx)

Пример: Bitcoin

Bitcoin – децентрализованная пиринговая платежная система, не имеющая центрального органа или посредников, функционирование которой обеспечивается ее же пользователями. В 2009 году Сатоши Накамото опубликовал первую спецификацию Bitcoin вместе с описанием концепции криптографическиой защиты для списка рассылки [106]. В основе концепции функционирования Bitcoin лежит центральный платежный реестр, известный как «цепочка блоков». Этот реестр содержит данные о каждой когда-либо выполненной операции и используется для проверки их легитимности [107]. Целостность и хронологический порядок операций в реестре обеспечиваются криптографией.

Согласно представленной в главе 5 классификации, bitcoin – это конвертируемая децентрализованная виртуальная валюта, известная также как криптовалюта. Bitcoin присущи некоторые новаторские технические характеристики, которые значительно осложняют проведение расследований отмывания преступных доходов, совершенного с использованием этой криптовалюты. По этой причине представляется разумным попытаться разобраться в вопросе, как функционирует Bitcoin.

Исходя из вышесказанного, рассмотрим работу системы Bitcoin с точки зрения ее характеристик как децентрализованной виртуальной валюты.

Передача bitcoin

Первый, и, пожалуй, наиболее очевидный вопрос, – как пользователи осуществляют передачу bitcoin.

Каждый пользователь сети Bitcoin имеет один или более Bitcoin-адрес. Пользователь может создать любое количество Bitcoin-адресов, хоть даже свой адрес для каждой отдельной сделки, если есть такое желание[108].

Адрес является уникальным идентифицирующим значением, используемым для обозначения принадлежности конкретных

106 https://bitcoin.org/en/faq
107 https://bitcoin.org/en/how-it-works
108 В некоторых наиболее доступных программных обеспечениях Bitcoin личность пользователя идентифицируется посредством единого "кошелька", который содержит несколько "получающих адресов".

bitcoin[109,110]. Для перечисления bitcoin от лица «А» лицу «В» в сеть Bitcoin поступает сообщение, содержащее адрес отправителя, адрес получателя (его «получающий адрес») и сумму передаваемых bitcoin. Каждый узел сети Bitcoin, получивший такое сообщение, обновляет свою версию платежного реестра, а затем передает сообщение о проведенной операции другим узлам[111].

Что может помешать злоумышленнику, скажем лицу «С», оправить в сеть сообщение о передаче bitcoin с адреса лица «А» на адрес лица «С» (или другого лица), то есть, украв у лица «В» его bitcoin? Такая возможность полностью предотвращается, поскольку подлинность сообщений о совершении операций обеспечивается криптографической защитой цифровых подписей[112]. Для создания легитимного сообщения об операции по передаче bitcoin с адреса лица «А», лицо, генерирующее такое сообщение, должно знать пароль, который связан с данным адресом[113].

Возникает два вопроса:

1. Как лицо «В» может знать, что лицо «А» на самом деле владеет bitcoin, которые передаются?
2. Каким образом лицу «В» может быть известно, что лицо «А» еще не передало bitcoin кому-то еще?

Ответы на эти вопросы будут даны далее.

Подтверждение прав собственности на bitcoin

Для того, чтобы сгенерировать легитимное сообщение о передаче bitcoin, отправитель bitcoin должен доказать, что он является их владельцем.

Рассмотрим ситуацию, когда, к примеру, лицо «А» желает передать 10 bitcoin лицу «В». Для этого лицу «А» необходимо включить в сообщение

109 Строго говоря, каждый адрес представляет собой пару из открытого/закрытого ключей."Получающий адрес" – это открытый ключ. Закрытый ключ хранится в секрете и используется для цифровой подписи транзакций, тем самым подтверждая легитимность транзакции.

110 См.: http://en.wikipedia.org/wiki/Public-key_cryptography for general information on public key cryptography

111 http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

112 http://en.wikipedia.org/wiki/Digital_signature

113 Собственного говоря, лицо должно иметь закрытый ключ, связанный с открытым ключом, который идентифицирует адрес отправителя. Напомним, что каждый адрес является парой из открытого/закрытого ключей. "Получающий адрес" является открытым ключом, а соответствующий закрытый ключ используется для цифровой подписи транзакций, посредством которых передаются bitcoin с "принимающего адреса" отправителя.

ссылки на предыдущие транзакции, вследствие которых было получено более 10 bitcoin. Они обозначаются как «входы» транзакции[114].

Напомним, что каждый пользователь сети Bitcoin имеет копию платежного реестра («цепочку блоков»), в котором содержится история всех предыдущих транзакциях. Поэтому лицо «B» может легко удостовериться, что bitcoin, на которые идет ссылка в сообщении, на самом деле принадлежат лицу «A».

Для упрощения процесса верификации было установлено правило, в соответствии с которым все сделки должны быть сбалансированы. Другими словами, количество bitcoin на входах транзакции должно совпадать с количеством bitcoin на выходах.

Лучше всего это можно понять на конкретном примере. Рассмотрим транзакцию, где лицо «A» пересылает 10 bitcoin по лицу «B». Список входов и выходов, показанных в Таблице 1, поможет продемонстрировать баланс.

«Входы»		***«Выходы»***	
Идентификатор транзакции	**Сумма**	***Идентификатор кошелька***	**Сумма**
123	1	Лицо «B»	10
456	3	Лицо «A»	2
999	4		
888	4		

Таблица 1: Примерный перечень «входов» и «выходов» транзакции

На «входной» стороне транзакции приведен список из четырех операций, которые содержат «принимающий адрес» лица «A». Они служат доказательством того, что лицо «A» в общей сложности владеет 12 bitcoin. Лицо «B» может проверить идентификаторы этих транзакций в цепочке блоков и убедится, что в каждом случае адрес получателя был адресом лица «A». Лицо «B» также может проверить, не были ли эти транзакции «входом» в какой-то другой транзакции, другими словами, что bitcoin еще не были потрачены.

На «выходной» стороне транзакции – 10 bitcoin, которые лицо «A» желает переслать лицу «B». Оставшиеся 2 bitcoin лицо «A» отсылает обратно на свой адрес. Это последняя «выходная» запись означает, что

[114] Получатель(и) bitcoin обозначаются как «выходы» транзакции.

общее количество bitcoin на «входе» равно общему количеству bitcoin на «выходе», и, таким образом, сделка является сбалансированной.

Предотвращение двойной траты

Важный вопрос – нивелирование рисков двойной траты. Это является большой проблемой для одноранговых сетей[115], таких как Bitcoin, потому что нет никакой гарантии, что порядок, в котором какой-либо отдельно взятый узел в сети получает уведомление о проведении операций, представляет собой хронологический порядок, в котором они действительный были проведены.

С практической точки зрения, что может помешать лицу «А», создавая сообщение об отправке bitcoin лицу «В», одновременно создать другое сообщение об отправке bitcoin кому-то еще, и, таким образом дважды потратить одни и те же bitcoin? Вполне вероятно, что некоторые узлы сети Bitcoin первоначально получат вторую по счету транзакцию. И когда через некоторое время сообщение о первой транзакции придет в эти узлы, она будет считаться недействительной, поскольку в ней использованы «входы», которые ранее уже были использованы в другой транзакции.

Ключевым технологическим преимуществом сети Bitcoin является метод, с помощью которого эта проблема была решена[116].

Транзакции собираются в группы, известные как блоки, а блоки, в свою очередь, соединяются и формируют цепочку блоков. Транзакции в одном блоке считаются такими, которые произошли в одно время. Блоки выстраиваются так, что каждый последующий блок в цепочке связан с предыдущим.

Транзакции, которые не определены в блок, называются неподтвержденными. Любой узел в сети может собрать неподтвержденные транзакции, сгруппировать их и предложить в качестве следующего блока в цепочке. Предлагаемый блок должен содержать решение сложной математической задачи, которую трудно решить[117]. Сеть Bitcoin динамически регулирует сложность математической задачи таким образом, чтобы каждый новый блок добавлялся в цепь в среднем раз в десять минут.

Может такое случиться, хоть вероятность и очень мала, что несколько узлов в сети Bitcoin предложат блоки приблизительно в одно время. В

[115] В отличие от модели «клиент-сервер» одноранговые сети не имеют центральной точки, а пиры распространяют информацию через сеть. Общую информацию об одноранговых сетях можно найти на: http://en.wikipedia.org/wiki/Peer-to-peer.

[116] Многочисленные хорошие описания этого процесса можно найти в сети Интернет. Например: https://en.bitcoin.it/wiki/Block_chain and http://www.youtube.com/watch?v=Lx9zgZCMqXE

[117] Собственно говоря, создавая блок, узел добавляет к нему большое количество различных числовых значений до тех пор, пока не будет найдено значение, при котором криптографический хэш блока будет ниже определенного порога.

таком случае с добавлением различными узлами разных блоков, цепочка блоков временно разветвится.

Эта ситуация разрешится, когда следующий блок добавится к цепочке. Новый блок будет, как уже говорилось ранее, содержать ссылку на предыдущий блок и, таким образом, присоединится к одному из двух возможных ответвлений в цепочке блоков. Тогда одна из двух ветвей станет длиннее. А правило сети Bitcoin гласит о том, что узлы должны переключаться на самую длинную из доступных ветвей. В результате, очень быстро цепочка блоков стабилизируется, и все узлы согласятся по всем блокам, которые оказались в стороне от конца цепочки.

По этой причине считается безопаснее выждать некоторый период времени, прежде чем, например, отправить товары, оплаченные посредством bitcoin. Вычисление одного блока в среднем занимает десять минут. Таким образом, добавление шесть блоков будет означать ожидание около одного часа.

Майнинг

Процесс построения блоков и добавления их к цепочке как описано выше называется майнингом. Тот, кто создаст блок и добавит его в цепочку, получает вознаграждение в 25 bitcoin. Каждые четыре года вознаграждение за майнинг уменьшается на половину и так будет до тех пор, пока эмиссия bitcoin не прекратится. В общей сложности будет выпущено 21 млн. bitcoin.

Помимо вознаграждения за создание новых блоков майнеры имеют возможность получать комиссию, которая по желанию может быть включена в транзакцию. В настоящее время главной наградой за майнинг являются сами bitcoin. Но со временем транзакционная комиссия станет основным стимулом майнинга.

Как правило, майнинг осуществляется не отдельными лицами, а организованными группами майнеров, известные как пулы. Полученное вознаграждение распределяется между членами пула пропорционально количеству затраченных каждым майнером усилий по вычислению блоков.

Вопросы для самооценки

Вопрос 1: Используя терминологию ФАТФ, дайте определение «виртуальной валюте», «электронным деньгам» и «цифровой валюте», четко объясняя разницу между ними.

Вопрос 2: Опишите характеристики, отличающие конвертируемую виртуальную валюту от неконвертируемой. Приведите пример для каждой категории.

Вопрос 3: Опишите характеристики, отличающие централизованную виртуальную валюту от децентрализованной. Приведите пример для каждой категории.

Вопрос 4: Разбираясь в вопросах о виртуальных валютах важно понимать интерфейс между виртуальными валютами и традиционной финансовой системой. В этой связи расскажите о роли, которую играют биржи виртуальных валют, делая, в частности, акцент на возможных источниках финансирования (способах оплаты), которые могут быть использованы для приобретения виртуальных валют.

Вопрос 5: Помимо бирж виртуальных валют приведите еще три примера интерфейса между традиционной финансовой системой и виртуальными валютами, важные с точки зрения легализации преступных доходов посредством виртуальных валют.

Вопрос 6: Назовите причины, почему некоторые виртуальные валюты являются привлекательным средством оплаты для законных предпринимателей.

Вопрос 7: Объясните, что такое криптовалюта.

Вопрос 8: Объясните, как функционирует сеть Bitcoin, обращая особое внимание на цели майнинга.

Вопрос 9: Расскажите, каким образом в сети Bitcoin предотвращается возможность «двойной траты».

Вопрос 10: Объясните, как пользователь сети Bitcoin может доказать другому пользователю свое право собственности на определенное количество bitcoin.

Вопрос 11: Опишите взаимосвязь между принципами технологической нейтральности и использованием виртуальных валют в незаконных целях.

Вопрос 12: Опишите возможную привлекательность криптовалют для целей отмывания денег.

Вопрос 13: В чем разница между преступлениями против конфиденциальности, целостности и доступности компьютерных данных / систем и преступлениями, связанных с данными контента?

Вопрос 14: Назовите, по крайней мере, две страны, которые запретили или ограничили использование bitcoin, и дайте подробные объяснения причинам таких решений.

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Модуль 2
Проблемы, связанные с виртуальными валютами

1 Краткое изложение

В контексте борьбы с отмыванием преступных доходов с виртуальными валютами связан ряд специфических проблем. Цель этого модуля – дать описание этим проблемам.

Сначала будут рассмотрены причины, в силу которых виртуальные валюты представляют сложность для раскрытия и расследования отмывания преступных доходов. Затем будут рассмотрены типологии отмывания преступных доходов посредством виртуальных валют, и, наконец, обозначены некоторые важные тенденции.

2 Цели обучения

По окончанию данного модуля Вы будете:

- Понимать связанные с виртуальными валютами угрозы.
- Знать о типологиях отмывания денег посредством виртуальных валют.
- Знать о сложностях в выявлении отмывания денег, совершенного с помощью виртуальных валют.
- Знать о проблемах, с которыми могут столкнуться следственные органы на национальном уровне при расследовании отмывания денег, совершенного посредством виртуальных валют.
- Знать о проблемах, с которыми могут столкнуться следственные органы на международном уровне при расследовании отмывания денег, совершенного посредством виртуальных валют.
- Знать о важных тенденциях в сфере виртуальных валют и их использования для отмывания преступных доходов.

3 Угрозы, связанные с виртуальными валютами

Данный раздел преследует своей целью дать ответ на вопрос, какие свойства присущи виртуальным валютам, которые затрудняют проведение расследования в случае их использования для отмывания преступных доходов. Чтобы ответить на этот вопрос, в следующих ниже главах описываются трудности, характерные для расследований по отмыванию денег, совершенных посредством виртуальных валют.

3.1 Быстрые и невозвратные транзакции

С точки зрения отмывания преступных доходов представляется важным обратить внимание на такие факторы, как скорость и возможность отмены транзакций с виртуальными валютами.

Скорость транзакций, осуществление которых возможно при помощи новых способов платежей [1], [2], была обозначена как фактор риска в проведенных ранее исследованиях. В частности, средства могут быть сняты или конвертированы гораздо быстрее, чем при помощи традиционных методов. Высокая скорость транзакций осложняет проведения мониторинга и замораживания средств. В контексте данного исследования новые способы платежей также включают в себя виртуальные валюты.

Возможность отмены транзакций зависит от конкретной виртуальной валюты. Например, получив подтверждение осуществления, операции с bitcoin не подлежат отмене[3]. Bitcoin, в прочем, могут быть возмещены получателем. Это, конечно, не является отменой транзакции, а скорее операцией по возврату средств получателем обратно отправителю. С другой стороны, централизованные виртуальные валюты, как правило, функционируют в соответствии с условиями пользовательского соглашения, установленных администратором [4]. В подавляющем большинстве систем централизованных виртуальных валют администратор предостерегает, что транзакции с виртуальными валютами не подлежат отмене. Тем не менее, администратор, как правило, имеет исключительное право действовать по своему усмотрению, в том числе, полностью отменять транзакции, если посчитает необходимым это сделать.

Возможны разные категории операций, которые следует рассмотреть. В каждом из предложенных сценариев поведение виртуальных валют будет рассматриваться с точки зрения скорости и возможности отмены операций.

---

[1] В данном контексте новые способы платежей (НСП) включают предоплаченные карты, мобильные платежи и Интернет-платежи. Интернет-платежи среди прочего включают платежи посредством цифровых / электронных валют.

[2] Параграф 43 «Новые способы платежей, используемые для отмывания денег», ФАТФ-ГАФИ, Октябрь 2010. (Источник: http://www.fatf-gafi.org/media/fatf/documents/reports/ML using New Payment Methods.pdf)

[3] https://bitcoin.org/en/you-need-to-know

[4] Например, http://lindenlab.com/tos.

Итак, для рассмотрения предлагаются следующие три категории операций:

1. Конвертация фиатной валюты в виртуальную (и обратно)
2. Конвертация из одной виртуальной валюты в другую
3. Перевод виртуальной валюты с одного счета на другой

3.1.1 Конвертация фиатной валюты в виртуальную

Собственно говоря, конвертация фиатной валюты в виртуальную может осуществляться одним из двух способов:

- Некоторые централизованные виртуальные валюты можно приобрести или продать непосредственно администратору[5]. В таких случаях операции по покупке / продаже иногда называют депонированием / снятием.
- Другие централизованные и децентрализованные виртуальные валюты, как правило, приобретаются через биржи виртуальных валют.

Как уже упоминалось в Модуле 1, существует много различных источников финансирования (способов оплаты), которые могут быть использованы для приобретения виртуальных валют, в том числе: банковский перевод, денежный перевод, платежная карта, наличными или посредством услуг Интернет-платежей, как, например, PayPal. Расчетные циклы (включая скорость и возможность отмены транзакций) варьируется в зависимости от источника финансирования, но их рассмотрение выходит за рамки данного пособия.

3.1.2 Конвертация из одной виртуальной валюты в другую

С точки зрения бирж виртуальных валют конвертация одной виртуальной валюты в другую является частным случаем покупки / продажи виртуальной валюты. Возможность использования виртуальной валюты в качестве источника финансирования для приобретения другой виртуальной валюты предоставляется некоторыми биржами виртуальных валют[6], [7], [8].

В большинстве случаев задержки в конвертации виртуальной валюты связаны с мерами по предотвращению мошенничества, проводимые биржами виртуальных валют. Такие задержки часто применяются к новым счетам или источникам финансирования и отменяются после проведения нескольких операций, когда клиент уже имеет так называемую историю транзакций.

---

[5] https://account.entropiauniverse.com/account/deposits/index.xml?
[6] https://firstmetaexchange.com/home
[7] https://www.virwox.com/?stage=1
[8] http://howtobuybitcoins.info/

В зависимости от конкретной виртуальной валюты, а также от характера операции, возможны мгновенные переводы виртуальной валюты. Например, можно приобрести Linden Dollars в Second Life и мгновенно зачислить их на свой счет[9].

3.1.3 Перевод виртуальной валюты с одного счета на другой

Особенности перевода виртуальной валюты с одного счета на другой вполне естественно зависят от конкретной виртуальной валюты. Так, скорость подтверждения транзакций варьируется в зависимости от используемой виртуальной валюты, и, как правило, находится в диапазоне от мгновенной передачи до задержки в несколько минут[10,11].

К примеру, как уже упоминалось ранее, операции с децентрализованными виртуальными валютами (такими, как bitcoin) после подтверждения являются невозвратными. Преимущество этого для законного пользователя состоит в том, что нет возможности отменить («отозвать») транзакцию, преследуя мошеннические цели. Для преступников невозвратный характер транзакций означает, что не существует расчетного цикла или других возможностей в платежной системе для истребования средств обратно.

Но по тем же причинам (скорость и невозвратность операций) bitcoin стали привлекательным способом оплаты и в криминальном мире[12, 13, 14].

Переводы централизованных виртуальных валют между счетами обычно протекают также мгновенно. Тем не менее, существует возможность, по крайней мере, для администратора отменить транзакцию.

3.2 Анонимность

Такая угроза характерна, прежде всего, для децентрализованных виртуальных валют. Некоторые из этих виртуальных валют специально создавались для обеспечения анонимности транзакций. Самым ярким примером является bitcoin. Именно по этой причине эта виртуальная валюта выбрана для демонстрации угроз, связанных с анонимностью операций[15].

---

[9] Биржа Virwox немедленно зачисляет доллары Linden на соответствующий виртуальный счет (аватар).
[10] 10-минутное ожидание для подтверждения транзакции в сети Bitcoin (см. Модуль 1)
[11] 2.5-минутное ожидание для подтверждения транзакции в сети (https://litecoin.org/)
[12] «Задумайся о своем кошельке: почему уголовный мир предпочитает bitcoin», Reuters, Март 2014. (Источник: http://www.reuters.com/article/2014/03/14/us-bitcoin-criminals-insight-idUSBREA2D09820140314)
[13] «ФБР опасается популярности bitcoin среди преступников», Wired, Сентябрь 2012. (Источник: http://www.wired.com/2012/05/fbi-fears-bitcoin/)
[14] «Что можно приобрести за bitcoin в уголовном мире», Cybercrime Review, Май 2012. (Источник: http://www.cybercrimereview.com/2012/05/what-bitcoins-can-buy-you-in-criminal.html)
[15] Описание работы сети Bitcoin дано в Модуле 1.

Напомним, что характерной чертой сети Bitcoin является наличие общедоступного реестра совершенных платежей. После подтверждения транзакции регистрируются в реестре. Напомним также, что право собственности на bitcoin определяется связью определенного количества bitcoin с конкретным адресом. Посредством транзакций в сети Bitcoin осуществляется передача прав собственности на определенное количество bitcoin с одного адреса на другой. Каждая операция, таким образом, содержит данные адресов отправителя и получателя, а также сумму передаваемых bitcoin.

Однако, помимо регистрационной записи о совершении транзакции и данных о двух адресах, не существует никакого способа связать один Bitcoin-адрес с другим. Также нет никакой возможности связать Bitcoin-адрес с каким-либо лицом из реального мира. И на самом деле, отличить транзакцию, при которой один единственный человек контролирует и адрес отправителя, и адрес получателя, от транзакции, в которой эти два адреса контролируются разными людьми, невозможно.

Особенность анонимности, которую предлагают такие децентрализованные виртуальные валюты, заключается в том, что, хотя и не трудно отследить поток значений, передаваемых через сеть Bitcoin, понять, как этот поток связан с передачей ценностей между различными сторонами в реальном мире, представляется чрезвычайно сложным.

В некоторых очень ограниченных случаях можно связать транзакции по получению/отправке bitcoin с/на конкретный Bitcoin-адрес с определенным IP-адресом. Однако, использование технологий, скрывающих трафик, значительно осложняют выполнение такой задачи[16].

В отличие от децентрализованных виртуальных валют, вполне возможно, что администраторы централизованных виртуальных валют хранят некоторую информацию об операциях, такую как источник финансирования; счет, на который была зачислена виртуальная валюта; информация о движении виртуальной валюты между счетами или о конвертации ее в фиатную валюту. Такое представляется возможным в тех случаях, когда администратор либо непосредственно занимается обменными транзакциями, либо выступает посредником в таких операциях. Однако, в большинстве случаев контроль, который осуществляют администраторы виртуальных валют, направлен скорее на предотвращение мошенничества, а не на борьбу с отмыванием денег. Более детально этот вопрос будет рассмотрен в следующей главе.

3.3 Недостаточные данные об операциях

Как уже упоминалось в предыдущей главе, не исключено, что администраторы централизованных виртуальных валют хранят информацию о транзакциях. Такая информация может включать контактные данные пользователей, источники финансирования, данные о

[16] https://www.torproject.org/

конвертации фиатной валюты в виртуальную, о движении виртуальной валюты между счетами, о конвертации виртуальной валюты в фиатную или другую виртуальную валюту.

Однако, отсутствие юридически закрепленного обязательства к администраторам виртуальных валют как элемента всеобъемлющей нормативной базы по регулированию виртуальных валют, означает, что администраторы и биржи виртуальных валют могут не сохранять данные, которые, как правило, сохраняются традиционными финансовыми учреждениями.

В действительности в прошлом были случаи, когда биржи виртуальных валют не требовали какой-либо реальный удостоверяющий личность клиента документ. Например, закрытый Департаментом юстиции США в мае 2013 года Liberty Reserve требовал для видимости базовые идентификационные данные, однако, их достоверность не проверялась. Пользователи создавали счета на вымышленные имена, в том числе, на имена, явно относящиеся к криминальной среде («Хакерский счет», «Мошенник Джо»), и указывали явно вымышленные адреса («123 Поддельная Главная Улица, «Чистой Выдумки Город Нью-Йорк»). Также Liberty Reserve требовал от своих пользователей производить операции по депонированию и снятию денег через определенные обменники, которые, как правило, либо были нелицензированы, либо находились в юрисдикциях со слабыми режимами регулирования и контроля в сфере противодействия отмыванию денег. Не проводя непосредственно операций по депонированию и снятию денег, Liberty Reserve удалось, таким образом, уйти от необходимости собирать информацию о пользователях, обычно необходимую в случае осуществления банковских операций или другой финансовой деятельности[17].

Но даже в случаях, когда не предпринимаются умышленные действия, направленные на сокрытие идентификационных данных участников операций, отсутствие нормативных требований по обязательному хранению данных означает, что администраторы и обменники могут не хранить информацию, которая имела бы очень важное значение для расследования. Информация об источниках финансирования, записи по надлежащей проверке клиентов и данные об операциях хранятся, если они вообще собиралась, только до тех пор, пока это имеет смысл с коммерческой точки зрения. Поэтому сроки хранения таких данных могут оказаться недостаточными для целей расследований, в частности, для международных расследований.

Вдобавок к этому, учитывая отсутствие должного регулирования, ни администраторы, ни биржи виртуальных валют могут не иметь никаких обязательств по предоставлению сообщений о подозрительных операциях.

---

[17] «Прокурор Манхэттена выдвигает обвинения против Liberty Reserve, одной из крупнейших мировых компаний цифровых валют, а также семи ее руководителей и сотрудников за организацию схем по отмыванию $ 6 млрд.», Департамент юстиции США, Май 2013 (Источник: http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php?print=1)

3.4 Установление фактов использования виртуальных валют

Относительно слабая изученность виртуальных валют (по сравнению с наличными деньгами, платежными картами или другими формами онлайновых платежей) может стать проблемой для установления фактов использования виртуальных валют для отмывания денег.

Понимание того, что подозреваемые, возможно, использовали виртуальные валюты для отмывания преступных доходов, потребует от следственных органов знаний об особенностях виртуальных валют, а также технических возможностей по сбору необходимых доказательств. Следственные инструменты, такие как красные флажки / индикаторы, могут оказаться полезными для выявления фактов использования виртуальных валют.

Помимо этого, для выявления отмывания денег, совершенного посредством виртуальных валют, должна быть соответствующая правовая база.

3.5 Сложные / запутанные модели транзакций

Отсутствие связи между счетами в виртуальных валютах и реальными людьми в сочетании с возможностью иметь неограниченное множество счетов создает благоприятную почву для создания новых сложных моделей, направленных на сокрытие криминального происхождения средств.

Для примера рассмотрим тот факт, что любой пользователь сети Bitcoin может создать любое количество адресов. Транзакции между двумя адресами, оба из которых контролируются одним и тем же человеком, не отличаются от операций, в которых разные люди контролируют эти адреса. Таким образом, теоретически злоумышленники могут провести, к примеру, 100 000 Bitcoin-транзакций между адресами, которые ними же и контролируются, перед тем, как преобразовать bitcoin в другую форму. Восстановление такой цепи операций, особенно если это делается вручную, заняло бы, как минимум, очень много времени, если бы вообще оказалось возможным. Такой прием может быть частью сложной схемы по отмыванию денег с использованием нескольких лиц, виртуальных валют и т.д.

Так же, как и первичная торговля виртуальными валютами, которая происходит с администраторами или биржами виртуальных валют, вторичная торговля виртуальными валютами, как, например, при использовании Интернет-аукционов или других торговых площадок, также создает благоприятные возможности для увеличения сложности проведения расследования транзакций.

3.6 Отсутствие ограничений по сумме

В случае с централизованными виртуальными валютами администратор имеет возможность ввести ограничение по максимальной сумме операции. Но такие меры, как правило, направлены на предупреждение потенциального мошенничества [18]. Аналогичным образом биржи виртуальных валют могут устанавливать ограничения по сумме для новых счетов. Но, опять же, такие меры применяются, как правило, для минимизации рисков мошенничества.

Любые суммы без ограничений или контроля могут быть переведены при помощи децентрализованных виртуальных валют. В случае с bitcoin, например, сумма сделки никак не влияет на алгоритм проведения транзакции. До тех пор, пока владелец определенного Bitcoin-адреса может подтвердить свои права собственности на определенное количество bitcoin, он имеет возможность перевести все это значение на один или несколько Bitcoin-адресов, независимо от количества передаваемых bitcoin.

4 Типологии

Рассмотрев в предыдущем разделе трудности, которые виртуальные валюты представляют собой для выявления и расследования отмывания денег, в этом разделе будут рассмотрены способы, используемые злоумышленниками, чтобы воспользоваться этими угрозами в своих преступных целях. Ранее были проведены два важных типологических исследования, в которых собраны практические и типологические примеры, предоставленные ПФР разных стран:

1. «Новые способы платежей, используемые для отмывания денег», опубликованное ФАТФ в октябре 2010 [19] (именуемый ниже как ФАТФ-НСП).
2. «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», опубликованное Международным проектом Совета Европы по борьбе с киберпреступностью и МАНИВЕЛ в марте 2012[20] (именуемый ниже как СЕ-КДП).

В этом разделе будет проведен анализ вышеуказанных двух источников, обращая особое внимание на содержащиеся в них типологии. Приведенные примеры также, в основном, взяты из этих двух исследований.

---

[18] https://secondlife.com/my/lindex/describe-limits.php (требует входа с помощью счета Second Life).

[19] «Новые способы платежей, используемые для отмывания денег», ФАТФ-ГАФИ, Октябрь 2010. (Источник: http://www.fatf-gafi.org/media/fatf/documents/reports/ML using New Payment Methods.pdf)

[20] «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», Международный проект Совета Европы по борьбе с киберпреступностью и МАНИВЕЛ, Март 2012. (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

4.1 Использование виртуальных валют

Определение цифровой / электронной валюты, данное в СЕ-КДП отличается от используемого в данном пособии понятийного аппарата. Так, цифровая / электронная валюта в СЕ-КДП определена таким образом:

«Электронные или цифровые валюты относятся к системам обмена ценностей, которые осуществляются электронно. Электронная валюта – это зашифрованный код, представляющий собой некую стоимость, привязанный к определенному «счету», т.е. как и обычные бумажные банкноты, обладающие определенными характерными чертами, позволяющими перевести их в символьную ценность.»[21]

Хотя данное определение отличается от использующегося в настоящем пособии, очевидно, что феномен, о котором идет речь, один тот же. Грубо говоря, можно сказать, что «цифровая / электронная валюта» в СЕ-КДП соответствует определению «цифровая валюта», данное в Модуле 1 настоящего пособия. Напомним, что данное в Модуле 1 определение «цифровая валюта» включает в себя как «виртуальные валюты», так и «электронные деньги».

Как указывалось, в главе 3, такие характеристики транзакций с виртуальными валютами, как скорость, невозвратность и анонимность, делают их привлекательными для целей отмывания денег. Эта точка зрения в СЕ-КДП была сформулирована следующим образом:

«Киберпреступники и лица, отмывающие деньги, обычно используют системы цифровых или электронных валют, которые предлагают в зависимости от их эмитента различный уровень анонимности, и дают возможность осуществлять мгновенные безналичные расчеты и небольшой шанс возврата или даже отсутствие такового. Некоторые системы почти всегда используются преступниками, включая, но не ограничиваясь только ими, например, e-Gold, WebMoney.ru, Liberty Dollars, Pecunix, Liberty Reserve, Fethard и E-Bullion.» [22]

Аналогичная точка зрения содержится в ФАТФ-НСП:

«Анонимность, большое количество мест, в которых принимается оплата с помощью новых способов платежей, возможность осуществления различных операций, а также возможность снятия наличных денег через банкоматы являются одними из главных факторов, повышающих привлекательность новых способов платежей для преступных элементов, занимающихся отмыванием денег. Анонимность может быть обеспечена «непосредственно» – путем использования по-настоящему анонимных продуктов (т.е. не требующих какой-либо идентификации личности клиента). Кроме того, анонимность может быть достигнута «косвенным

[21] СЕ-КДП, Глава 3.1.7, Параграф 181.
[22] Предоставлено США, СЕ-КДП (Параграф 186).

образом» – посредством незаконного использования персональных продуктов (т.е. путем ухода от проверки личности с помощью поддельных или украденных удостоверений личности либо за счет использования фиктивных или подставных лиц, и т.д.).»[23]

Под новыми способами платежей (НСП) подразумеваются предоплаченные карты, мобильные платежи и платежные сервисы в сети Интернет. Услуги по оплате через Интернет включают в себя платежи посредством цифровых / электронных валют. [24] Таким образом, это еще раз свидетельствует, что феномен, о котором идет речь в ФАТФ-НСП, идентичен тому, который в настоящем пособии определяется термином «виртуальная валюта».

Несмотря на возможные различия в терминологии, в указанных двух типологических исследованиях представлены многочисленные примеры использования виртуальных валют для отмывания преступных доходов. Рассмотрим их в последующих главах.

4.2 Администраторы и биржи виртуальных валют

Администраторы и биржи виртуальных валют регулируются лишь в некоторых юрисдикциях и в определенной степени. Учитывая присущий виртуальным валютам трансграничный характер, этот факт представляет собой проблему с точки зрения выявления и расследования преступлений по отмыванию преступных доходов. В СЕ-КДП эта проблема неоднократно подчеркивалась, в частности, таким образом:

«В большей части поступивших от стран ответов было указано на то, что деятельность поставщиков платежных услуг урегулирована в недостаточной степени или за ними осуществляется слабый надзор в части выполнения требований ПОД/ФТ. Слабый контроль со стороны регулятора или отсутствие такового – это ключевой фактор риска как для учреждений, так и для юрисдикций наряду с отсутствием или недостаточным санкционным режимом.

Одной из трудностей в части лицензирования и надзора является то, что юрисдикция регистрации и юрисдикция, где осуществляется основная деятельность, не совпадают. В некоторых случаях проблемой может стать отсутствие специального законодательства для поставщиков финансовых услуг.»[25]

Иным типичным случаем, согласно ФАТФ-НСП, является соучастие в незаконной деятельности администраторов и бирж виртуальных валют, а также их сотрудников.

---

[23] ФАТФ-НСП, Краткий обзор, Параграф 5.
[24] ФАТФ-НСП, Глава 2.2, Параграфы 43-45.
[25] СЕ-КДП, Глава 2.4.3, Параграфы 118-119. См. также Главу 2.4.4.

«В ряде представленных случаев фигурируют эмитенты предоплаченных карт и провайдеры УИП[26], которые контролируются преступниками и которые либо намеренно, либо по неосторожности содействуют осуществлению деятельности по отмыванию денег и финансированию терроризма. В указанных случаях ограничения по выходу на рынок, как, например, проверка на профессиональную пригодность и добросовестность, оказались либо не эффективны, либо не применимы к той или иной организации, находящейся на территории соответствующей юрисдикции»[27]

Ниже приводится пример соучаствующей в незаконной деятельности валютной биржи.

И наконец, особое внимание в СЕ-КДП обращается на тот факт, что биржи (обменники) виртуальных валют, в частности те, которые предлагают услуги по конвертации одной виртуальной валюты в другую, представляют собой особый риск:

«Легкая конвертация в различные виртуальные валюты и счета, выполняемая так называемыми «менялами» предоставляет преступникам замечательную возможность скрыть средства.»[28]

Подводя итог, еще раз назовем типологии, связанные с администраторами и биржами виртуальных валют:

1. Применение схем юридического или коммерческого структурирования с целью использования слабых мест в регулировании.
2. Причастность провайдеров услуг или их сотрудников к деятельности по отмыванию денег.
3. Конвертирование одной виртуальной валюты в другую при помощи бирж (обменников) виртуальных валют.

[26] Услуги Интернет-платежей.
[27] ФАТФ-НСП, Глава 4.3, Параграф 130.
[28] СЕ-КДП, Параграф 187 (предоставлено Германией)

Пример: Причастные провайдеры услуг или их сотрудники

«Пример 33: Отмывание денег с помощью провайдера услуг, связанных с электронными драгоценными металлами.

В 2008 году Интернет-провайдер услуг электронных валют, а также три главных директора и владельца данного предприятия признали себя виновными по всем пунктам уголовного обвинения в отмывании денег и осуществлении деятельности, связанной с незаконным перечислением денежных средств.

Определенные возможности, предоставляемые указанным провайдером услуг электронных валют, как, например, отсутствие необходимости указывать не только свою настоящую личность, но и какие-либо идентификационные данные вообще, привлекли к нему пользователей, занимающихся незаконной деятельностью. Указанный провайдер позволял открывать счета без проверки личности пользователя, несмотря на то, что ему было известно об их использовании для совершения преступлений, в том числе таких, как эксплуатация детского труда, инвестиционные аферы, мошенничество с кредитными картами, отмывание денег и хищение персональных данных. Кроме того, мониторинг сотен тысяч счетов осуществлялся в указанной компании лицами, не имевшими необходимого опыта работы. Компания также участвовала в разработке системы, в рамках которой пользователей, о преступной деятельности которых становилось известно, прямо призывали перечислять незаконные средств через другие счета данной компании. В отличие от других провайдеров УИП, указанная компания не включила в свое пользовательское соглашение каких-либо положений, запрещающих использование ее услуг для осуществления преступных действий.

Источник: США»[29]

4.3 Финансирование третьими лицами

И в ФАТФ-НСП, и в СЕ-КДП обсуждается тот факт, что возможность использования в качестве источника финансирования для покупки виртуальной валюты переводов от одного лица другому дает причастным третьим лицам возможность совершать платежи на счета в виртуальной валюте для целей отмывания денег.

В СЕ-КДП подробно рассматривается вопрос использования денежных мулов с целью отмывания преступных доходов в сети Интернет. Использование денежных мулов резюмировалось следующим образом:

[29] ФАТФ-НСП, стр. 45.

«Мулы получают на свои банковские счета средства, например, со взломанных онлайновых банковских счетов и могут их перевести на другие счета или обналичить их, используя иные средства, такие как системы по переводу денег или электронные деньги. Мул удерживает комиссию, являющейся частью операции.»[30]

Обратите внимание, что в СЕ-КДП подчеркивается, в частности, тот факт, что средства, которыми оперирует мул, могут быть источником финансирования виртуальной валюты.

Третьи лица могут быть либо добровольными участниками преступления по отмыванию денег, либо оказаться втянутыми обманным путем в качестве мула. Типичный прием для вербовки ничего не подозревающих денежных мулов – размещение на рекрутинговых сайтах фальшивых объявлений о работе. Такие объявления часто содержат такие привлекающие внимание фразы, как «финансовый менеджер» или «работа на дому».

Пример: Отмывание денег с использованием цифровых валют и с помощью подставного лица

«Пример 11: Использование электронных денег для целей мошенничества в Интернете и отмывания денег

Молодой человек, действующий в качестве подставного лица, открыл счет в электронной валюте для получения доходов от кражи средств с банковских счетов в Интернете, осуществляемой его знакомым, находившимся за рубежом. После этого он попытался снять деньги со счета электронной валюты, обратившись в пункт обмена электронных валют с просьбой выдать ему почтовые платежные поручения. Для того, чтобы скрыть свою личность, он сообщил, что потерял паспорт и попросил сотрудника обменного пункта позвонить в контору компании, оказывающей денежные услуги, и сообщить им, что человек с его внешностью придет в их контору в определенное время для получения наличных по платежному поручению. Предполагалось, что он не собирался отправлять деньги за рубеж, а оставить весь доход себе. Он был арестован и предстал перед судом.

Источник: Австралия»[31]

[30] СЕ-КДП, Глава 3.1.5, Параграф 168.
[31] ФАТФ-НСП, стр. 39.

Пример: Банковское мошенничество и отмывание денег при помощи мулов и виртуальных валют

«Банк предлагал своим клиентам дистанционное банковское обслуживание с тем, чтобы последние могли осуществлять операции со своими счетами с домашнего компьютера. У некоторых клиентов счета были взломаны. Денежные средства с их счетов были переведены на счета в других странах. Компьютеры жертв были заражены вредоносными программами, что позволило украсть реквизиты счетов и иные персональные данные (возможно, как часть бот-сети). Международное расследование, проводимое представителями всех заинтересованных государств, позволило выявить большую и сложную систему связей денежных мулов, которая охватывала по меньшей мере порядка десяти стран и огромные суммы похищенных средств.

Мулов вербовали на разных языках при помощи рассылки сообщений, предлагавших легкий способ заработать деньги. С теми, кто «клюнул» связывались по телефону или посредством Протокола передачи голоса через Интернет (VOIP), который очень сложно отследить и за использование которого оплата осуществлялась при помощи карточек-клонов или украденных дебетовых карт. Мулам «первого уровня» давалось указание открыть банковский счет. По прошествии нескольких дней на их счета поступали деньги. Затем с ними снова связывались и отдавали распоряжения перевести их денежные средства в страны Восточной Европы. В Бельгии такое явление считается отмыванием денег.

Мулы «второго уровня», находившиеся в большинстве своем в странах Восточной Европы, снимали их со счета и отдавали наличные третьим лицам – «сборщикам денег». Мулы обоих уровней ничего не знали об источнике происхождения этих денег. Сборщика денег информировали по электронной почте о сумме, которая должна быть получена, коде операции, осуществленной поставщиком услуг по переводу денег. Также сообщались имена и адреса мулов первого и второго уровня. Сборщик денег передавал деньги четвертому лицу, е-банкиру, который переводил их в WebMoney.

В расследуемом деле через сборщика денег прошло 150,000 долларов США два месяца.

Все эти процессы были хорошо организованы и доведены до автоматизма. Это дает основание полагать, что к организации приложил руку менеджер, имевший широкий доступ к данным или лицо, подобное ему.

Источник: Бельгия»[32]

[32] CE-КДП, стр. 49.

4.4 Использование заочного характера виртуальных валют

Большинство операций с виртуальными валютами предполагают минимальный или не предполагают вообще контакт «лицом к лицу». Такое положение вещей способствует тому, что виртуальные валюты используются преступниками для целей отмывания денег.

Одна категория случаев использования виртуальных валют в криминальных целях включает в себя сценарий, при котором преступники получают контроль над счетами законных пользователей и возможность осуществлять операции с их использованием. ФАТФ-НСП сообщает о двух возможных ситуациях, ранее имевших место:

- Первый случай связан со взломом счетов в невиртуальных валютах, принадлежащие законным клиентам. Деньги украдены и использованы для финансирования счета в виртуальной валюте:

  «В ряде случаев продукты, связанные с новыми способами платежей, использовались для отмывания незаконных доходов после хищения персональных данных или кражи денег с банковских счетов или кредитных / дебетовых карт посредством взлома компьютерных сетей или «фишинга». Поскольку банковские счета или кредитные и дебетовые карты были изначально открыты на имя законных клиентов, преступники могли использовать их в качестве счетов, с которых будут поступать деньги для размещения средств на предоплаченные карты или счета, или использовался для осуществления Интернет-платежей. В этих случаях провайдеры НСП не могли установить, что операции проводились не их законными клиентами, а также не могли выявить никакой другой подозрительной деятельности.»[33]

- Во втором случае идентификационные данные законных клиентов похищались и использовались для создания счетов в виртуальных валютах, которые затем использовались в качестве транзитных счетов для целей отмывания незаконных доходов:

  «В других случаях украденные или поддельные персональные данные использовались для открытия счетов НСП, которые также использовались в качестве транзитных счетов для отмывания незаконных доходов, либо для одновременного совершения преступлений (например, мошенничества) и отмывания денег.»[34]

Вторая категория случаев использования заочной природы НПМ связана с использованием анонимного характера некоторых таких услуг. В СЕ-КДП эта проблема сформулирована следующим образом:

[33] ФАТФ-НСП, Глава 4.2, Параграф 126
[34] ФАТФ-НСП, Глава 4.2, Параграф 127

«В некоторых юрисдикциях электронные платежи осуществляются анонимно. Также необходимо отметить, что оборот электронных денег осуществляется вне банков и, как результат, вне банковской системы надзора. Банки выступают в качестве агентов, которые вводят деньги в электронную платежную систему или выводят их из нее, а в некоторых случаях как эмитенты электронных денег.»[35]

В отличие от приведенной в СЕ-КДП точки зрения, по всей видимости, взаимодействие финансовых учреждений с виртуальными валютами весьма ограниченное[36]. На практике все большее количество центральных банков выступают против использования виртуальных валют. [37] Использование электронных денег (цифрового выражения фиатной валюты) в отличие от виртуальных валют становится все более распространенным явлением. Но такая форма цифровой валюты подпадает под действие установленной системы финансового мониторинга.

Таким образом, резюмируя вышесказанное, типологии, связанные с заочной природой виртуальных валют, могут быть классифицированы следующим образом:

1. Использование присущего некоторым виртуальным валютам анонимного характера. Децентрализованные виртуальные валюты, такие как bitcoin, имеют высокую степень анонимности. Это связано, прежде всего, с тем, что не существует никакой связи между Bitcoin-адресами и индивидуумами из реального мира.

2. Использование возможностей по анонимному пополнению счетов в виртуальных валютах. И централизованные, и децентрализованные виртуальные валюты могут быть анонимно приобретены, как в силу их заочной природы (рассматривалось в этой главе), так и при содействии сторонних лиц (рассматривалось в главе 4.3)

[35] Предоставлено Российской Федерацией, СЕ-КДП, Параграф 189.
[36] «Биржа Bitcoin проходит процедуру по получению лицензии на осуществление полноценной банковской деятельности во Франции», The Verge, Декабрь 2012. (Источник: http://www.theverge.com/2012/12/7/3740136/bitcoin-exchange-bank-france-bitcoin-central).
[37] http://www.virtualcurrencyreport.com/files/2014/03/Virtual-Currencies_International-Chart.pdf

Пример 1

«Министерство внутренних дел получило информацию от компании «WM Transfer» о том, что неидентифицированный пользователь их системы нарушил контракт с администрацией сайта и похитил 60,000 долларов США со счета компании. Затем в США была открыта платежная система «E-GOLD». Преступник пополнял счет при помощи банковской карты с использованием платежной системы «WM Transfer», а затем обналичивал средства.

Сотрудники правоохранительных органов задержали лицо, которое пыталось получить деньги в банке в размере 14,000 долларов США, используя паспорт и платежную карту другого лица. Были конфискованы паспорт, сим-карты к мобильному телефону, банковские платежные карты. Был выявлен IP-адрес, с которого осуществлялся незаконный доступ в Интернет и использовалось компьютерное оборудование. Оборудование было использовано для присвоения чужого имущества (т.е. кошелек обменного пункта) путем мошенничества.

В результате расследования Министерство внутренних дел возбудило уголовно дело по ст. 361, Раздел 2 Уголовного кодекса. Были задержаны двое подозреваемых: один – выходец из Кавказа, который организовал снятие наличных через банкоматы с использованием поддельных и утерянных паспортов граждан Украины, другой был осужден на 3,5 года за совершение подобных преступлений, но был освобожден условно-досрочно. Уголовное дело вместе в обвинительным актом было передано в суд.

Источник: Украина»[38]

[38] CE-КДП, стр. 52

Пример 2

«Пример 25: Отмывание незаконно полученных доходов через провайдера электронных денег.

В 2009 году подозреваемый незаконным образом получил доступ к банковским Интернет-счетам физических лиц и отдал распоряжение компьютерной системе перевести примерно 740 000 иен (8 300 долларов США) в пункт обмена электронных валют для получения электронных денег. После этого обвиняемый продал часть электронных денег в другой пункт обмена электронных валют за реальные деньги. И, наконец, обвиняемый отдал распоряжение сотрудникам пункта обмена электронных валют перевести деньги на несколько банковских счетов, которые были открыты незаконным образом и контролировались обвиняемым.

Источник: Япония»[39]

4.5 Связь с другими методами отмывания денег

Как указывалось, ранее, виртуальные валюты могут использоваться в сочетании с другими платежными технологиями, например, с предоплаченными картами, для того, чтобы увеличить количество используемых в схеме методов отмывания преступных доходов. В частности, ФАТФ-НСП описывает это следующим образом:

*«**Услуги Интернет-платежей становятся все более взаимосвязанными с различными новыми и традиционными платежными услугами**. В настоящее время деньги могут быть переведены или получены с помощью различных способов платежей: путем передачи наличных денег, с помощью услуг денежных переводов (например, Western Union), посредством новых способов платежей, банковским телеграфным переводом, а также с помощью кредитных карт. Более того, некоторые провайдеры услуг Интернет-платежей стали предоставлять своим клиентам предоплаченные карты, давая им, таким образом, возможность **снимать наличные деньги через сети банкоматов во всем мире**»*[40] [выделение шрифтом присутствует в исходном документе].

Та же проблема в СЕ-КДП описана так:

«В отличии от «традиционного» отмывания денег, для совершения которого используется банковская система, кибер-отмывание основано на использовании различных видов операций и поставщиков финансовых услуг, начиная банковскими переводами, внесением/снятием наличных,

39 ФАТФ-НСП, стр 43.
40 ФАТФ-НСП, Section 2.2, Параграф 47

использованием электронных денег, и заканчивая денежными мулами и услугами по переводу денег. Таким образом, выявление и преследование преступных денежных потоков является очень сложной задачей для правоохранительных органов.

Обычно цепочка прерывается на операциях с наличными средствами, совершаемыми как правило денежными мулами, за которой иногда следует использование традиционной платежной системы. Если соответствующий платежный сервис интегрирован с услугами по онлайновым платежам, то деньги могут быть обменены на электронные и без промедления практически анонимно переведены в другое государство.»[41]

Ниже приводятся несколько дополнительных примеров, демонтирующих использование нескольких методов, в том виртуальных валют, с целью создания еще более сложных схем отмывания денег.

Пример 1

«Пример 30: Предполагаемое использование УИП (в т.ч. услуг, связанных с электронными драгоценными металлами) и предоплаченных карт многоэмитентных (открытых) систем для отмывания денег, полученных в результате мошенничества.

Расследование данного случая было начато после получения информации от одного из правоохранительных органов и одного из иностранных подразделений финансовой разведки (ПФР) о том, что некий канадский провайдер УИП, его филиал в США и иные ассоциированные предприятия предположительно причастны к отмыванию преступных доходов, полученных в результате использования схемы Понци (финансовой пирамиды) и мошеннических схем телемаркетинга.

Было установлено, что у данного провайдера УИП из Канады также имелись филиалы в одной из европейских стран и в одной из стран Азии. Кроме того, было обнаружено, что в данной сложной схеме по отмыванию денег участвовали (преднамеренно или непреднамеренно) не менее пяти контор по обмену электронных валют (расположенных в Канаде, США и в одной из стран Северной Европы), два провайдера услуг, связанных с драгоценными металлами (из США), и три эмитента предоплаченных карт многоэмитентных (открытых) систем (из Канады и США). Было установлено, что один из эмитентов предоплаченных карт многоэмитентных (открытых) систем предложил виртуальным игрокам использовать такие предоплаченные карты для пополнения виртуальных счетов и обналичивания виртуальных валют через банкоматы.

Как правило, денежные средства, поступающие из других стран на счета банков в Канаде, принадлежавшие канадскому провайдеру УИП и

[41] СЕ-КДП, Глава 2.4.5, Параграфы 130-131.

эмитентам предоплаченных карт, использовались либо для пополнения предоплаченных карт, либо для расчета65 с другими провайдерами УИП и эмитентами предоплаченных карт из других стран. В некоторых случаях подозрительные средства поступали в финансовую систему Канады, откуда впоследствии перечислялись в другие страны в рамках операций, направленных на сокрытие незаконных источников их происхождения («расслоение» денежных средств). В ряде случаев такие средства в конечном итоге возвращались в Канаду.

Подозрительные транзакции также включали в себя выставление банковских тратт и крупные взносы наличными на банковские счета, после совершения которых средства зачастую перечислялись с помощью электронных денежных переводов (ЭДП) в другие страны в рамках операций, направленных на сокрытие незаконных источников их происхождения («расслоение» денежных средств) с использованием различных банковских счетов.

Источник: Канада»[42]

[42] ФАТФ-НСП, стр. 44-45.

Пример 2

«Пример 31: Отмывание незаконных средств с помощью электронных валют и предоплаченных карт

При проведении расследования было установлено, что международная преступная группировка использовала одного из провайдеров финансовых услуг для перечисления незаконных денежных средств в восточно-европейские страны, в которых члены данной группировки обналичивали и обращали указанные средства в электронные деньги в конторах по обмену электронных валют.

Электронные деньги перечислялись на счета, открытые членами данной группировки у одного из провайдеров финансовых услуг, занимавшегося операциями с электронной валютой в указанных странах. Указанный провайдер финансовых услуг выпускал, совместно с одним оффшорным банком, предоплаченные карты MasterCard «Cirrus», которые можно было приобретать анонимно и вносить на них суммы в электронной валюте. Такие карты можно было использовать в любых странах – в банкоматах и при оплате покупок через терминалы, принимающие карты «Cirrus».

Данная схема позволяла преступникам эффективно скрывать незаконные денежные средства и обеспечивала быстрый и анонимный доступ к таким средствам.

Источник: Германия»[43]

[43] ФАТФ-НСП, стр. 45.

5 Следственные трудности

В предыдущих разделах были рассмотрены угрозы, свойственные виртуальным валютам, а также некоторые используемые преступниками способы эксплуатации этих угроз для целей отмывания денег. Выявление и расследование отмывания преступных доходов, совершенного с помощью виртуальных валют, сталкиваются с некоторыми специфическими сложностями, которые мы и рассмотрим в этом разделе.

5.1 Недостаток знаний

Реальность такова, что уровень знаний следователей и прокуроров о виртуальных валютах и их возможностях, а также об инструментах и методах эффективного проведения расследований преступлений, совершенных посредством виртуальных валют, весьма ограничены.

К тому же, учитывая относительную новизну этого феномена, имеется очень немного специалистов с практическим опытом в проведении расследований, связанных с виртуальными валютами.

Трудности организации и проведения соответствующего обучения, а также проблемы инкорпорирования такого обучения в программу профессиональной подготовки соответствующих специалистов, ранее уже исследовались[44].

5.2 Ставка на электронные доказательства

Возможности использования виртуальных валют непосредственно связаны с информационно-коммуникационными технологиями. Виртуальные валюты функционируют в онлайновой среде. И все такого рода операции, так или иначе, связаны с компьютерными системами и данными. Характерной особенностью указанных транзакций является фактическое отсутствие «бумажного следа», за исключением немногочисленных операций по обмену виртуальной валюты в фиатную или наоборот. Но актуальность такого «бумажного следа» в контексте расследований преступлений, совершенных с использованием виртуальных валют, также невелика. Поэтому с точки зрения незаконного использования виртуальных валют доказательная база совершения преступления будет состоять почти полностью из электронных доказательств и этот факт является принципиальным моментом, как для правоохранительных органов, так и для подразделений финансовой разведки.

Электронные доказательства – это полученная, хранимая или переданная с помощью электронных устройств информация, которая может быть

[44] См., к примеру, «Обучение судей и прокуроров в вопросах компьютерных преступлений: концепция», Совет Европы, Октябрь 2009. (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf)

использована в суде. [45] В отличие от традиционных для уголовного судопроизводства форм доказательств, как например, документы, фотографии, показания свидетелей и т.д., источником электронных доказательств являются компьютерные системы и их периферийные устройства. Такие системы и устройства могут разительно отличаться с точки зрения технологии и принципов функционирования. К ним, среди прочего, относятся: компьютерные сети, мобильные телефоны, цифровые камеры, устройства хранения данных, облачные системы хранения данных и Интернет как таковой – все то, что способно создавать, обрабатывать и хранить информацию, которая может быть использована в качестве электронных доказательств.

С точки зрения возможных трудностей электронные доказательства в целом не отличаются от других, традиционных форм доказательств. Они также должны быть подлинными, допустимыми и иметь отношение к делу. Тем не менее, электронные доказательства обладают уникальными характеристиками, которые отличают их от других форм доказательств, что имеет принципиально важное значение в контексте расследования преступлений, совершенных с использованием виртуальных валют:

Сложность выявления: Электронные доказательства часто встречается в тех местах, где найти их могут только специалисты, или в местах, куда можно добраться только с помощью специальных инструментов. Цифровая криминалистическая экспертиза электронных доказательств требует наличия инструментов, подходящих не только для анализа электронных доказательств, но и для изучения и анализа необработанных, несортированных и, казалось бы, не связанных между собой данных, найденных в компьютерных системах;

Необходимость привлечения узких специалистов: Без необходимых экспертных знаний и опыта найденную в компьютерных системах информацию может оказаться невозможным извлечь способом, который бы гарантировал ее аутентичность, неизменность и сохранность. Специалисты также потребуются для того, чтобы установить и правильно обработать доказательства, которые могут иметь отношение к расследованию. Кроме всего привлечение специалистов в области финансов, налогообложения и/или в сфере борьбы с отмыванием денег может оказаться необходимым для целей расследования преступлений, совершенных посредством виртуальных валют.

Высокая волатильность: Компьютерные системы, которые создают, обрабатывают и хранят электронные доказательства, регулярно уничтожают существующие данные при наступлении определенных событий. Например, система автоматического обновления перезаписывает

[45] Комплексное исследование УНП ООН по киберпреступности, стр. 157 и далее. См. также, «Электронные доказательства: базовое руководство для сотрудников полиции, прокуроров и судей», подготовленное в рамках совместного проекта Совета Европы и Европейского Союза по региональному сотрудничеству по борьбе с киберпреступностью, стр. 11 (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp)

старую информацию для того, чтобы освободить место для хранения новой информации. Таким образом, проблема состоит в том, чтобы правильно и своевременно заполучить устройства, на которых могут храниться электронные доказательства, до того, как имеющие важное значение данные будут потеряны.

Склонность к изменениям: Компьютерные системы и устройства постоянно изменяют состояние своей памяти, будь то по запросу пользователя (например, операции «сохранить», «копировать», «обновить») или автоматически операционной системой компьютера (распределение места, временное хранение информации для свопинга, запланированное обновление и т.д.). Эту характеристику важно хорошо понимать, чтобы избежать недооценки временных ограничений и состояний электронных доказательств, а также для того, чтобы быть готовым обрабатывать такие доказательства соответствующим образом с момента их обнаружения.

Неограниченные возможности копирования: цифровая информация может быть скопирована неограниченное количество раз и каждая из копий будет точной и безупречной копией оригинала. Этот уникальное свойство становиться проблемой, когда суд или защита потребует доказать, что предъявленное электронное доказательство является оригинальным. Однако, как только будет доказано равенство оригинала и копии компьютерных данных, а, соответственно, допустимость предъявленного доказательства, проблема может превратиться в преимущество, позволяющее производить многочисленные точные копии оригинала, которые могут быть одновременно предоставлены разным специалистами для проведения анализа и предъявлены суду «как есть» вместе с заключением специалистов. [46]

Таким образом, возможности расследовать дела, связанные с виртуальными валютами, будут напрямую зависеть от наличия специализированных подразделений по сбору и анализу электронных доказательств. Подбор соответствующих кадров, обеспечение надлежащего уровня их квалификации посредством обучения и инвестирование в оборудование и другие ресурсы являются тремя ключевыми опорами, которые определяют потенциал такого специализированного подразделения[47].

[46] Руководство по электронным доказательствам, стр. 11-12.

[47] Главы 6.4, 6.5 и 6.6 исследования «Специализированные подразделения по вопросам киберпреступлений – хорошая практика», подготовленного в рамках совместного проекта Совета Европы и Европейского Союза по региональному сотрудничеству по борьбе с киберпреступностью. (Источник: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf)

5.3 Пробелы в законодательстве

Можно спорить, является ли отсутствие надлежащего регулирования и прямых норм самой большой проблемой для проведения расследования преступлений, совершенных посредством виртуальных валют. Целью этой главы пособия, однако, является не изучение вопросов законодательного регулирования, что уже было сделано в Модуле 1, и не рассмотрение имеющегося инструментария материального и процессуального права и нормативных положений по расследованию преступлений с использованием виртуальных валют, что является предметом рассмотрения Модуля 3. Внимание в этой главе сосредоточено на вопросах, относящиеся к правилам доказывания в контексте надлежащего сбора и обработки электронных доказательств.

Прежде всего, проблема состоит в наличии в национальной системе уголовного правосудия понятия электронных доказательств и его практического использования. Наиболее предпочтительный подход – это гарантировать признание и использование электронных доказательств в уголовном судопроизводстве, предусмотрев специализированные определения в уголовно-процессуальном законодательстве. В большинстве случаев, однако, юристы-практики должны удостовериться, что электронные доказательства должным образом признаются в национальной системе уголовного правосудия, т.е. попадают под всеобъемлющее понятие «документы» или «информация», и являются допустимыми в уголовных разбирательствах на основе одних и тех же стандартов, и процедур (правил доказательств), применимых к другим установленным и признанным формам доказательств.

Кроме того, одним из важных аспектов допустимости электронных доказательств, который часто игнорируется, находится за пределами уголовного и процессуального права и, по большей части, связан с признанием электронных документов в качестве допустимых источников данных и доказательств. Дело в том, что принятые на международном уровне стандарты, касающиеся электронных документов, часто требуют соответствующей электронной подписи, чтобы такие документы имели равный правовой статус с физическими, на бумажном носителе, документами, которые используются в официальном судопроизводстве.[48] Это может привести к дополнительным требованиям приемлемости, которое может оказаться трудно доказать в судах общего права. В сущности, возникает необходимость изучения следователями и прокурорами, участвующих в расследовании об использовании виртуальных валют в криминальных целях, вопроса о допустимости электронных документов как действительных электронных доказательств с точки зрения формата, содержания или уровня национального регулирования.

48 Директива 1999/93/ЕС Европейского парламента и Совета от 13 декабря 1999 года об основах законодательства Сообщества об электронных подписях (Источник: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31999L0093)

Понятие электронных документов особенно важно для финансовых расследований, связанных с виртуальными валютами, так как многие версии и материалы, которые на более поздней стадии могут быть не представлены в качестве доказательств (из стратегических или процессуальных соображений), но могли бы быть или будут использованы для целей финансового или уголовного расследований, могут быть в формате, который отличается от общепринятого формата официально признанных документов. Эта проблема потенциально может быть использована в уголовном судопроизводстве стороной защиты для подрыва доказательной силы представленных доказательств.

Не в последнюю очередь электронным доказательствам, подобно традиционным доказательствам, должны быть гарантирована защита от уничтожения, дополнения или любых других форм изменений, оказывающих существенное влияние на форму и содержание таких доказательств. Сама природа данных и информации, содержащейся в электронной форме, предоставляет более широкие возможности по манипулированию ними в сравнении с традиционными формами доказательств. Это создает определенные сложности для системы правосудия и требует, чтобы обращение с такими данными осуществлялось способом, обеспечивающим неизменную целостность информации. [49] С этой точки зрения основная сложность, связанная с электронными доказательствами в расследованиях о виртуальных валютах, состоит в соблюдении официальных стандартов доказывания. В частности, стандарты доказывания в уголовных делах часто и в значительной мере опираются на традиционные доказательства, в то время как высокая волатильность и подверженность изменениям электронных доказательств способны оказать влияние на соблюдение даже более низких стандартов доказывания («разумные основания для сомнения», «обоснованное подозрение» или «резонное основание»). Следственные органы должны изначально быть готовы к тому, что защита, исходя из стандартов доказывания, будет стараться оспорить допустимость электронных доказательств. Особенно в случае с децентрализованными виртуальными валютами, неотъемлемой характеристикой операций, с которыми является анонимность сторон. Критически важно всегда иметь в виду, что исключение из рассмотрения любых доказательств по причине их несоответствия стандартам доказывания, могут оказать пагубное воздействие на исход всего дела.

[49] Руководство по электронным доказательствам, стр. 10-11.

5.4 Сложности, связанные с регуляторным / надзорным режимом

Требования к финансовым учреждениям о регулировании и соответствии лучшим практикам в сфере противодействия отмыванию денег хорошо известны. В частности:

«Прочие финансовые учреждения должны проходить процедуру лицензирования или регистрации, и их деятельность следует должным образом регулировать, и за ней следует осуществлять надзор или контроль в целях ПОД/ФТ, с учетом риска отмывания денег или финансирования терроризма в этом секторе. Следует, как минимум, применять процедуру лицензирования или регистрации в отношении финансовых учреждений, предоставляющих услуги по переводу денежных средств или ценностей или по обмену денег, и эффективно контролировать их деятельность на предмет соблюдения национальных требований ПОД/ФТ.»[50]

Исходя из используемой ФАТФ терминологии, не возникает сомнений, что провайдеры услуг централизованных виртуальных валют подпадают под определение «финансовые учреждения»[51]. Ситуация гораздо менее понятна в случае с децентрализованными виртуальными валютами. Если пользоваться терминологией ФАТФ, то в случае децентрализованных виртуальных валют не существует финансовых учреждений, которые предоставляли бы услуги перевода денег или ценностей, или обмена валют. Тем не менее, услуги перевода ценностей существуют (сама сеть Bitcoin), как и услуги обмена валют (предоставляются биржами виртуальных валют, которые покупают / продают bitcoin).

Еще более усугубляет проблему, даже если существует соответствующая законодательная основа для регулирования децентрализованных виртуальных валют, тот факт, что практическая реализация функции надзора или регулирования таких валют представляется крайне затруднительной в виду отсутствия какого-либо центрального административного органа (администратора).

---

[50] Рекомендация 26, «Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения – Рекомендации ФАТФ», ФАТФ-ГАФИ.

[51] «Руководство по риск-ориентированному подходу к предоплаченных картам, мобильным платежам и платежных услуг посредством Интернет», ФАТФ-ГАФИ, Июнь 2013. (Источник: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf)

5.5 Уголовное преследование и осуждение

Трудности, связанные с уголовным преследованием за совершение преступлений с использованием виртуальных валют радикально не отличаются от традиционных следственных проблем, так как все страны-участницы ГУАМ имеют схожие уголовно-процессуальные системы, при которых прокуроры осуществляют руководство и контроль в отношении всех уголовных расследований. [52] Таким образом, со всеми ранее перечисленными проблемами, связанные с электронными доказательствами, будут сталкиваться в зависимости от стадии процесса или отведенной законом роли либо следователи, либо прокуроры. Тем не менее, некоторые из специальных полномочий прокуроров, предоставленные им национальными системами уголовного правосудия, заслуживают более внимательного рассмотрения в контексте уголовного преследования за преступления, совершенные посредством виртуальных валют.

Прокуроры по закону обладают дискреционными полномочиями и регулярно пользуются ними при рассмотрении уголовных дел. [53] Дискреционное уголовное преследование означает применение стандартов государственных интересов к конкретным уголовным делам для того, чтобы решетить, возбуждать или продолжать ли уголовное преследование или применить к преступнику альтернативные виды наказания. Это представляется особенно актуальным в случаях, потенциально связанных с отмыванием денег посредством виртуальных валют. Принимая во внимание, что большинство предикатных или вспомогательных преступлений, скорее всего, будут компьютерными преступлениям, наказания за которые гораздо мягче, чем за отмывание денег, существует большая вероятность прекращения производства в обмен на альтернативное наказание. В таких случаях практикующие юристы должны хорошо изучить потенциальную или существующую доказательную базу с точки зрения состоятельности обвинений в отмывании денег для того, чтобы не расстроить возможные перспективные преследования в обмен на более мягкие альтернативные судебные решения.

В большинстве юрисдикций прокуроры имеют право идти на сделку с обвиняемым в обмен на признание ним своей вины. [54] Такие сделки становятся все более популярным инструментом, который позволяет обвиняемому в ускоренном режиме (отправления правосудия) получить значительно меньшее наказание или вообще быть освобожденным от уголовной ответственности в обмен на сотрудничество со следствием. С точки зрения расследования преступлений, связанных с виртуальными валютами, сделки со следствием о признании обвиняемым своей вины

[52] Статья 84 Уголовно-процессуального кодекса Азербайджанской Республики; статья 33 Уголовно-процессуального кодекса Грузии; статья 52 Уголовно-процессуального кодекса Республики Молдова; статья 36 Уголовно-процессуального кодекса Украины.

[53] Например, статьи 16 и 166-168^2 Уголовно-процессуального кодекса Грузии.

[54] Например, Раздел XXI Уголовно-процессуального кодекса Грузии; Раздел III Уголовно-процессуального кодекса Республики Молдова.

скрывают в себе риски, аналогичные дискреционным полномочиям. Вполне вероятны случаи, когда обвиняемые предпочтут признать себя виновными в совершении менее тяжелых компьютерных преступлений, чтобы избежать обвинений в отмывании денег, предусматривающих более суровое наказание к тому же с конфискацией преступных доходов. Тем не менее, сделки со следствием о признании обвиняемым своей вины могут быть очень эффективным инструментом для следствия, предоставляя следователям доступ к информации, получение которой иным способом потребовало бы много времени и усилий.

Наконец, прокуроры имеют уникальную возможность влиять на эффективность уголовного процесса путем создания, при необходимости, совместных следственных групп, включающих в себя следователей и экспертов из различных ведомств и сфер. И хотя есть неоспоримые выгоды от объединения усилий финансовых экспертов, специалистов по киберпреступности и следователей, специализирующихся в расследованиях по отмыванию денег посредством виртуальных валют, для проведения эффективного расследования может возникнуть необходимость в надлежащем руководстве, принимая во внимание тот факт, что представители перечисленных профессий используют разные инструменты и методы сбора и анализа доказательств.

С точки зрения потенциальных судебных трудностей, имеющих отношение к виртуальным валютам, все вышеописанное едва ли будет иметь большое значение. Основные судебные проблемы связаны с правильным пониманием судьями узкоспециализированных вопросов, касающихся киберпреступности и электронных доказательств, а также с соответствующим уровнем подготовки судей и наличием у них необходимых знаний, позволяющих им квалифицированно разбирать такие дела. [55]

5.6 Сотрудничество на национальном уровне

В данном пособии пошагово рассматриваются взаимосвязи между компьютерными преступлениями и преступлениями, совершенные посредством виртуальных валют. Учитывая неурегулированный статус виртуальных валют во многих юрисдикциях, преступления, связанные с виртуальными валютами или являющиеся предикатными к их незаконному использованию, на практике часто могут относиться либо ни к чьей, либо к следственной компетенции сразу нескольких ведомств: проводящим финансовые расследования следственным органам, ПФР и подразделению по вопросам киберпреступлений/ высокотехнологичных преступлений. По этой причине основные угрозы, имеющие отношение к вопросам борьбы с киберпреступностью, в равной степени являются актуальными и для виртуальных валют. Один из таких ярких примеров – сотрудничество в национальном и международном уровнях.

[55] Совет Европы, «Судебная подготовка: Вводный курс по киберпреступности и электронных доказательствам для судей и прокуроров», стр. 5-6 (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime.)

Межведомственное сотрудничество на национальном уровне является первостепенной необходимостью как для проведения расследований финансовых и компьютерных преступлений, так и для уголовного преследования за совершение преступлений в сфере информационных технологий. Без надлежащего сотрудничества предоставление сообщений о преступлениях, следственные действия, проведение экспертиз, возврат активов, а также меры по минимизации последствий и различные превентивные меры имели бы небольшие шансы на успех. В рамках национальной системы уголовного правосудия и за ее пределами существует много потенциальных партнеров, чьи знания и возможности очень важны для целей расследования преступлений, связанных с виртуальными валютами.

Основным партнером для правоохранительных органов в раскрытии и расследовании преступлений, связанных с виртуальными валютами, является подразделение финансовой разведки (ПФР). ПФР – специализированное ведомство государственной власти, которое получает от финансовых учреждений и других физических и юридических лиц сообщения о подозрительных операциях, анализирует их и передает результаты своего анализа в национальные правоохранительные органы и иностранные подразделения финансовой разведки с целью борьбы с отмыванием денег.[56], [57] Непосредственная специализация в вопросах противодействия отмыванию денег, а также обладание современными знаниями о типологиях и практиках легализации преступных доходов делают это ведомство особо ценным источником информации и важным партнером при расследовании преступлений, совершенных с использованием виртуальных валют. И наоборот, в условиях постоянного развития методов и практик отмывания денег и с появлением новых информационных технологий, способных облегчить преступникам осуществление легализации доходов от преступлений, подразделения финансовой разведки, со своей стороны, нуждаются в современных знаниях и опыте, имеющиеся у подразделений по вопросам киберпреступлений/ высокотехнологичных преступлений или других следственных органов, которые специализируются в борьбе с киберпреступностью. К сожалению, уровень такого взаимодействия на сегодняшний момент далек от желаемого.[58]

[56] Международный Валютный Фонд /Мировой Банк, « Подразделения финансовой разведки: обзор» (Источник: http://www.imf.org/external/pubs/ft/FIU/fiu.pdf).

[57] Рекомендация 26, «Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения – Рекомендации ФАТФ», ФАТФ-ГАФИ, Февраль 2012. (Источник: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

[58] Совет Европы/МАНИВЕЛ, «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», стр.6.

Подобным образом крайне важным в системе правоохранительных органов является взаимодействие и сотрудничество между подразделением по вопросам киберпреступлений/ высокотехнологичных преступлений и финансовыми следователями. [59] Главной проблемой такого сотрудничества может оказаться то, что часто уголовные и финансовые следователи относятся к различным ведомствам, практикующих различные подходы к выявлению и расследованию преступлений, совершенных с использованием информационных технологий. Это имеет важное значение в контексте расследований преступлений, совершенных посредством виртуальных валют, в силу того, что зачастую финансовые следователи полагаются на методы уголовного расследования, применимые к традиционным вещественным формам доказательств, в то время как подразделения по вопросам киберпреступлений/ высокотехнологичных преступлений полагаются на электронные доказательства. Такое сотрудничество также может оказаться полезным и продуктивным благодаря уникальным экспертным знаниям финансовых следователей в вопросах преступлений, связанных с финансовым мошенничеством, налогообложением и бухгалтерским учетом. Кроме того, обширные знания в области организованной преступности может быть очень важными источником информации для расследований преступлений, связанных с незаконным использованием виртуальных валют.

В контексте криминальной разведки и анализа все чаще встречаются случаи сотрудничества между подразделениями по вопросам киберпреступлений/ высокотехнологичных преступлений и центрами по реагированию на инциденты в области компьютерной безопасности (CSIRT). CSIRT – это группа специалистов, которая играет важную роль в защите ключевой национальной информационной инфраструктуры посредством различных методов, в основном направленных на предупреждение, управление и минимизацию последствий инцидентов в сфере кибернетической безопасности. [60]

CSIRT обрабатывает огромное количество данных, полученных через национальные механизмы мониторинга, а также из международных баз, данных (например, Shadowserver или Arbor Networks) об инцидентах в области кибернетической безопасности и об уязвимостях компьютерных систем. Применительно к виртуальным валютам CSIRT может быть привлечен в качестве партнера, обладающего знаниями в вопросах анализа вредоносного программного обеспечения, хакерских программ и известных слабых местах компьютерных систем, а также как источник информации о хакерском сообществе. CSIRT, преследуя экономическую выгоду, может оказаться весьма активным партнером в вопросах расследования компьютерных преступлений. Проблема, однако, в том,

---

[59] Совет Европы, «Стратегические приоритеты сотрудничества в сфере борьбы с киберпреступностью в регионе Восточного партнерства, проект Cybercrime@EaP» (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@EAP/2523_EAP_Strat_Priorities_V7 ENG.pdf).

[60] http://www.enisa.europa.eu/activities/cert.

многие правоохранительные органы не знают о существовании CSIRT в своей стране, равно как и о возможностях его использования.

Существуют и некоторые другие проблемы, касающиеся государственно-частного сотрудничества в контексте расследований преступлений, совершенных посредством виртуальных валют. Сотрудничество с провайдерами Интернет-услуг, которые являются основным источником информации о пользователях, данных трафика и других важных электронных доказательствах, часто затруднено либо из соображений правового (конфиденциальность данных пользователей, отсутствие правовых оснований для сбора и хранения данных) или практического (нежелание сотрудничать с государственными органами в связи с отсутствием соглашений/ меморандумов, затраты на специализированное оборудование для сбора и/ или хранения данных и т.д.) характера. [61] Финансовые учреждения, которые могут быть основным источником информации и доказательств о финансовых операциях и схемах по отмыванию денег, также могут не желать сотрудничать по причинам конфиденциальности данных или же по причине неполного понимания вопросов использования информационных технологий для совершения преступлений посредством виртуальных валют. [62] Организациям по защите прав потребителей, которые могут быть источником сообщений о преступлениях в сфере электронной торговли (финансовые махинации, в том числе с использованием виртуальных валют), может не хватать понимания о возможностях, открывающиеся вследствие официального сотрудничества с правоохранительными органами. [63] Эти и другие примеры потенциального взаимодействия более подробно рассматриваются в Модуле 3 пособия.

5.7 Сотрудничество на международном уровне

Продолжая тему тесных связей между преступлениями, совершенными посредством виртуальных валют, и киберпреступлениями, одной из самых характерных особенностей этих видов преступлений является их транснациональный характер, когда элементы преступления, преступники, жертвы или доказательства находятся в различных юрисдикциях. Таким образом, международное сотрудничество при расследовании отмывания денег, совершенного с использованием виртуальных валют, зачастую зависит от наличия и грамотного использования механизмов международного сотрудничества между следственными органами и другими ведомствами системы уголовного правосудия соответствующих стран.

---

61 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/lea_isp/default_EN.asp.

62 Совет Европы / МАНИВЕЛ, «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», стр.4.

63 http://www.ftc.gov/enforcement/consumer-sentinel-network.

Однако, такое сотрудничество может оказаться весьма непростой задачей по целому ряду причин, не последней из которых является отсутствие соответствующего регулирования в отношении виртуальных валют. Если на национальном уровне для уголовного преследования, связанного с использованием виртуальных валют отмывания денег, мошенничества и киберпреступлений могут применяться аналогии, то международное сотрудничество основано на международных соглашениях, которые требуют времени и усилий для разработки четких определений, которых стороны должны будут придерживаться в процессе международного взаимодействия. Иными словами, сотрудничество на международном уровне гораздо более формализовано, чем сотрудничество на национальном уровне. Поэтому практикующие юристы должны очень внимательно изучить эти обстоятельства, чтобы отсутствие понимания или признания не стало вопросом целесообразности такого сотрудничества.

Еще одним возможным проблемным аспектом международного сотрудничества является оказание взаимной правовой помощи (ВПП) или подобные ему процедуры.[64] ВПП, будь то на основе двухсторонних или многосторонних договоров, как правило, предусматривает длительные и сложные процедуры с множеством формальностей. И, возможно, именно по этой причине, ВПП потребует много времени в ходе расследований, связанных с виртуальными валютами, с их акцентом на электронных доказательствах, которые обладают высокой волатильностью и предрасположенностью к изменениям в очень короткие промежутки времени. Эти вопросы, а также другие механизмы международного сотрудничества более подробно будут рассматриваться в Модуле 3 данного пособия.

Подобные сложности, хотя и в меньшей степени, характерны также и для непосредственного (прямого) международного сотрудничества между органами полиции, а также для сотрудничества следственных органов на этапе, предшествующем ВПП, или выходящего за рамки официальных процедур. Несмотря на то, что существует ряд механизмов международного сотрудничества, созданных в рамках различных договоров в сфере борьбы с киберпреступностью (контактные центры 24/7 в соответствии с Конвенцией Совета Европы о компьютерных преступлениях,[65] национальные бюро Интерпол,[66] G8 Сеть подразделений в сфере высокотехнологичных преступлений[67]) и отмыванием денег (сотрудничество между ПФР), эффективность использования таких механизмов часто недостаточна из-за отсутствия необходимых знаний у правоохранительных или надзорных/регулирующих органов, или во многих случаях неэффективна из-за несвоевременного реагирования на запросы правоохранительных органов вследствие дискреционных подходов, практикующихся в таком сотрудничестве.

64 Комплексное исследование УНП ООН по киберпреступности, стр. 185 и далее.
65 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points of contact/aboutpoc_EN.asp.
66 http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
67 http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf

В контексте государственно-частного сотрудничества существует и другая, часто упускаемая из виду, форма международного сотрудничества – сотрудничество следственных органов с иностранными компаниями (т.е. субъектами международного частного права), которые могут иметь данные, актуальные для целей расследований, связанных с виртуальными валютами. Это, например, социальные сети, телекоммуникационные компании, имеющие филиалы на местном рынке, провайдеры электронной почты и подобные им, часто глобальные, игроки. Проблемой в этой связи может оказаться юридически обязательное условие сотрудничества с иностранными материнскими компаниями. Даже если правовые акты или нормы прямо применимы к местным компаниям, некоторые из наиболее важных данных могут обрабатываться и/ или находится у материнской компании или другого лица, находящегося в другой стране. Поэтому неудивительно, что, как свидетельствует практика, иностранные корпорации, если нет официального соглашения о сотрудничестве, менее склонны сотрудничать с зарубежными правоохранительными органами, нежели национальные компании. [68] Таким образом, установление и поддержание постоянных контактов с местными представительствами может оказаться очень важным, когда возникнет необходимость доступа к информации и доказательствам.

6 Тенденции

Феномен виртуальных валют быстро меняется. Некоторые виртуальные валюты и биржи закрываются и исчезают, а в это же время появляются все новые и новые виртуальные валюты.

Виртуальные валюты стали известны широкой публике с появлением сети Bitcoin в 2009 году. Тем не менее, bitcoin не был первой виртуальной валютой. Не станет он и последней.

В этом разделе мы рассмотрим некоторые тенденции, связанные с эволюцией виртуальных валют в последние годы.

6.1 Рост количества виртуальных валют

Как уже упоминалось в Модуле 1, одной из первых популярных виртуальных валют была появившаяся в 1996 году E-Gold. E-Gold была централизованной виртуальной валютой, как и практически все другие виртуальные валюты, появившиеся в последующие тринадцать лет. Бизнес-модели этих централизованных виртуальных валют отличались, но во всех случаях наличествовал либо центральный администратор, либо централизованный обмен виртуальных валют.

[68] «Трудности правоохранительных органов в трансграничном получении электронных доказательств от "поставщиков облачных вычислений"», дискуссионный документ, подготовленный для Совета Европы (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079_reps_IF10_reps_joeschwerha1a.pdf).

Первая криптовалюта (Bitcoin) была создана в 2009 году. Исходный код Bitcoin находится в свободном доступе, поэтому любой желающий может создать децентрализованную виртуальную валюту либо идентичную, либо основанную на модели bitcoin. В период между 2009 и 2014 появилось много других криптовалют. Представленные в таблице ниже данные демонстрируют динамику увеличения количества известных криптовалют[69]:

Год	Общее кол-во криптовалют	Названия криптовалют
2009	1	Bitcoin
2010	1	Bitcoin
2011	3	Bitcoin, Litecoin, Namecoin
2012	4	Bitcoin, Litecoin, Namecoin, Peercoin
2013	8	Bitcoin, Litecoin, Namecoin, Peercoin, Ripple, Dogecoin, Mastercoin, Primecoin
2014	12	Bitcoin, Litecoin, Namecoin, Peercoin, Ripple, Dogecoin, Mastercoin, Primecoin, Auroracoin, Vertcoin, MazaCoin, Coinye

Данные об общем количестве виртуальных валют всех типов очень скудны. Несмотря на это, заслуживают внимания следующие наблюдения:

- Принимая во внимание отмеченную в таблице выше динамику роста криптовалют, не исключено, что в ближайшие годы число децентрализованных виртуальных валют существенно увеличится.
- Бизнес-модель неконвертируемых централизованных виртуальных валют в настоящее время имеет ряд успешных прецедентов (Second Life Linden Dollars, World of Warcraft Gold, Project Entropia Dollars). Поэтому нет оснований не предположить, что и другие владельцы ролевых игр или администраторы виртуальных миров не создадут в будущем свои виртуальные валюты.
- Amazon.com недавно представила виртуальную валюту, известную как Amazon Coins. Amazon Coins могут быть использованы для приобретения различных элементов приложения, электронных книг и других предметов на сайте amazon.com. Они также могут быть переданы другим пользователям amazon.com. [70] Пока не совсем ясно, как эта бизнес-модель будет развиваться далее, но если она будет успешной для Amazon, то не будет оснований не ожидать, что другие крупные торговые сайты не внедрят аналогичный подход.

69 http://en.wikipedia.org/wiki/Cryptocurrency#Notable_cryptocurrencies
70 http://www.amazon.com/gp/feature.html?docId=1001166401

6.2 Растущая доступность виртуальных валют

Чтобы приобрести виртуальную валюту, все, что потребуется, это располагать источником финансирования, приемлемым для биржи (обменника) виртуальной валюты, которая реализует интересующую виртуальную валюту. Как уже упоминалось в Модуле 1, существуют биржи, которые принимают широкий спектр возможных источников финансирования (способов оплаты), включая другие виртуальные валюты, банковские и денежные переводы, платежные карты, наличные деньги и другие услуги Интернет-платежей, такие как PayPal. Растущее число доступных источников финансирования означает, что все большее количество людей будут иметь возможность приобрести виртуальную валюту, стоит им только этого захотеть.

Bitcoin, например, можно приобрести во многих странах. На момент подготовки данного пособия биржи виртуальных валют, доступные в сети Интернет, обеспечивали возможность приобретения bitcoin в 246 юрисдикциях мира.[71], [72].

В сущности, если удовлетворяются требования администратора или биржи виртуальных валют, направленные на борьбу с мошенничеством, то не будет и никаких географических ограничений, препятствующих приобретению любой конвертируемой виртуальной валюты.

6.3 Увеличивающаяся сложность схем отмывания денег

Как уже упоминалось в главе 3.5, отсутствие связей между счетами в виртуальных валютах и реальными людьми в сочетании с возможностью иметь любое количество счетов позволяет создавать новые сложные схемы с целью сокрытия незаконного источника происхождения средств.

Виртуальные валюты, таким образом, представляют собой дополнительные возможности для создания новых методов отмывания денег. Вполне естественно ожидать, что преступники продолжат развивать способы отмывания преступных доходов, используя для этого виртуальные валюты. Результатом этого станет появление более запутанных схем с широким использованием в преступных целях угроз и рисков, речь о которых шла в этом модуле.

6.4 Ужесточение регулирования виртуальных валют

Как уже упоминалось в главе 5.4, администраторы централизованных виртуальных валют и биржи виртуальных валют могут регулироваться как финансовые учреждения, предлагающие услуги перевода ценностей. Можно ожидать, что тенденция по ужесточению регулирования этих видов провайдеров услуг виртуальных валют в дальнейшем будет усиливаться.

---

[71] http://howtobuybitcoins.info/
[72] http://planetbtc.com/complete-list-of-bitcoin-exchanges/

В последнее время стало известно о ряде инициатив, направленных на ужесточение регулирование децентрализованных виртуальных валют. На сегодняшний день упрочилось два подхода:

- Запретить или ограничить использование децентрализованных виртуальных валют [73]
- Рассматривать и регулировать виртуальные валюты как товар [74], [75]
- Регулировать определенные виды деятельности, связанные с виртуальными валютами, как отмечалось выше.

И снова-таки. Ожидается, что тенденция по ужесточению регулирования децентрализованных виртуальных валют будет продолжаться, особенно с учетом рисков использования виртуальных валют в целях отмывания преступных доходов[76].

[73] «Китай запретил финансовым учреждением проводить операции с bitcoin», Bloomberg, Декабрь 2013. (Источник: http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html)

[74] «Налоговики США: bitcoin – это имущество, а не валюта», FinExtra, Март 2014. (Источник: http://www.finextra.com/News/FullStory.aspx?newsitemid=25895)

[75] «Техас приравняет виртуальные валюты, подобные bitcoin, к деньгам», RT.com, Апрель 2014. (Источник: http://rt.com/business/texas-bitcoin-regulation-currency-257/)

[76] http://en.wikipedia.org/wiki/Legality_of_Bitcoins_by_country

Вопросы для самооценки

Вопрос 1: Опишите угрозы, связанные с виртуальными валютами, которые делают их привлекательными для целей отмывания преступных доходов.

Вопрос 2: Расскажите, как преступники используют заочную природу виртуальных валют для отмывания преступных доходов.

Вопрос 3: Объясните, почему регуляторные и надзорные угрозы, связанные с администраторами централизованных виртуальных валют, представляют собой риски отмывания денег.

Вопрос 4: Перечислите следственные трудности, которые скрывают в себе виртуальные валюты, и предложите возможные пути их решения.

Вопрос 5: Перечислите некоторые из особенностей электронных доказательств, которые отличают их от физических (традиционных) доказательств.

Вопрос 6: Каковы юридические основания допустимости электронных доказательств в уголовных делах в вашей стране?

Вопрос 7: Дайте объяснение понятию дискреционного уголовного преследования и его применимости в расследованиях, связанных с виртуальными валютами.

Вопрос 8: Расскажите о преимуществах, которые правоохранительные органы могут извлечь из сотрудничества с подразделением финансовой разведки.

Вопрос 9: Перечислите возможные механизмы прямого международного сотрудничества следственных органов (полиции), которые могут быть использованы в расследования, связанных с виртуальными валютами.

Вопрос 10: Какие тенденции вероятнее всего окажут влияние на использование виртуальных валют для целей отмывания доходов от преступлений?

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Модуль 3
Выявление и расследование отмывания преступных доходов, совершенного с помощью виртуальных валют

1 Краткое изложение

Данный модуль посвящен рассмотрению существующих инструментов и методов выявления и расследования отмывания преступных доходов, совершенного с помощью виртуальных валют. Существующие инструменты и методы собраны в две большие группы – законодательный и следственный инструментарий. Каждая из этих групп будет подробно рассмотрена в данном модуле.

Изучение модуля завершится рассмотрением возможных контрмер, которые призваны помочь следователям более эффективно выявлять и противодействовать отмыванию денег посредством виртуальных валют.

2 Цели обучения

По окончанию данного модуля Вы будете:

- Знать об имеющихся законодательных инструментах, применимых для расследования преступлений по отмыванию преступных доходов посредством виртуальных валют.

- Знать о доступном следственном инструментарии, который может быть использован для расследования преступлений по отмыванию преступных доходов, совершенного с использованием виртуальных валют.

- Понимать следственные методики, используемые для расследования преступлений по отмыванию преступных доходов посредством виртуальных валют.

- Знать об возможных контрмерах, направленных на предотвращение отмывания преступных доходов с помощью виртуальных валют.

3 Законодательный инструментарий

3.1 Материальное право

Одной из главных задач любого уголовного расследования является обеспечение надлежащей квалификации предполагаемой преступной деятельности соответственно нормам материального уголовного права, то есть, определение состава преступления. И хотя большая часть текущей практики в этом отношении определена многолетним прецедентарным правом, некоторые новые формы преступной деятельности – незаконное использование виртуальных валют является одним из таких примеров – могут потребовать переосмысления и адаптации норм материального уголовного права к современным реалиям жизни, которые предстоит комплексно решать либо законом, либо практикой. Таким образом, цель данного раздела заключается в рассмотрении различных вариантов использования существующих норм материального уголовного права для определения состава преступления по отмыванию денег в контексте виртуальных валют.

Перед тем, как приступить к решению поставленной задачи, следует еще раз обратить внимание на то, что в настоящее время статус виртуальных валют остается неоднозначным. А принимая во внимание, что использование виртуальных валют не криминализировано ни в одном из государств ГУАМ (как и в любой другой стране, если на то пошло), использование таких валют *per se* не может рассматриваться как преступление в силу принципа технологической нейтральности.

3.1.1 Отмывание денег: элементы преступления

Отмывание денег предполагает наличие схемы финансовых операций, целью которой является сокрытие принадлежности, источника и назначения незаконно полученных средств. Причины, по которым преступники – будь то наркоторговцы, казнокрады или коррумпированные государственные чиновники – пользуются такими схемами, лежат в намерении скрыть или замаскировать незаконное происхождение имущества или посодействовать лицу, участвующему в совершении предикатного преступления, избежать правовых последствий его/ ее незаконной деятельности, путем сокрытия или маскировки подлинного характера, источника, местонахождения, способа распоряжения, перемещения, владения или прав на имущество, полученного преступным путем. [1] Другими словами, преступники стараются «отмыть» полученные преступным путем активы, чтобы, с одной стороны, скрыть доказательства своих преступлений, а с другой

[1] Статья 6 Конвенции Организации Объединенных Наций против транснациональной организованной преступности.

стороны – уберечь незаконно полученное имущество от ареста и конфискации. Преступники все чаще эксплуатируют результаты глобализации мировой экономики для осуществления трансграничных переводов. Не в последнюю очередь они пользуются достижениями в области информационно-коммуникационных технологий, которые позволяют перемещать деньги в любую точку мира с высокой скоростью и относительной легкостью. Независимо от того, кто осуществляет отмывание денег, этот процесс состоит их трех основных этапов:

Этап **размещения** представляет собой первоначальную интеграцию денежных средств в финансовую систему. В случае крупных сумм это может оказаться весьма трудной задачей, особенно если речь идет о наличных деньгах.

После размещения следует этап **расслоения**, который, как правило, состоит из серии операций, направленных на сокрытие истинного происхождения средств. Это самый сложный этап процесса отмывания и наиболее международный по своей природе. Преступники, занимающиеся отмыванием денег, могут начать с электронных переводов денег из одной страны в другую, затем дробить их на более мелкие суммы и инвестировать в удобные финансовые инструменты или совершить приобретения на зарубежных рынках, постоянно перемещая деньги, чтобы избежать обнаружения. При этом преступники умело пользуются лазейками или различиями в национальных законодательствах, равно как и проволочками судебном или полицейском сотрудничестве.

Заключительный этап процесса отмывания денег называется **интеграцией**, потому что в этот момент незаконно полученные средства окончательно интегрируются в легальную экономику. Пройдя первоначально этап размещения наличных денег в финансовой системе, за которым следовало расслоение незаконно полученных средств посредством множественных финансовых транзакций, «грязные» деньги окончательно ассимилируются в финансовой системе с легальными деньгами и могут быть использованы для любых целей. [2]

В настоящее время в современных условиях отмывание денег с использованием виртуальных валют становится все более частым явлением в реальной жизни и все более актуальным вопросом на повестке дня компетентных органов. В то время как существуют значительные различия с точки зрения использования централизованных и децентрализованных виртуальных валют, о чем, пожалуй, наиболее красноречиво свидетельствуют примеры Silk Road и Liberty Reserve,

[2] Азиатский Банк Развития, "Руководство по борьбе с отмыванием денег и финансированием терроризма", стр. 10-11 (Источник: https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf).

анонимность, сложность выявления или ставка на криптографию, характерные для децентрализованных виртуальных валют, могут предложить привлекательные варианты для сокрытия доходов преступлений.

Пример: Liberty Reserve

В деле о самом большом на сегодняшний день случае отмывания денег в онлайновой среде в мае 2013 года Департамент юстиции США предъявил обвинения Liberty Reserve, провайдеру денежных переводов из Коста-Рика, и семи ее руководителям и сотрудникам, вменив им ведение незарегистрированной деятельности по переводу денег, а также отмывание незаконных доходов на сумму более $ 6 млрд. При поддержке Департамента казначейства, определившего Liberty Reserve как финансовое учреждение, которое в соответствии с главой 311 Патриотического акта США представляет собой наибольшие риски отмывания денег, Liberty Reserve была эффективно отрезана от финансовой системы США.

Основанная в 2006 году, Liberty Reserve изначально задумывалась для того, чтобы избежать внимания и проверок регулирующих и правоохранительных органов и способствовать преступникам в распространении, хранении и отмывании доходов, полученных от мошенничества с кредитными картами, краж личных данных, инвестиционного мошенничества, хакерских атак, незаконного оборота наркотиков и детской порнографии, предоставляя им возможность проводить анонимные и сложно отслеживаемые финансовые операции. Масштабы деятельности Liberty Reserve впечатляют: более миллиона клиентов по всему миру, в том числе более 200 000 в Соединенных Штатах, и около 55 млн. операций, почти все из которых были незаконными. Liberty Reserve имел свою собственную виртуальную валюту – Liberty Dollars (LR), но, в конечном счете, переводы имели привязку либо к фиатной валюте, либо золоту.

Чтобы воспользоваться виртуальной валютой LR, пользователю было необходимо открыть счет на сайте Liberty Reserve. Требуя для видимости лишь базовые идентификационные данные, Liberty Reserve не проверял их достоверность. Пользователи создавали счета на вымышленные имена, в том числе на имена, явно относящиеся к криминальной среде («Хакерский счет», «Мошенник Джо»), и указывали явно вымышленные адреса («123 Поддельная Главная Улица», «Чистой Выдумки Город Нью-Йорк»). Также Liberty Reserve требовала от своих пользователей производить операции по депонированию и снятию денег через определенные обменники, которые, как правило, либо были

нелицензированы, либо находились в юрисдикциях со слабыми режимами регулирования и контроля в сфере противодействия отмыванию денег. Не проводя непосредственно операций по депонированию и снятию денег своих клиентов, Liberty Reserve удалось, таким образом, уйти от необходимости собирать информацию о пользователях, обычно необходимую при осуществлении банковских операций или другой финансовой деятельности. После создания счета пользователь мог совершать операции с другими пользователями Liberty Reserve путем перевода LR со своего счета на счета других пользователей, в том числе подставной «коммерческой» компании, которая принимала LR в качестве оплаты. За дополнительную «оплату конфиденциальности» (75 центов США за каждую транзакцию) пользователи могли скрыть номера своих счетов в Liberty Reserve, делая, таким образом, переводы полностью неотслеживаемыми. Узнав, что правоохранительные органы США заинтересовались его деятельностью, Liberty Reserve для видимости прекратил свою деятельность в Коста-Рике, но продолжил работу через ряд подставных компаний, переводя миллионы через счета в Австралии, на Кипре, Китае, Гонконге, Марокко, России, Испании и в других юрисдикциях. [3]

3.1.2 Вспомогательные или предикатные киберпреступления

Как отмечалось в главе 7.2 Модуля 1 данного пособия, аспекты киберпреступности в контексте незаконного использования виртуальных валют могут проявляться множественными способами. Киберпреступления как автономная категория преступлений, которые, так или иначе, связаны с виртуальными валютами, на первый взгляд могут и не представлять особого значения для расследований отмывания преступных доходов. В то же время даже автономные киберпреступления против систем виртуальных валют часто могут стать важными источником оперативных данных, которые могут помочь в выявлении схем отмывания денег.

Предикатное преступление – это преступление, доходы от которого могут стать предметом «отмывания». [4] Отмывание денег, совершенное с использованием виртуальных валют, может быть связано с преступными доходами, полученными вследствие совершения киберпреступлений, таких как преступления в отношении компьютерных учетных данных или

[3] «Прокурор Манхэттена выдвигает обвинения против Liberty Reserve, одной из крупнейшей мировой компании цифровых валют, а также семи его руководителей и сотрудников за организацию схемы по отмыванию $ 6 млрд.», Департамент юстиции США, Май 2013 (Источник: http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php?print=1)

[4] Инструментарий УНП ООН по борьбе с торговлей людьми, стр. 119 (Источник: http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf)

подлог / мошенничество с использованием компьютерных технологий. Статус предикатного к отмыванию денег преступления будет варьироваться в зависимости от юрисдикции. Если разрешено законодательством, киберпреступления будут считаться предикатными к отмыванию денег. В таком случае чтобы установить состав преступления об отмывании денег, расследования будут опираться на элементы киберпреступлений. С другой стороны, киберпреступления чаще всего будут являться вспомогательными по отношению к отмыванию денег, совершенного посредством виртуальных валют. Поэтому расследование таких преступлений может иметь прямую взаимосвязь с основным обвинением в отмывании денег, и, таким образом, предоставлять для правоохранительных органов важные доказательства совершения отмывания денег с помощью виртуальных валют.

Как уже говорилось в главе 7.2 Модуля 1, «основное» киберпреступление против компьютерных систем или данных также может быть вспомогательным к целому ряду преступлений, связанных с виртуальными валютами, например, когда кошелек «взламывается» с целью кражи bitcoin или, когда счета третьих лиц используются для проведения операций без их на то ведома и согласия. Таким образом, важно понимать природу отдельных киберпреступлений, в том числе связанных с неправомерным доступом, вмешательством в системы, вмешательством в данные и незаконным использованием устройств. Практика показывает, что многие из потенциальных случаев киберпреступлений не расследуются должным образом в связи с отсутствием должного понимания того, что представляет собой киберпреступление. С этой целью приведем Вашему вниманию некоторые определения, важные с точки зрения их применения и использования для целей расследования преступлений, связанных с виртуальными валютами: [5]

Преступление по **неправомерному доступу** является базовым преступлением, представляющим собой угрозы и атаки в отношении безопасности (то есть, в отношении конфиденциальности, целостности и доступности) компьютерных систем и данных. Иными словами, неправомерный доступ обозначает «хакерское» деяние, которое не обязательно предполагает непосредственные негативные последствия для систем или данных (вмешательство, потеря и т.д.), но само по себе является опасным поведением, которое ставит под угрозу безопасность и конфиденциальность систем/ данных (например, предоставление публичного доступа к конфиденциальным данным, в том числе к паролям, данным о системе) и может служить основой для более опасных атак/

[5] Обращаем внимание на то, что описания киберпреступлений, особенно в части необходимых элементов, базируется по большей части на текстах национальных правовых документов, ссылки на которые даны в соответствующих сносках. Сопровождающее их описание и пояснения приведены только для целей данного пособия и не являются официальными обязывающими определениями.

преступлений.[6] Элементы преступления по неправомерному доступу[7], в равной степени имеющие отношение, как к централизованным, так и к децентрализованным виртуальным валютам, включают: а) акт «доступа», означающий проникновение в компьютерную систему или ее часть (в оборудование, компоненты, сохраненные данные установленной системы, каталоги, данные трафика и контента), независимо от типа соединения и способа связи. Целями могут служить базы данных эккаунтов в компьютерных играх, кошельки/ ячейки с bitcoin, серверная инфраструктура обменников валют и т.п.; б) доступ к компьютерной системе должен быть осуществлен незаконно, то есть без разрешения (по закону, в рамках исполнительного, административного, судебного производства, договоренности или по обоюдному согласию) или являться поведением, которое, так или иначе, не имеет легальных оснований, объяснений, оправданий в соответствии с национальным законодательством; в) умысел неправомерного доступа к компьютерной системе должен всегда наличествовать и быть доказан; г) нет необходимости в причинении конкретных убытков, последствий или прочего негативного влияния – сам по себе факт совершения такого деяния, даже без конкретных последствий, является уголовным преступлением (эта особенность может быть важной для квалификации попытки отмывания денег);

Криминализация **вмешательства в данные** как киберпреступления направлена на защиту целостности и конфиденциальности компьютерных данных от поведения, подвергающего опасности их целостность и/ или доступность.[8] Это преступление может интерпретироваться как-то, которое направленно против надлежащего функционирования или использования компьютерных данных или компьютерных программ вследствие незаконного повреждения, удаления, порчи, изменения или подавления компьютерных данных.[9] Это преступление состоит из следующих элементов:[10] а) акт манипуляции данными (повреждение, удаление, порча, изменение или подавление компьютерных данных). Например, использование вирусных, троянских или любых других вредоносных программ, которые могут представлять угрозу как для виртуальной валюты, так личных данных пользователей системы, включая кражу личных данных; б) вмешательство в данные должно быть осуществлено неправомерно, что, подобно преступлению по неправомерному доступу, означает любое несанкционированное

[6] Комплексное исследование УНП ООН по киберпреступности, стр. 82.
[7] Статья 271 Уголовного кодекса Азербайджанской Республики; статья 284 Уголовного кодекса Грузии; статья 259 Уголовного кодекса Республики Молдова.
[8] Комплексное исследование УНП ООН по киберпреступности, стр. 88.
[9] См., например, Пояснительную записку к Конвенции Совета Европы о компьютерных преступлениях, п.61.
[10] Статья 286 Уголовного кодекса Грузии; статья 260^2 Уголовного кодекса Республики Молдова; статьи 361 и 362 Уголовного кодекса Украины.

(соглашением или законом) действие. В контексте виртуальных валют должны быть запрещены «определенные деяния, связанные с анонимной коммуникацией, например, когда информация заголовка пакета изменяется для того, чтобы скрыть личность преступника, совершающего преступление» [11]. Это означает, что использование дополнительных онлайновых инструментов для повышения уровня анонимности пользователей систем децентрализованных виртуальных валют может рассматриваться как элемент преступления; в) умысел вмешательства в компьютерные данные должен быть доказан;

Преступление по **вмешательству в системы** имеет много общего с преступлением по вмешательству в данные с точки зрения большинства своих целей и применимых элементов, за исключением разницы в объекте и/ или последствиях преступления. Иными словами, оно означает препятствование функционированию компьютерной системы. [12] Это преступление должны образовывать следующие элементы [13]: а) акт препятствования путем ввода, передачи, повреждения, удаления, изменения или блокирования компьютерных данных, то есть действие, которое вызывает кратко- или долгосрочный выход из строя системы обработки данных виртуальных валют, или выход из строя серверной инфраструктуры компьютерных игр, в которых используются централизованные виртуальные валюты; б) такое препятствование должно быть «серьезным», то есть, иметь существенное негативное влияние на способность владельца или оператора использовать систему или осуществлять взаимодействие с другими системами (например, с помощью программ, генерирующих атаки по «отказу в обслуживании», других враждебных программных кодов, таких как вирусы, которые препятствуют или существенно замедляют работу системы); в) препятствование должно быть осуществлено неправомерно; г) умысел серьезно воспрепятствовать функционированию компьютерной системы должен быть доказан.

Преступление по **незаконному использованию устройств** признает потенциал программного обеспечения и аппаратных средств, которые могут быть использованы для совершения преступлений против конфиденциальности, целостности и доступности компьютерных систем или данных. Понимается, что многие из таких инструментов могут представлять собой устройства или технологии двойного назначения (т.е. могут быть использованы как в законных, так и незаконных целях). Таким образом, чтобы избежать чрезмерной криминализации, основное

---

[11] См., например, Пояснительную записку к Конвенции Совета Европы о компьютерных преступлениях, п.64 (Источник: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm).

[12] Комплексное исследование УНП ООН по киберпреступности, стр. 88-89.

[13] п.2 статьи 286 Уголовного кодекса Грузии; статья 260^3 Уголовного кодекса Республики Молдова; статьи 361 и 363^1 Уголовного кодекса Украины.

внимание сосредоточено на устройствах, которые могут быть в основном использованы или адаптированы для таких целей. [14] Состав такого преступления определяют следующие элементы [15]: а) акты владения, производства, продажи, покупки с целью использования, импорт, распространение или иные деяния, делающие доступными устройства, включая компьютерные программы, которые предназначены или приспособлены главным образом для совершения преступлений против компьютерных систем и данных. К последним относятся хакерские утилиты, вирусы или другие вредоносные программы, которые могут быть использованы для целевых атак на компьютерные системы и данные систем виртуальных валют и их пользователей, а также «взломанные» системы и счета клиентов, используемые для отмывания доходов от преступлений; б) акты производства, продажи, покупки с целью использования, импорт, распространение или иные деяния, делающие доступными компьютерные пароли, коды доступа или подобные данные, с помощью которых можно получить доступ ко всей или части компьютерной системы (к примеру, к защищенным данным о логинах и паролях пользователей виртуальных валют); в) такие деяния должны быть совершены неправомерно; г) умысел любого из перечисленных выше деяний должен быть доказан.

Преступление по **компьютерному мошенничеству** является ассимилирующим преступлением, совмещающим элементы традиционного мошенничества с информационно-коммуникационными технологиями. По этой причине компьютерное мошенничество часто не криминализируется как отдельное преступление, а скорее представляет собой юридическую конструкцию, интегрирующей элементы информационных и коммуникационных технологий в основное обвинение в мошенничестве. В контексте виртуальных валют такие элементы могут сводиться к манипуляциям с компьютерными данными, таким как ввод, изменение, удаление, подавление или, если рассматривать более широко, вмешательство в функционирование компьютерной программы или системы. Однако, в отличие от других киберпреступлений, для доказывания умысла в этом случае необходимо наличие комбинации двух элементов: во-первых, наличие общего умысла по вводу, изменению, удалению, подавлению или вмешательству в функционирование компьютерной программы или системы и, во-вторых, доказательства конкретного мошеннического или другого незаконного умысла получить экономическую или иную выгоду для себя или другого.

---

[14] Комплексное исследование УНП ООН по киберпреступности, стр. 92-93 (Ссылка на "неправомерное использование компьютерных инструментов").

[15] Статья 271^6 Уголовного кодекса Азербайджанской Республики; статья 285 Уголовного кодекса Грузии; статья 260^4 Уголовного кодекса Республики Молдова; статья 361^1 Уголовного кодекса Украины.

Пример: Mt. Gox

Mt. Gox была самой популярной Bitcoin-биржей из Токио, Япония, которая начала свою деятельность в июле 2010 г. и уже к 2013 г. через нее проводилось 70% всех сделок с bitcoin. Биржа объявила о своем банкротстве в феврале 2014 г. после заявления о потери почти 850 000 bitcoin, принадлежащих ее клиентам.

По утверждению представителей Mt. Gox, все ее беды связаны с так называемой «гибкостью транзакций» с bitcoin. Когда осуществляется bitcoin-транзакция, в системе генерируется важная информация, включающая сумму отправляемых bitcoin, номера счетов отправителя и получателя. Идентификационный номер транзакции, ее уникальное «имя», формируется на основании этой информации. Но некоторые данные, которые используются для генерирования идентификационного номера транзакции, происходят из неподписанных, незащищенных частей транзакции. В результате существует возможность изменить идентификационный номер транзакции без необходимости авторизации отправителем.

В этом случае ничто важное не теряется, потому что вся ключевая информация об операции по-прежнему надежно защищена. Но проблемы могут возникнуть, если отправитель ожидает увидеть сделку под конкретным идентификационным номером. Как утверждают в Mt.Gox, ожидалось, что транзакции в публичном реестре будут показаны под определенными идентификационными номерами. Когда такое не случалось – вор вносил изменения в идентификационные номера – вор предъявлял жалобу, что операция не состоялась, и система автоматически повторяла попытку провести операцию, что приводило к повторной отправке bitcoin.

Гибкость транзакций является недостатком сети Bitcoin и нет никакой вины Mt.Gox в том, что транзакции могут быть переименованы таким образом. Но этот недостаток был известен с 2011 года и его можно было бы компенсировать с помощью программного обеспечения, которое показывает точный баланс и количество операций.[16]

В современной практике вмешательство в данные и системы представляется наименее значимыми преступлениями в контексте виртуальных валют. В то же время случай с Mt. Gox демонстрирует, что

[16] The Guardian, «Как ошибка в Bitcoin привела к краху Mt.Gox» (Источник: http://www.theguardian.com/technology/2014/feb/27/how-does-a-bug-in-bitcoin-lead-to-mtgoxs-collapse)

последствия таких преступлений могут иметь непосредственное влияние на рынок виртуальных валют.

3.1.3 Использование виртуальных валют: объективные и субъективные стороны

В более традиционной теории уголовного права, принятой в странах ГУАМ, элементы преступления можно категоризировать на объективную (само по себе деяние, а также объекты и орудия преступления) и субъективную (умысел, цель, соучастие и т.д.) стороны. Рассмотрим эти категории на примере отмывания денег с использованием виртуальных валют. Объективные элементы состава преступления, которые включают акты использования виртуальной валюты, технически говоря, не будут отличаться от объективных элементов любого другого преступления, в том числе «традиционного» отмывания денег. Привлечение экспертов и использование их экспертных заключений может понадобиться для описания технических вопросов, имеющих отношение к централизованным и децентрализованным виртуальным валютам, а также, чтобы провести аналогии с традиционными финансовыми операциями.

В сущности, использование виртуальной валюты как объективный элемент уголовного преступления по отмыванию денег может усматриваться таким образом:

- На этапе **размещения** (когда полученные преступным путем средства вводятся в финансовый оборот) факт покупки виртуальной валюты через обменники (в случае децентрализованных валют) или администратора (в случае централизованных валют) может быть представлен как элемент преступления;

- На этапе **расслоения** (процесс, посредством которого полученные преступным путем средства легализируются, а их принадлежность и источник происхождения маскируются), присущие черты виртуальных валют (наиболее важные из которых – анонимность и сложность отслеживания операций) могут быть представлены как элемент преступления по отмыванию денег. При этом обвинение будет пытаться доказать, что выбор на виртуальную валюту пал именно в силу ее свойств, чтобы, таким образом, скрыть преступное происхождение средств. На самом деле, в контексте использования виртуальных валют концентрация внимания именно на «расслоении» представляется наиболее разумной для целей доказывания умысла (см. ниже);

- На этапе **интеграции** (процесс, посредством которого легализованное на этапе расслоения имущество реинтегрируется в экономику) использование виртуальной валюты может являться одним из элементов преступления в зависимости от ситуации. В сущности, если «отмытые» доходы реинвестируются на рынке виртуальных валют, это может быть дополнительным элементом преступления.

Что касается доказательств наличия **умысла**, являющимся одним из основных элементов преступления по отмыванию денег, ситуация обстоит несколько иначе. Аргументы стороны обвинения могут быть более весомыми, если сконцентрироваться, опять же, на наиболее характерных особенностях виртуальных валют:

- **анонимность** и отсутствие взаимодействия лицом к лицу может быть допустимым доказательством умысла преступления о незаконном использовании виртуальных валют на фоне наличия традиционных, более прозрачных и проверенных финансовых механизмов;
- **трудности отслеживания**, включая отсутствие «бумажного/ документального» следа, с тем же логическим заключением о намерении избежать использования традиционных финансовых механизмов, также может свидетельствовать о наличии умысла;
- в случае децентрализованных виртуальных валют – ставка на **криптографию**, которая может сделать проведение криминалистической экспертизы крайне сложным;
- едва ли не главный вопрос, касающийся виртуальных валют с точки зрения доказательств умысла, таится в самой сущности виртуальных валют, а именно: обращение виртуальных валют вне установленных финансовых учреждений при полном **отсутствии регулирования**, что может быть представлено как осознанный выбор.

3.2 Процессуальное право

Процессуальные аспекты расследований по отмыванию денег, совершенного с использованием виртуальных валют, направлены на обеспечение правовой основы для конкретных действий, которые надзорные или правоохранительные органы могут предпринять с целью выявления, расследования и уголовного преследования таких преступлений. Продолжая логику, согласно которой киберпреступления являются предикатными или вспомогательными преступлениями по отношению к отмыванию денег, совершенного посредством виртуальных валют, основное внимание в этой главе будет уделено процессуальным правилам и инструментам, используемых для сбора и обеспечения

сохранности электронных доказательств. Но даже в случае, когда киберпреступления не являются предикатными или вспомогательными к отмыванию денег, понимание перечисленных ниже процедур важно хотя бы с той точки зрения, что они специально задумывались и создавались для обработки и сохранения электронных доказательств.

Процессуальные полномочия с точки зрения их предназначения подразделяются на:

- Процедуры, направленные на сбор оперативных данных, т.е. выявление преступных деяний и/ или доходов от преступлений; и
- Процедуры, направленные на обеспечение и внедрение доказательств в уголовное судопроизводство.

3.2.1 Оперативные данные

Сбор оперативных данных об использовании виртуальных валют для отмывания преступных доходов возможен вследствие мероприятий по обеспечению кибернетической безопасности, а также в рамках расследований киберпреступлений. Все это более детально рассматривается далее.

3.2.1.1 Сообщения CSIRT об инцидентах в области компьютерной безопасности

CSIRT (центры по реагированию на инциденты в области компьютерной безопасности) являются давними партнерами правоохранительных органов при расследовании киберпреступлений, предоставляя им данные и информацию о различных инцидентах против компьютерных систем и данных. Некоторые из них могут стать предметом расследований, которые проводятся подразделениями по вопросам киберпреступлений / высокотехнологичных преступлений. Но в реальности большинством таких инцидентов (количество сообщений может исчисляться сотнями за один день) будут заниматься CSIRT в соответствии со специальными процедурами, в результате которых не обязательно будут получены доказательства, допустимые в уголовном судопроизводстве.

Поэтому, принимая во внимание тесные связи между киберпреступлениями, виртуальными валютами и отмыванием денег в сети Интернет, можно использовать следующие источники информации, находящиеся в распоряжении национального CSIRT:

- Сообщения об инцидентах в сфере компьютерной безопасности, которые непосредственно связаны с финансовым сектором. Сообщения об инцидентах могут быть получены как из местных,

секторальных или национальных сенсорных сетей (аппаратное или программное обеспечение, специально предназначенное для мониторинга национального Интернет-сегмента на предмет подозрительных отклонений в трафике), так и из международных баз данных CSIRT, таких как ShadowServer[17] или Arbor Networks[18]. Для истребования данных об инцидентах могут понадобится специальные, часто письменные, соглашения с CSIRT о предоставлении данных (которые могут также содержать конфиденциальную информацию). При этом в запросе должно быть четко указано, с какой целью запрашивается такая информация;

- Информация об использовании вредоносных программ, которые непосредственно нацелены на кражу личных данных или нарушение неприкосновенности частной финансовой информации, в том числе о случаях, когда следы трафика таких вредоносных программ содержат данные программного обеспечения, используемого для управления централизованными или децентрализованными виртуальными валютами;
- Общие сведения о хакерском сообществе и угрозах национальному киберпространству, которые зачастую могут стать наиболее ценным источником оперативных данных в контексте расследований о виртуальных валютах. CSIRT по характеру своей деятельности тесно связаны с хакерским сообществом и часто может предоставить ценнейшую информацию о киберпреступниках, а также различных форумах и платформах по обмену имеющей к ним отношение информацией.

В связи с тем, что находящиеся в распоряжении CSIRT данные часто носят частный и/ или конфиденциальный характер, сведения об инцидентах в сфере компьютерной безопасности должны запрашиваться в каждом конкретном случае и в рамках текущего расследования по отмыванию денег. Не смотря на то, что существует возможность предусмотреть механизм регулярного представления таких данных в рамках межведомственного сотрудничества, учитывая большой объем и чрезвычайно технической характер обрабатываемой информации, регулярная отчетность вряд ли будет иметь большое практическое значение или ценность для расследования отмывания денег.

3.2.1.2 Сбор информации о трафике в реальном времени

Сбор информации о трафике в реальном времени [19] – это процедура сбора генерируемых компьютерами данных о потоках информации, которые позволяют адресовать информацию от источника ее происхождения к

[17] http://www.shadowserver.org/wiki/
[18] http://www.arbornetworks.com/
[19] Статья 137 Уголовно-процессуального кодекса Грузии; статья 263 Уголовно-процессуального кодекса Украины.

месту назначения («данные трафика»). Данные трафика, которые можно собрать при помощи соответствующих процедур, включают: источник информации, точку назначения, маршрут, время (GMT), дату, размер, продолжительность и тип сервиса.[20]

С технической точки зрения сбор данных трафика возможен посредством специализированного оборудования, которым располагают правоохранительные органы (подразделения по вопросам киберпреступлений/ высокотехнологичных преступлений) и/ или Интернет-провайдеры.[21] Сбор информации о трафике в реальном времени, как правило, осуществляется с санкции суда. Поэтому должны быть соблюдены надлежащие процедуры: в зависимости от юрисдикции, либо следователь, либо прокурор обращается с ходатайством к судье, полномочному рассматривать и санкционировать следственные мероприятия. В ходатайстве обязательно должны быть указаны средства, с помощью которых будет проводиться сбор таких данных, и подразделение, которое будет этим заниматься.

Национальные подразделения по вопросам киберпреступлений/ высокотехнологичных преступлений, как правило, имеют опыт в сборе данных трафика в режиме реального времени. Но на практике в связи с необходимостью соблюдать разумный баланс между интересами следствия и вторжением в частную жизнь Интернет-пользователей эти процедуры используются ними только в самых серьезных случаях. Но даже в случае наличия государственных (например, центр цифровой криминалистической экспертизы) или частных (Интернет-провайдеры) партнеров, которые могут и будут готовы осуществить сбор данных трафика в режиме реального времени, ведомствам, занимающимся финансовыми расследованиям, или ПФР (в зависимости от сложившийся практики) все равно будет необходимо обратиться в национальное подразделение по вопросам киберпреступлений/ высокотехнологичных преступлений, запросив у них инструкции в отношении необходимых процедур/ ходатайств.

3.2.1.3 Перехват данных контента

В отличие от сбора данных трафика в реальном времени перехват данных контента (то есть, любые другие данные коммуникации, отличные от данных трафика) представляет собой применение традиционных методов сбора данных контента с телекоммуникационных устройств (например, телефонные разговоры) к среде информационных технологий. С точки зрения оперативных данных этот метод является эффективным

[20] См., например, Пояснительную записку к Конвенции Совета Европы о компьютерных преступлениях, п.30 (Источник: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm)

[21] Комплексное исследование УНП ООН по киберпреступности, стр.131.

следственным инструментом, позволяющим установить, носит ли коммуникация незаконный характер (например, содержит в себе криминальные угрозы, элементы харассмента, преступного сговора или мошенничества). С точки зрения расследования киберпреступлений такой перехват означает получение, просмотр, сбор или копирование всего содержания или его части любой коммуникации, в том числе данных контента, компьютерных данных, данных трафика и/ или их электронных эмиссий, передаваемых при помощи проводных, радио-, электронных, оптических, магнитных, устных или других форм и средств коммуникации.[22]

Что касается стран ГУАМ, процедуры перехвата данных устанавливаются либо законами об оперативно-розыскной деятельности (перехват данных из любых информационных и коммуникационных сетей как продолжение традиционных процедур перехвата/ прослушивания) [23] или же инкорпорированы в основное уголовно-процессуальное законодательство[24]. Независимо от источника права, перехват данных контента может проводиться различными ведомствами и прежде всего либо национальным подразделением по вопросам киберпреступлений/ высокотехнологичных преступлений, либо оперативными подразделениями полиции. Перехват данных контента в силу принципов неприкосновенности частной жизни может проводиться исключительно с санкции суда. Поэтому суду надлежащим образом должны быть представлены все необходимые ходатайства, в которых обязательно указываются цели, методы и средства перехвата данных контента, а также называются подразделения, которые будут его осуществлять.

3.2.2 Обеспечение доказательств совершения преступления

Целью этой подглавы является ознакомление со специальными процессуальными полномочиями по сбору электронных доказательств, которые используются национальным подразделением по вопросам киберпреступлений/ высокотехнологичных преступлений.

---

[22] International Telecommunication Union, «Инструментарий МСЭ по законодательству в сфере борьбы с киберпреступностью», стр. 12 (Источник: http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf)

[23] Раздел 10 Закона Азербайджанской Республики «Об оперативно-розыскной деятельности»; статья 18 Закона Республики Молдова «О специальной розыскной деятельности».

[24] Статья 138 Уголовно-процессуального кодекса Грузии; статьи 258 и 264 Уголовно-процессуального кодекса Украины.

3.2.2.1 Оперативное обеспечение сохранности компьютерных данных

Правоохранительные органы могут затребовать или подобным образом получить оперативное обеспечение компьютерных данных, необходимых в связи с конкретным уголовным расследованием или судебным разбирательством. В основном это делается с целью предотвращения уничтожения компьютерных данных, имеющих важное значение для расследования киберпреступлений.[25] Обеспечение сохранности данных подразумевает сохранение их целостности и обеспечение защиты от всего, что может вызвать ухудшение или изменение их качества или доступности.[26]

Обеспечение сохранности компьютерных данных[27] применяется, в частности, когда имеются основания полагать, что компьютерные данные подвержены риску уничтожения или изменения (например, когда в соответствии с внутренней политикой учреждения данные подлежат удалению по истечению определенного периода времени, или когда данные, находящиеся на носителе, удаляются вследствие записи других данных, или в случае регулярного удаления данных трафика, которые доступны только ограниченный период времени).

Ордер на обеспечение сохранности компьютерных данных является очень эффективным инструментом, так как позволяет добиться сохранения целостности таких компьютерных данных на необходимый период времени, не превышающий 90 дней, в течение которого компетентные органы могут затребовать их раскрытие. С этой токи зрения ордер может использоваться как дополнительная гарантия обеспечения аутентичности данных, которые планируется представить в качестве доказательств в уголовном судопроизводстве. Физические или юридические лица, во владении или распоряжении которых находятся такие данные, обязаны не разглашать никому информацию о применении процедур обеспечения сохранности данных.[28]

Что касается ведомств, осуществляющих процедуру обеспечения сохранности данных, то в отличие от более специфических мероприятий по сбору оперативной информации, ордер на обеспечение сохранности компьютерных данных может использоваться любым следственным органом, так как для этого не требуется специальных знаний по обработке

---

[25] Комплексное исследование УНП ООН по киберпреступности, стр. 127.
[26] Инструментарий МСЭ по законодательству в сфере борьбы с киберпреступностью, стр. 35.
[27] Статья 7 Закона Республики Молдова «О борьбе с киберпреступностью».
[28] См., например, Пояснительную записку к Конвенции Совета Европы о компьютерных преступлениях, п. 162 (Источник: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm)

электронных доказательств, а лишь понимание того, сохранность каких именно данных должна быть обеспечена. Консультации с национальным подразделением по вопросам киберпреступлений/ высокотехнологичных преступлений об особенностях таких ордеров и порядке их исполнения является желательным, но не обязательным.

3.2.2.2 Оперативное обеспечение сохранности и частичное раскрытие данных трафика

Обеспечение сохранности данных трафика осуществляется посредством описанной выше процедуры на основании запроса правоохранительных органов, требующих раскрытия таких данных. Получение данных о трафике может иметь важное значение для определения источника или адресата соответствующей коммуникации, что в свою очередь будет иметь решающее значение для установления лиц, совершивших преступления против компьютерных систем или данных. Следует иметь в виду, что такие данные часто хранятся лишь в течение короткого периода времени, что обусловлено политикой о защите данных, в соответствии с которой данные не должны храниться более, чем это необходимо для обеспечения их обработки.[29]

С другой стороны, данные трафика, имеющие отношение к совершению компьютерных преступлений, могут находится в распоряжении не одного, а нескольких провайдеров. В этом случае провайдер, получивший ордер на обеспечение сохранности данных трафика, должен незамедлительно сообщить в запрашивающий правоохранительный орган количество данных трафика, достаточное для того, чтобы компетентные органы могли выявить других провайдеров услуг, а также маршрут передачи данных.[30]

Подобно ордерам об оперативном обеспечению сохранности компьютерных данных для осуществления вышеуказанной процедуры в отношении провайдеров услуг не требуется никаких специфических знаний или опыта. Зато критически необходимо четкое понимание того, что представляют собой данные трафика и как их можно впоследствии использовать в качестве доказательств по уголовному делу. По этим вопросам, а также относительно других практических особенностей таких ордеров можно консультироваться с национальным подразделением по вопросам киберпреступлений / высокотехнологичных преступлений.

---

[29] Комплексное исследование УНП ООН по киберпреступности, стр. 127.

[30] См., например, Пояснительную записку к Конвенции Совета Европы о компьютерных преступлениях, п. 169 (Источник: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm).

3.2.2.3 Ордера на предоставление информации

Значительная часть инфраструктуры и компьютерные системы, используемые для Интернет-связи, управляется и принадлежит частному сектору. В распоряжении Интернет-провайдеров, а также провайдеров электронной связи и вэб-сервиса находятся функции управления, хранения и контроля над значительным количеством компьютерных данных, связанных с подключениями к Интернету, транзакциями и контентом. Использование правоохранительными органами принудительных мер, таких как обыск и арест, для получения этих данных невозможно в большинстве случаях как по причине большого количества отдельно проводимых расследований, так и из-за неминуемой угрозы нарушения законной предпринимательской деятельности. Таким образом, адресованные таким третьим лицам ордера на расследование компьютерных данных призваны обеспечить должную юридическую процедуру, конечной целью которой является получение электронных доказательств.[31]

Ордер на предоставление информации используется для получения компьютерных данных или информации об абоненте, которая находится в распоряжении или под контролем физического лица или провайдера услуг. Понятия «владение» и «контроль» относятся к данным, которые и юридически, и технически находятся в физическом владении провайдера услуг или они доступны ему удаленно (например, в управляемом им «облаке» или в удаленном хранилище). Что касается «информации об абоненте», этот термин относится к любой информации, находящейся в распоряжении провайдера услуг и имеющей отношение к абоненту и предоставляемым ему услугам.

Такая информация может быть использована для установления того, какие услуги и связанные с ними технические мероприятия были использованы или используются абонентом, или в случае, когда известен технический адрес, и информация об абоненте необходима для установления личности интересующего лица. [32]

Ордеры на предоставление информации [33] могут использоваться любым правоохранительным органом, который имеет сотрудников, хорошо понимающих, что такое информация об абоненте, и разбирающихся в вопросах приватности и конфиденциальности электронной связи.

---

[31] Комплексное исследование УНП ООН по киберпреступности, стр. 128.

[32] См., например, Пояснительную записку к Конвенции Совета Европы о компьютерных преступлениях, п. 177 (Источник: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm)

[33] Статья 136 Уголовно-процессуального кодекса Грузии; Глава 15 Уголовно-процессуального кодекса Украины.

3.2.2.4 Обыск и изъятие компьютерных данных

Процедуры обыска и изъятия компьютерных данных (т.е., электронных доказательств) являются, по сути, ассимилирующими положениями, направленные на гармонизацию уже существующих уголовно-процессуальных полномочий по обыску и изъятию материальных объектов с точки зрения их применения к компьютерным системам и данным. Обыск и изъятие таких данных существенно отличается от обыска и изъятия материальных объектов, которые предполагают осмотр физической территории и изъятие материального объекта из обыскиваемых помещений. В цифровой среде сбор данных происходит во время обыска и применительно к данным, существующим на тот момент. Есть два основных способа проведения расследования: войти в систему и проводить поиск данных, которые содержатся в компьютерной системе или ее части (как, например, через подключенное устройство хранения данных), или проводить поиск данных на независимом носителе (съемных носителях и т.д.).[34]

Характер электронных доказательств (т.е., данных, хранящихся в компьютерной системе в цифровой форме) предопределяет необходимость иного подхода по сравнению с традиционными процедурами обыска и изъятия. Самое главное – это обеспечить читабельность данных: если данные могут быть прочитаны только с помощью компьютерной системы, в которой они хранятся, должна быть изъята вся система. В остальных случаях достаточно скопировать данные на физический носитель. Аналогичным образом данные могут быть извлечены из подключенных устройств (накопителей, сетей и т.д.). С этой точки зрения процедура изъятия найденных компьютерных данных, в сущности, не отличается от традиционных процедур изъятия.[35]

Одними из самых важных полномочий, предоставляемых в соответствии с Конвенцией Совета Европы о борьбе с компьютерными преступлениями применительно к обыску и изъятию компьютерных данных, является запрещение доступа к соответствующим данным. Такими полномочиями располагают компетентные органы всех государств ГУАМ. [36] Наличие таких полномочий особенно важно в контексте расследований отмывания денег, совершенного с применением информационных технологий, поскольку деактивация оборудования, программного обеспечения и онлайновых платформ, используемых для отмывания преступных доходов, может понадобиться для минимизации причиняемого жертвам ущерба.

---

[34] Инструментарий МСЭ по законодательству в сфере борьбы с киберпреступностью, стр. 36.

[35] См., например, Пояснительную записку к Конвенции Совета Европы о компьютерных преступлениях, п. 187 (Источник: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm)

[36] п. 3 статьи 19 Конвенции Совета Европы о компьютерных преступлениях.

Однако, совсем не многие страны предусмотрели подобные полномочия в своем национальном уголовно-процессуальном законодательстве, лишая, таким образом, свои правоохранительные органы весьма желательных процессуальных полномочий.

С точки зрения практического применения, ситуация с обыском и изъятием может оказаться еще менее понятной, нежели с другими, более специфическими процессуальными полномочиями. С одной стороны, обыск и изъятие традиционно может осуществляться любым правоохранительным органом. При необходимости, могут привлекаться специалисты. [37] С другой стороны, изъятие данных из компьютерных систем или же изъятие самих компьютерных систем из обыскиваемых помещений может потребовать более глубоких экспертных знаний, чтобы обеспечить читабельность и целостность данных. Поэтому следование инструкциям и, при необходимости, непосредственное участие в таких случаях национальных подразделений по вопросам киберпреступлений / высокотехнологичных преступлений имеет очень важное значение.

3.3 Электронные доказательства и обеспечение их последовательности

Электронные доказательства, полученные с помощью надлежащих правовых процедур, как описано в предыдущих главах, все еще потребуют должной обработки для того, чтобы их можно было представить в качестве допустимых доказательств в суде. В большинстве случаев соблюдения правовых требований, предъявляемых к процессуальным действиям по сбору и изъятию доказательств, будет достаточно, чтобы гарантировать допустимость доказательств в уголовном судопроизводстве. Однако, электронные доказательства имеют некоторые дополнительные характеристики, которые необходимо учитывать для обеспечения соответствия таким требованиям.

3.3.1 Экспертная оценка и анализ

Системы уголовного правосудия в странах ГУАМ полагаются на экспертизу и свидетельские показания во многих случаях, когда доказательства должны быть должным образом обработаны и представлены в уголовном судопроизводстве.[38] Ставка на экспертную поддержку особенно актуальна для обработки электронных доказательств, так как современные

[37] п. 4 статьи 19 Конвенции Совета Европы о компьютерных преступлениях.

[38] Статья 97 Уголовно-процессуального кодекса Азербайджанской Республики; статья 52 Уголовно-процессуального кодекса Грузии; статья 88 Уголовно-процессуального кодекса Республики Молдова; статья 69 Уголовно-процессуального кодекса Украины.

компьютерные системы и устройства имеют индивидуальные специфические характеристики и конфигурации, требующие точного соблюдения определенных процедур для извлечения из них соответствующих данных. И наоборот, обработка электронных доказательств неспециалистами значительно увеличивает риск их непреднамеренных изменений и, как следствие, недопустимости таких доказательств в уголовном судопроизводстве.

В ходе проведения расследований по отмыванию денег, совершенных с использованием виртуальных валют, может возникнуть необходимость в самых разнообразных знаниях. Первая очевидная необходимость – в финансовых экспертах, способных провести профессиональный анализ операций или определить стоимость преступных доходов. Однако, электронные доказательства, являющиеся основными в таких делах, могут потребовать еще более узкоспециальных знаний технического характера, иными словами – цифровой криминалистической экспертизы.

Цифровая криминалистическая экспертиза в одной стране может быть отнесена к компетенции сразу нескольких ведомств. Первичная экспертиза оперативных данных обычно проводится национальными подразделениями по вопросам киберпреступлений/ высокотехнологичных преступлений. Поэтому если возникает необходимость в сборе данных трафика или перехвате данных контента, за экспертной поддержкой целесообразно обращаться непосредственно в это подразделение. Однако, основная часть цифровой криминалистической экспертизы, направленная на обработку уже собранных доказательств, проводится либо специализированными центрами цифровой криминалистической экспертизы (обычно являются частью полиции), либо независимыми государственными или частными экспертными центрами, которые имеют более обширный опыт по всем видам традиционных и электронных доказательств. Важным фактором при выборе между такими учреждениями является уровень знаний и опыта, которые часто можно получить только в результате специализированного обучения и сертификации.

Кроме уровня знаний и опыта первостепенное значение также имеет использование соответствующих процедур, инструментов и методов. Равно как общей диагностики компьютерных систем не достаточно для предоставления надежных доказательств, так и специализированное оборудование и программное обеспечение являются важными условиями для проведения анализа электронных доказательств и имеют непосредственное влияние на их допустимость. Такие инструменты, методы и процедуры должны быть прослеживаемыми и воспроизводимыми другими специалистами, чтобы полученная информация имела силу доказательств, и что могло бы быть доказано в суде, если возникнет такая необходимость.

Помимо экспертизы собранных доказательств, есть еще сферы, где может понадобиться помощь специалистов по цифровой криминалистической экспертизе или аналогичных специалистов. Например, для перехвата, поиска и изъятия данных контента или для обеспечения сохранности данных. Экспертная помощь в таких случаях может служить дополнительной гарантией надлежащего обращения с электронными доказательствами с целью обеспечения их допустимости в уголовном судопроизводстве.

Знания, необходимые для обработки и анализа электронных доказательств, могут наличествовать во многих учреждениях как государственных, так и частных. Но при подборе экспертов нужно учитывать не только вопросы качества или целесообразности экспертной оценки, но и вопросы ее объективности. Поскольку эксперты, как правило, опрашиваются в суде в качестве свидетелей, их общественный и моральный облик и, что более важно, профессиональная принадлежность может вызвать сомнения в их объективности. Проецируя это на вопросы электронных доказательств, может оказаться весьма заманчивым воспользоваться экспертным анализом, предлагаемым подразделением по вопросам киберпреступлений / высокотехнологичных преступлений. Однако, учитывая, что такое подразделение является частью криминальной полиции и участвует в расследовании и уголовном преследовании киберпреступлений, изначальная склонность таких экспертов к позиции государственного обвинения и государственным интересам может вызвать сомнение в их непредвзятости и объективности.

3.3.2 Обеспечение последовательности электронных доказательств

Обеспечение последовательности электронных доказательств, по сути, не отличается от обеспечения последовательности традиционных доказательств. Уголовное производство полагается на весьма формализованные процедуры и требования. Поэтому соблюдение установленных процедур, допуск к обработке доказательств только лиц, имеющих для этого достаточную квалификацию, а также сохранение всей необходимой документации, дающей представление о том, как доказательства хранились и обрабатывались, является стандартным подходом, используемый в любых уголовных производствах и применимый к любому типу доказательств. С другой стороны, электронные доказательства имеют ряд особенностей, которые необходимо учитывать для того, чтобы обеспечить их надлежащую последовательность:

- **Целостность данных**: Электронные доказательства являются крайне волатильными. Доступ к компьютерной системе, даже просто для просмотра файлов или вэб-страниц, в большинстве случаев приведет к изменению данных (например, списка последних просмотренных документов) до такой степени, что они не смогут быть использованы в качестве доказательств в уголовном судопроизводстве. Поэтому компьютерные данные следует надежно предохранять от возможных изменений. Для обеспечения аутентичности данных могут применяться разнообразные приемы и методы (например, доступ в режиме «только для чтения», анализ цифровой копии, а не оригинала доказательств, формирование изображений или фиксация обработки доказательств и т.д.).

- **Контрольный след**: Сохранение всех официальных документов, подтверждающих процесс расследования, является очень важным. В рамках уголовного производства следователи пользуются стандартизированными формами или контрольными списками для документирования расследования, а также, чтобы не упустить какой-нибудь из этапов экспертизы с целью комплексного изучения компьютерных систем жертвы и подозреваемого. Аналогичным образом должны фиксироваться все этапы обработки доказательств вне зависимости от того, происходит это на месте преступления или в лаборатории судебной экспертизы. Скриншоты, фотографии и видеозаписи значительно повысят качество контрольного следа обработки электронных доказательств.

- **Экспертная поддержка**: Во многих случаях сугубо технический характер компьютерной среды и содержащихся в ней данных потребует привлечения специалистов по компьютерной криминалистической экспертизе. Потребность в помощи специалистов обуславливается узкой специализацией цифровой криминалистической экспертизы (например, анализа мобильных вредоносных программ), а также ограниченной доступностью оборудования для проведения такой экспертизы. Поэтому, не являясь во всех случаях обязательным для проведения, экспертный анализ может значительно усилить аргументы стороны процесса, желающей предъявить такие доказательства.

- **Законность**: Компьютерные системы, являющиеся источником электронных доказательств, как правило, содержат, по меньшей мере, некоторое количество приватной информации, которая не будет иметь отношение или ценности для следствия. Поэтому очень важно отсортировать данные, которые имеют отношение к расследованию, от приватной информации, в которой нет необходимости. В некоторых случаях может оказаться весьма не просто провести такое разграничение. Поэтому для дальнейшего

анализа информации может понадобиться санкция суда, призванная обеспечить сохранность таких данных.[39]

3.3.3 Допустимость электронных доказательств

Поскольку конечной целью является использование полученных и проанализированных доказательств для поддержания обвинения в суде, электронные доказательства, чтобы быть допустимыми, должны быть получены в соответствии с действующим законодательством и соответствующей передовой практикой. Несмотря на различия в деталях в зависимости от национального законодательства, следующие базовые критерии, как правило, всегда должны приниматься во внимание:

- **Аутентичность**: Связь между материалами доказательной базы и расследуемым случаем должна быть неоспорима. В этом смысле электронные доказательства ничем не отличаются от вещественных доказательств, например, бумажного документа. При этом необходимо обеспечить аутентичность доказательств. Разница между электронными и физическими доказательствами по большей части заключается лишь в легкости, с которой электронные доказательства могут быть изменены намеренно или непреднамеренно.

- **Полнота**: Доказательства должны раскрывать все картину, а не отдельную ее часть. Доказательства оцениваются с точки зрения сбалансированности и объективности и в совокупности с другими доказательствами, будь-то физическими или электронными, должны выстраивать отдельные события в целостную картину.

- **Достоверность**: Не должно быть никаких сомнений в отношении того, как собирались доказательства и как они обрабатывались, что могло бы оказать влияние на их аутентичность и правдивость. В случае если есть сомнения в отношении электронных данных, приведенных в качестве доказательств, задача защиты поднять вопрос об их допустимости. Как только такой вопрос поднимается, обвинение должно реагировать на него, как правило, путем предоставления достаточных доказательств того, что «целостность данных заслуживает доверия и поэтому они являются достоверными».

---

[39] «Электронные доказательства: базовое руководство для сотрудников полиции, прокуроров и судей», подготовленное в рамках совместного проекта Совета Европы и Европейского Союза по региональному сотрудничеству по борьбе с киберпреступностью, стр. 131-134 (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp)

- **Правдоподобность**: Доказательства должны быть правдоподобны и понятны для участников уголовного судопроизводства, особенно для суда. Представляя их, важно продемонстрировать действительный вес экспертного заключения. Презентация электронных доказательств суду и присяжным должна быть наглядной, с использованием компьютерных презентаций, видео демонстраций, компьютерной графики, таблиц и диаграмм. Стороны, представляющие доказательства, должны быть осведомлены о предубеждении, которое использование такой технологии может вызвать, и быть готовы обсуждать эти вопросы, если защита оспорит использование такой технологии.[40]

3.4 Гарантии и меры защиты

Все процедуры, применимые к электронным доказательствам, должны основываться на уважении к фундаментальным правам и гарантиям участников уголовного судопроизводства. Поскольку процессуальные действия, имеющие отношение к расследованию отмывания денег с использованием виртуальных валют берут свое начало из законов и нормативных положений в сфере борьбы с киберпреступлениями, аналогичные подходы, предусмотренные действующими стандартами,[41] будут применяться и в этом случае. Такие меры и гарантии носят практический характер и должны рассматриваться в качестве неотъемлемой характеристики процессуальных действий, к которым они применяются.[42]

В первую очередь все процессуальные действия, которые предполагают вторжение в частную жизнь человека, должны осуществляться в рамках открытых уголовных расследований. И не имеет значения, о каких расследованиях идет речь – киберпреступлений, отмывания денег или мошенничества – официальное решение о начале уголовного расследования рассматривается в качестве одной из гарантий против злоупотребления процессуальными полномочиями, способных оказать непосредственное влияние на частную жизнь человека.

---

[40] «Электронные доказательства: базовое руководство для сотрудников полиции, прокуроров и судей», подготовленное в рамках совместного проекта Совета Европы и Европейского Союза по региональному сотрудничеству по борьбе с киберпреступностью, стр. 146-147.

[41] К примеру, статья 15 Конвенции Совета Европы о компьютерных преступлениях, актуальная для стран ГУАМ.

[42] Дополнительный анализ о гарантиях и мерах защиты, а также примеры из национальных законодательств можно найти во Всеобъемлющем исследовании УНП ООН по киберпреступности, стр. 136-141.

В некоторых юрисдикциях обязательным условием для применения некоторых специальных следственных полномочий, используемых для обеспечения электронных доказательств, например, перехвата данных контента или обеспечения сохранности данных трафика, является серьезный характер преступления. Иными словами, преступление должно предусматривать наказание в виде лишения свободы на определенный срок. Это нужно принимать во внимание по одной простой причине: большинство преступлений против компьютерных систем и данных не квалифицируются национальным уголовным законодательством как серьезные преступления, тем самым лишая возможности применения специальных процессуальных полномочий. Поэтому практикующие юристы должны предпочесть квалифицировать киберпреступные деяния в контексте преступления по отмыванию денег, которое в любом случае будет являться серьезным преступлением.

Судебный приказ на применение специальных процессуальных полномочий, предполагающие вторжение в частную жизнь человека, в частности, перехват данных контента, рассматривается как важнейшая гарантия соблюдения баланса интересов государства и индивидуума. В контексте преступлений, связанных с использованием виртуальных валют, это часто будет означать осознанный отказ правоохранителей от использования таких процедур не в последнюю очередь по соображениям оперативности. В то же время замена таких «щадящих» процедур другими опциями (как, например, обыск и изъятие в неотложных обстоятельствах без судебного приказа) может повлечь за собой определенные сложности, если такой выбор будет оспорен в суде с позиции пропорциональности.

И наконец, особое внимание должно быть уделено национальным нормам в области защиты персональных данных, в частности, тех «чувствительных» данных, которых так или иначе может коснуться расследование. И хотя существует общий международный стандарт о неприменимости гарантий защиты данных (например, согласие субъекта на обработку данных) в случаях проведения уголовных расследований, все более крепнет тенденция по применению требований по защите данных к полицейским мероприятиям по сбору и обработке оперативных данных. Правоохранительные органы должны быть осведомлены о таких стандартах и, если возможно, консультироваться с местными учреждениями по защите данных.

4 Следственные инструменты и методологии

В этом разделе будут рассмотрены некоторые из доступных инструментов, используемые для выявления и расследования отмывания преступных доходов, совершенного посредством виртуальных валют.

4.1 Красные флажки / Индикаторы

Красные флажки/ индикаторы являются важным следственным инструментом при проведении финансовых расследований. Под «финансовым расследованием» понимается расследование финансовых дел, имеющих отношение к преступной деятельности, с целью:

- выявления масштаба преступных сетей и/или масштабов преступности;
- выявления и отслеживания доходов от преступлений, средств террористов или иного имущества, которые подлежат или могут подлежать конфискации; и
- разработки доказательств, которые могут быть использованы в уголовном судопроизводстве[43].

Независимо от того, какое ведомство уполномочено проводить финансовые расследования, будь то подразделение финансовой разведки (ПФР), правоохранительный орган, регулятор, подразделение по вопросам киберпреступлений или любой другой следственный орган, следственные проблемы, возникающие при использовании виртуальных валют, будут схожими. Детальное рассмотрение специализированных подразделений по проведению финансовых расследований представлено в главе 5.5.

На сегодняшний момент еще не проводились исследования, посвященные вопросам расследований и разработки красных флажков/ индикаторов, которые можно было бы использовать для выявления фактов незаконного использования виртуальных валют. В то же время уже проводились исследования, в которых рассматривались красные флажки/ индикаторы, применимые к более общим случаям отмывания преступных денег в сети Интернет или к отмыванию денег с помощью новых способов платежей.[44], [45]

---

[43] Пояснительная записка к Рекомендации 30, «Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения – Рекомендации ФАТФ», ФАТФ-ГАФИ, Февраль 2012. (Источник: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

[44] «Отмывание денег посредством новых способов платежей», ФАТФ-ГАФИ, Октябрь 2010 (Источник: http://www.fatf-gafi.org/media/fatf/documents/reports/ML using New Payment Methods.pdf)

[45] «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», Международного проекта

Многие из красных флажков/ индикаторов, описанные в этих исследованиях, применимы и в случае отмывания преступных доходов с использованием виртуальных валют. Вот некоторые из них:

- Расхождения между представленными идентификационными данными пользователя и его IP-адресом. Например, когда при создании эккаунта пользователь указывает почтовый адрес в Великобритании, а на практике оказывается, что все IP-адреса, связанные с деятельностью этого пользователя, из Японии.
- Подозрительные IP-адреса и подозрительные имена пользователей (клички, прозвища, ICQ номера) помогут в обнаружении потоков криминальных денег.
- Вход или попытки входа с ненадежных IP-адресов или с IP-адресов, ранее идентифицированных как имеющие отношение к подозрительной деятельности.

Однако, красные флажки/ индикаторы, описанные в этих исследованиях, в том числе упомянутые выше, носят очень общий характер и применимы ко многим расследованиям, имеющие отношение к сети Интернет.

Возможно, несколько более значимыми могут оказаться красные флажки/ индикаторы, предложенные ФАТФ, и которые могут указать на причастного к незаконной деятельности провайдера платежных услуг. В исследовании ФАТФ эти красные флажки/ индикаторы как раз приводятся в контексте причастного провайдера платежных услуг. Однако, как уже отмечалось в Модуле 2, эта типология применима и к виртуальным валютам. Поэтому красные флажки/ индикаторы, указывающие на подозрительную деятельность провайдеров услуг предоплаченных карт, могут в равной степени быть актуальны и в случае провайдеров виртуальных валют. Примерами таких красных флажков/ индикаторов являются:

- Большое количество банковских счетов, принадлежащих одному администратору виртуальной валюты или компании, занимающейся обменом виртуальных валют (иногда находятся в разных странах), которые, по всей видимости, используются как транзитные счета (что может свидетельствовать о деятельности, характерной для второго этапа процесса отмывания денег – «расслоения»).
- Администратор виртуальной валюты или компания, занимающейся обменом виртуальных валют, находятся в одной стране, но имеет

Совета Европы по борьбе с киберпреступностью и МАНИВЕЛ, Март 2012 (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

счета в других странах, где они не имеют существенной клиентской базы (нелогичное обоснование такой бизнес-деятельности, что может быть подозрительным)

- Круговое движение денежных средств между банковскими счетами, находящихся в разных странах и принадлежащих разным администраторам виртуальной валюты или компаниям, занимающихся обменом виртуальных валют (может свидетельствовать о деятельности, характерной для второго этапа процесса отмывания денег – «расслоения», если такая деятельность не является обычной бизнес-активностью компании);
- Объем и частота операций с наличностью (иногда разбиты на суммы, меньшие порога предоставления отчетности), которые проводятся собственником администратора виртуальной валюты или компании, занимающейся обменом виртуальных валют, и не имеют экономического смысла.

4.2 Следственные индикаторы

Во время исследования компьютера, подозреваемого могут быть выявлены различные индикаторы использования виртуальных валют. В этой главе будут рассмотрены некоторых методы, позволяющие определить доказательства фактов использования подозреваемым виртуальных валют.

4.2.1 Наличие программного обеспечения, связанного с использованием виртуальных валют

Некоторые виртуальные валюты, особенно децентрализованные, предполагают установку соответствующего программного обеспечения. Наличие такого программного обеспечения (ПО) на исследуемом компьютере может быть индикатором использования виртуальных валют. Далее представлены примеры таких ПО.

4.2.1.1 Bitcoin

Программное обеспечение, устанавливающееся на компьютер и предоставляющее возможность использования сети Bitcoin, называется Bitcoin-кошелек. Существует множество различных Bitcoin-кошельков, как например:

- Bitcoin Core[46]
- MultiBit[47]

[46] https://bitcoin.org/en/download
[47] https://multibit.org/

- Hive[48]
- Bitcoin Armory[49]
- Electrum[50]

Некоторые, но не все, из этих ПО после установки потребуют загрузки всего файла цепочки блоков, размер которого достигает почти 20 Гб. Огромный размер цепочки блоков может помочь установить директорию, используемую программным обеспечением Bitcoin. Кроме того, наличие самого кошелька, часто обозначенного как wallet.dat, является весомым индикатором использования сети Bitcoin.

4.2.1.2 Другие распределенные виртуальные валюты

Существует также такое программное обеспечение как LiteCoin [51] и DogeCoin [52] . Наличие таких типов ПО также является показателем использования соответствующих виртуальных валют.

Подобно Bitcoin-кошелькам, упомянутым выше, некоторые из этих ПО после установки проводят загрузку больших по объему файлов, являющиеся эквивалентом цепочки блоков Bitcoin для данной виртуальной валюты.

Аналогичным образом для отправки и получения переводов WebMoney необходимо загрузить соответствующую программу.[53]

4.2.1.3 Виртуальные валюты виртуальных миров

Многие виртуальные валюты виртуальных миров, такие как Second Life Linden Dollars[54], Project Entropia Dollars[55] или World-of-Warcraft Gold[56] могут быть приобретены при помощи приложений, используемых для взаимодействия с виртуальным миром.

Соответственно, наличие таких приложений может указывать на использование виртуальных валют этих виртуальных миров.

---

48 https://www.hivewallet.com/
49 https://bitcoinarmory.com/
50 https://electrum.org/
51 https://litecoin.org/
52 http://dogecoin.com/
53 http://www.wmtransfer.com/eng/about/demo/classic/index.shtml
54 https://secondlife.com/support/downloads/
55 http://www.entropiauniverse.com/download/
56 http://us.battle.net/wow/en/

4.2.2 История просмотра вэб-страниц, связанных с виртуальными валютами

Не все распределенные виртуальные валюты предусматривают установку программного обеспечения. Например, Ripple-клиент работает как приложение JavaScript в браузере пользователя. [57] Другие виртуальные валюты для отправки и получения виртуальной валюты предлагают на выбор как загружаемое программное обеспечение, так и возможность взаимодействия через вэб-браузер. [58]

Кроме того торговля виртуальными валютами на биржах виртуальных валют, как правило, осуществляется посредством вэб-браузера.

Таким образом, закладки, история посещенных вэб-страниц и кэш на компьютере подозреваемого могут предоставить ценные доказательства использования виртуальных валют.

4.2.3 Услуги удаленного хранения данных

Напомним, что виртуальные валюты, в частности, децентрализованные виртуальные валюты, представляют собой цифровое выражение стоимости. При этом цифровым выражением стоимости они являются сами по себе вне зависимости от того, как и где они хранятся, что является важной характеристикой.

Учитывая вышесказанное, нет причин полагать, что цифровое выражение стоимости обязательно должно храниться локально на исследуемом компьютере. Объем данных в цифровом выражении, как правило, небольшой (менее 100 байт), поэтому есть бесчисленное множество способов хранить их удаленно.

Один из таких возможных способов – воспользоваться услугами удаленного хранения данных. Сегодня предлагается большое количество подобных услуг, большинство из которых включают ограниченные возможности бесплатного обслуживания.[59], [60], [61]

Помимо этого с той же целью могут использоваться и другие услуги, не являющиеся непосредственно услугами удаленного хранения данных. Одним из таких примеров могут быть услуги электронной почты,

[57] https://ripple.com/wiki/Client_Manual
[58] http://www.wmtransfer.com/eng/about/demo/light/index.shtml
[59] https://www.dropbox.com/
[60] https://drive.google.com/
[61] https://www.amazon.com/clouddrive/home/

доступные через вэб-браузер[62], [63]. В некоторых случаях обеспечение приватности рекламируется в качестве отличительной характеристики таких услуг.[64], [65] Другим примером могут быть услуги по управлению заметками или задачами.[66]

Многие из этих услуг можно получить различными способами, в том числе через:

- Соответствующее установленное программное обеспечение
- Вэб-интерфейс
- Стандартные приложения, такие как электронная почта
- Мобильные приложения

Установление фактов использования услуг по удаленному хранению данных необязательно будут указывать на использование виртуальных валют. Однако, если есть подозрения или известно, что виртуальные валюты использовались для совершения преступления, установление и исследование сервисов по удаленному хранению данных может стать важным источником доказательств.

4.2.4 Программное обеспечение по хранению учетных данных

Существует программное обеспечение, позволяющее хранить информацию об эккаунтах и логинах пользователя.[67], [68], [69], [70] Такое ПО обычно устроено так, что пользователь, имея один пароль, получает доступ к данным об остальных своих учетных записях, хранящихся в зашифрованном файле. Такое ПО часто предоставляют возможность хранить небольшие текстовые заметки.

Многие вэб-браузеры также имеют возможность хранить пароли доступа к вэб-сайтам.[71], [72], [73], [74]

---

62 https://www.gmail.com/intl/en/mail/help/about.html
63 https://mail.yahoo.com/
64 https://www.hushmail.com/
65 https://lavaboom.com/
66 https://evernote.com/
67 https://agilebits.com/onepassword
68 https://lastpass.com/
69 https://www.my1login.com/content/index.php
70 http://www.f-secure.com/en/web/home_global/key
71 https://support.mozilla.org/en-US/kb/password-manager-remember-delete-change-passwords
72 http://www.cnet.com/uk/how-to/how-to-save-passwords-for-all-web-sites-in-safari/
73 https://support.google.com/chrome/answer/95606?hl=en
74 http://windows.microsoft.com/en-ie/internet-explorer/fill-in-forms-remember-passwords-autocomplete#ie=ie-11

Вполне возможно, если такое программное обеспечение будет выявлено, что учетные данные, связанные с использованием виртуальных валют или даже сама виртуальная валюта будут храниться в таком ПО.

Многие из этих ПО поддерживают функции удаленного хранения (учетных данных, заметок и т.п.), плагинов для браузеров и синхронизации информации с мобильным приложением.

Однако, опять же установление фактов использования такого ПО необязательно будут свидетельствовать об использовании виртуальных валют. Но если есть подозрения или известно, что виртуальные валюты использовались для совершения преступления, такое ПО может быть потенциальным источником ценных доказательств.

4.2.5 Виртуальные машины

Виртуальная машина – это программное обеспечение, позволяющее эмулировать работу целой операционной системы. [75], [76], [77] Это означает, к примеру, что пользователь может иметь как бы второй windows-компьютер, обозначаемый как «гость», который хранится на компьютере, обозначаемый как «хозяин». Большинство виртуальных машин позволяет шифровать файлы, находящиеся на жестком диске виртуальной машины. Это означает, что виртуальная машина не может быть активирована без соответствующего пароля.

При таких обстоятельствах можно использовать защищенную паролем виртуальную машину для всех операций с виртуальными валютами, при этом не оставляя никаких следов использования виртуальных валют в основной операционной системе, обозначаемой как «хозяин».

Есть много законных оснований, как для использования виртуальных машин, так и для шифрования жестких дисков виртуальных машин. Но в случае, если предполагается или известно об использовании виртуальных валют, факт наличия виртуальных машин достоин расследования.

---

[75] http://www.vmware.com/
[76] https://www.virtualbox.org/
[77] http://www.parallels.com/

4.2.6 Мобильные устройства

Программное обеспечение для виртуальных валют (подглава 4.2.1) и просмотр вэб-страниц, связанных с виртуальными валютами (подглава 4.2.2) могут быть также найдены на мобильных устройствах. Примеры ПО, доступного для мобильных устройств, включают Bitcoin[78], [79], WebMoney[80] и Ripple[81] -клиенты.

Поэтому доказательства, собранные в ходе изучения мобильных устройств, также могут быть важным индикатором использования виртуальных валют для отмывания преступных доходов.

4.3 Криминалистическая экспертиза

Корректный сбор доказательств необходим для построения дела. При этом доказательства по делам, связанных с использованием виртуальных валют, могут быть найдены во многих местах. В нижеследующих подглавах будут рассмотрены некоторые из источников, данных, а также характер доказательств, которые могут быть там найдены.

Полное рассмотрение технических процедур по сбору и анализу электронных доказательств выходит за рамки данного пособия, но заметим, что такие процедуры должны быть проведены специализированным подразделением криминалистического анализа в соответствии с лучшим практиками по сбору и обработке электронных доказательств, как описано в главе 3.3.

4.3.1 Компьютер подозреваемого

Компьютер подозреваемого во многих случаях может быть ценным источником доказательств. Имеется в виду не только сам компьютер, но и любой другой носитель информации (CD, DVD, внешние жесткие диски, флэш-накопители и т.д.), которые были найдены подсоединенными к компьютеру подозреваемого или известно, что они контактировали с ним.

Вот некоторые примеры доказательств, которые могут быть извлечены из компьютера подозреваемого:

- Доказательства в виде учетных записей, посещения вэб-сайтов, электронной почты и пр., которые подтверждают взаимосвязь

78 https://play.google.com/store/apps/details?id=com.mycelium.wallet
79 https://play.google.com/store/apps/details?id=de.schildbach.wallet
80 https://wiki.wmtransfer.com/projects/webmoney/wiki/WM_Keeper_Mobile
81 https://ripple.com/blog/introducing-ripple-client-the-ios-app/

подозреваемого с администратором или биржей (обменником) виртуальных валют.

- Доказательства, свидетельствующие о владении подозреваемым некоторым количеством виртуальной валюты.
- В случае с bitcoin вероятно получится установить конкретные адреса, контролируемые подозреваемым. Впоследствии bitcoin-адреса могут быть исследованы с целью определить, с каких адресов bitcoin переводились на адрес подозреваемого и на какие адреса bitcoin переводились с адреса подозреваемого.[82]
- IP-адрес компьютера в определенное время может быть связан с известными операциями подозреваемого или другой финансовой деятельностью.
- Доказательство использования услуг удаленного хранения данных, посредством которых может обеспечиваться хранение виртуальных валют (см. следующую подглаву).
- Пароли или другие учетные данные, которые могут быть использованы для доступа к счетам в виртуальных валютах или к виртуальной валюте.

Пример: Bitcoin-кошелек

Этот пример демонстрирует программное обеспечение Bitcoin – Multibit.[83] Multibit – это облегченная версия Bitcoin-кошелька для Windows, MacOS и Linux.[84] На этом примере будет показана структура и функционирование этого ПО. Представим, что следователь имеет соответствующие инструменты и знания для сбора доказательств в соответствии с требованиями криминалистической экспертизы.

По умолчанию приложение устанавливается в директорию C:\Program Files (x86)\Multibit-0.5.18. При первом запуске Multibit создается новый, пустой кошелек с названием «multibit.wallet». По умолчанию этот кошелек не защищен паролем и находится по адресу C:\Users\<user>\AppData\Roaming\MultiBit\multibit.wallet, где «<user>» – это имя пользователя, вошедшего в систему. Пользователь может создать столько кошельков, сколько он захочет. По умолчанию они все будут храниться в той же папке «multibit.wallet».

Multibit будет создавать различные резервные копии созданных и настроенных кошельков в папку «<wallet name>-data», где <wallet name> – это название конкретного кошелька. Эта папка резервного

[82] http://blockchain.info/
[83] https://www.multibit.org/
[84] Данный пример проводился на Windows 7 Professional, 64-бит, Multibit версия 0.5.18.

копирования также по умолчанию хранится в вышеупомянутом каталоге данных Multibit.

Пример основного экрана Multibit можно увидеть на Изображение 2. На левой стороне основного экрана Multibit приведен список кошельков, которые пользователь создал и настроил, с указанием количества bitcoin в каждом кошельке. На правой стороне экрана находится вкладка для отправки bitcoin на другой кошелек, вкладка для получения bitcoin, включая выбранный принимающий Bitcoin-адрес, и вкладка, позволяющая просмотреть все проведенные транзакции.

Пользователь может создавать любое количество получающих Bitcoin-адресов, используя кнопку «New» на вкладке для получения bitcoin.

Получающий Bitcoin-адрес представляет собой буквенно-циферную строку, например:

1FjckeaGiEZWawYHmhKU79BxPHvNu4Egqu

Файл «.wallet» содержит приватные ключи, связанные с каждым из идентификаторов Bitcoin-кошелька, а также данные о транзакции, связанные с каждым адресом.[85] Файл хранится в двоичном формате и может быть открыт при помощи Multibit. Самый простой способ проверить содержимое файла «.wallet», найденный на компьютере подозреваемого, это скопировать директорию данных Multibit на компьютер, используемый для криминалистической экспертизы, и открыть его помощью с Multibit.

Все транзакции имеют связь с Bitcoin-адресами и сохраняются в цепочке блоков Bitcoin, которую можно найти в Интернете.[86] Таким образом, информация о Bitcoin-адресах, найденная в компьютере подозреваемого, может быть дополнительно изучена на предмет установления того, какие транзакции предшествовали и следовали после переводов с/ на Bitcoin-адреса, связанные с подозреваемым.

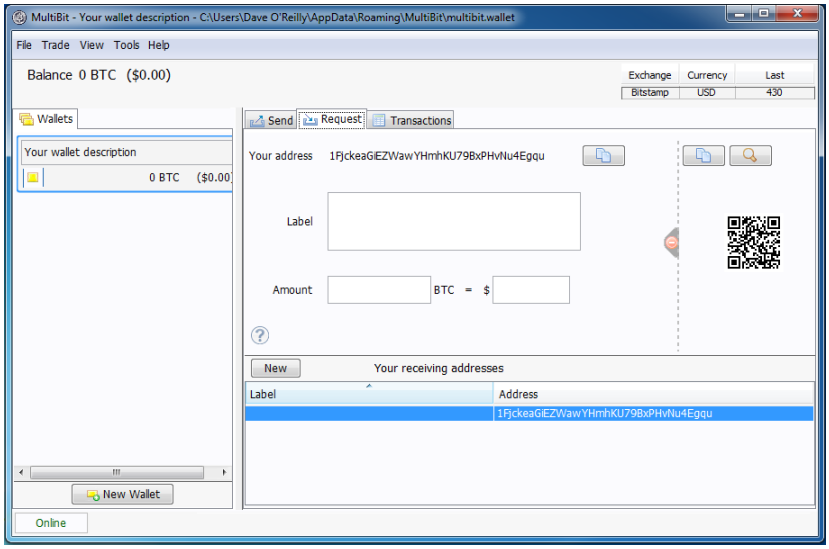
При этом невозможно с помощью информации, хранящейся в Multibit, связать Bitcoin-адреса с IP-адресами или другими идентификационными данными за исключением, конечно, Bitcoin-адресов, которые хранятся в настроечных файлах Multibit и могут иметь связь с другими идентификационными данными, найденными в компьютере подозреваемого.

Наряду с файлом «.wallet» можно найти соответствующий файл «.info», который будет содержать все адреса получения и отправки bitcoin.

85 https://multibit.org/en/help/v0.5/help_fileDescriptions.html
86 http://blockchain.info/

Пример «.info»-файла приведен на Изображение 3. Каждая строка, начинающаяся с «receive» является получающим адресом. Соответственно, отправляющий адрес будет в таком же формате, но строка начинается с «send». В конце «.info»-файла можно также увидеть месторасположение резервной копии кошелька.

Изображение 2: основной экран MultiBit



Изображение 3: info-файл кошелька MultiBit

multiBit.info,1
walletVersion,2
receive,16tX9dKcSLDuKDUhbB9Qy2KvdRKUKFgzNU,
receive,1CMVGKneZJD3S8vaARnHdnQLYmGrApVucE,
receive,16wGizcLnQo6xSs5iSigstN9Ah3KLK4yvK,
receive,1Bi8bwvaA8PWU1XoC8PD1UDHd16MfcT1x7,
receive,1LKTxZrLd2vbT3uRFKPSLn9pm8ZnHnjFiH,
receive,1GG6Sq5JxAm3aEWNc98m1NzQmFMwyggLVq,
receive,1PZtgVQHErx1aCtZfGxcx3zutbCaaCPEwu,
receive,1MCsQKTsqBfg2asQNy1x8dGDkxB6mkvpRy,
property,walletDescription,Your%20wallet%20description
property,receiveLabel,
property,walletCleanedOfSpam,true
property,receiveAddress,14nuoifKUmXDTnTbGDyXKFZr9rbDDteiao
property,walletBackupFile,C%3A%5CUsers%5CDave%20O%27Reilly%5CAppData%5CRoaming%5CMultiBit%5Cmultibit-data%5Crolling-backup%5Cmultibit-20140506170256.wallet

Пример: Second Life Linden Dollars

Second Life Linden Dollars можно приобрести в обменнике LindeX[87] или в виртуальном мире, используя Second Life Viewer.[88]

Для покупки Linden Dollars при помощи Second Life Viewer достаточно просто нажать кнопку «Buy L$», как показано на Изображение 4, введя желаемую сумму Linden Dollars, и покупка сделана. Такой способ покупки Linden Dollars нужно первоначально настроить через вэб-сайт Second Life.

Покупка и продажа виртуальной валюты может также происходит через обменник Linden непосредственно на вэб-сайте Second Life или через другой сторонний обменник. Покупка через обменник Linden осуществляется путем указания либо желаемого количества Linden Dollars, либо количества долларов США, которые будут потрачены на покупку, как показано на Изображение 5. Продажа происходит аналогичным образом.

Пароли, связанные с эккаунтами в Second Life, нельзя восстановить непосредственно из Second Life Viewer. Но их можно получить из программы по управлению паролями, как описано в подглаве 4.2.4. Кроме того, вполне возможно, что связанные с эккаунтами Second Life пароли могли быть сохранены вэб-браузером.

Информация о количестве Linden Dollars, способах оплаты и проведенных операциях хранится вместе с Second Life-эккаунтом. Поэтому Linden Labs может раскрыть такую информацию при условии соблюдения необходимых юридических формальностей любым из нижеперечисленных способов:

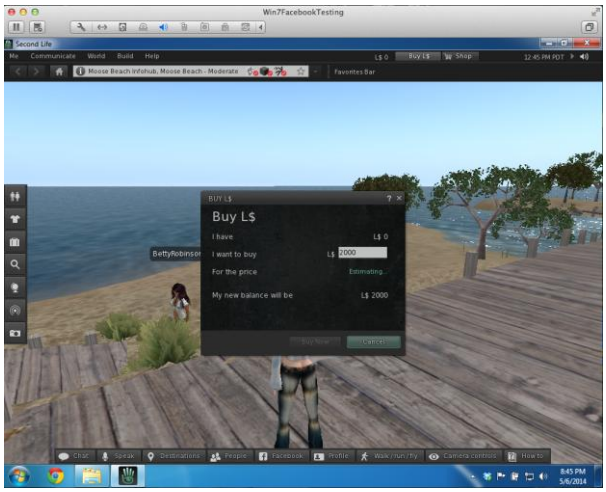
- Прямое обращение к Linden Labs с запросом о предоставлении данных об эккаунте, которые не являются конфиденциальными в соответствии с Условиями предоставления услуг.[89]
- Использование полицейских каналов, таких как контактные центры 24/7 (для государств-участниц Конвенции Совета Европы о компьютерных преступлениях) или G8 Сеть подразделений в сфере высокотехнологичных преступлений, или национальные бюро Интерпол, если ни один из первых двух каналов не может быть использован. Возможности и оперативность предоставления ответа

87 http://www.lindex.com/eu/
88 https://secondlife.com/support/downloads/
89 http://lindenlab.com/tos#tos7

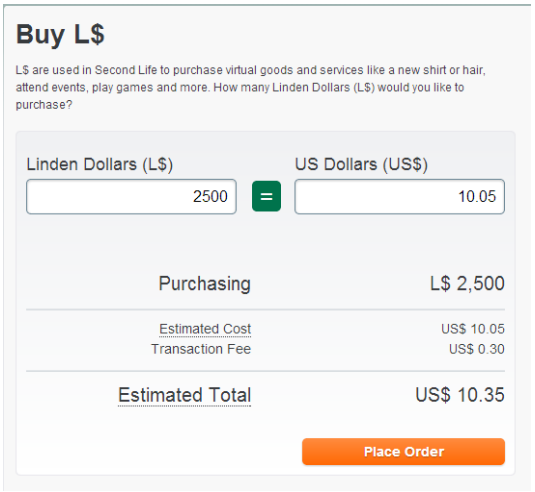
полностью зависит от адресата такого запроса. Но это будет все равно гораздо быстрее, чем использование официальных процедур взаимной правовой помощи.

- Процедура взаимной правовой помощи, осуществляемая Генеральной прокуратурой или Министерством юстиции. Оперативность является главной проблемой такой процедуры.

Изображение 4: Покупка Linden Dollars через Second Life Viewer



Изображение 5: Покупка Linden Dollars через вэб-сайт Second Life



4.3.2 Облачные сервисы

Поскольку виртуальные валюты являются цифровым выражением стоимости, как уже обсуждалось в Модуле 1, нет причин полагать, что такое цифровое выражение обязательно должно храниться локально на компьютере подозреваемого. Подозреваемый может предпочесть онлайновый сервис хранения данных. Существует много различных способов, например:

- Использование облачного сервиса хранения данных, такого как DropBox или подобного ему.[90], [91], [92]
- Использование услуг электронной почты в сети Интернет.[93], [94]
- Использование любых форм Интернет-сервиса, предоставляющего возможности хранения записей или других данных.[95]

Найти доказательства использования подозреваемым таких услуг со своего компьютера возможно, если удастся выявить либо программное обеспечение, необходимое для использования облачных услуг, либо установив по истории просмотра вэб-страниц признаки, указывающие на использование онлайновых услуг. Доказательства можно подкрепить запросом о предоставлении информации, адресованный провайдеру услуг, используя соответствующие правовые возможности, например:

- Прямой контакт (посредством официального запроса) с сервис-провайдером, требуя от последнего раскрытия интересующей информации.
- Использование полицейских каналов, таких как контактные центры 24/7 (для государств-участниц Конвенции Совета Европы о компьютерных преступлениях) или G8 Сеть подразделений в сфере высокотехнологичных преступлений, или национальные бюро Интерпол, если ни один из первых двух каналов не может быть использован. Возможности и оперативность предоставления ответа полностью зависит от адресата такого запроса, но это будет все равно гораздо быстрее, чем использование официальных процедур взаимной правовой помощи.
- Процедура взаимной правовой помощи, осуществляемая Генеральной прокуратурой или Министерством юстиции. Оперативность является главной проблемой такой процедуры.

---

90 https://www.dropbox.com/
91 https://cloud.google.com/products/cloud-storage/
92 https://www.amazon.com/clouddrive/home/
93 https://www.gmail.com/intl/en/mail/help/about.html
94 https://login.yahoo.com/config/login_verify2?&.src=ym&.intl=us
95 http://evernote.com/

Пример: Наличие облачного программного приложения

DropBox представляет собой файл-хостинг, который предлагает услуги облачного хранения файлов с возможностью синхронизации общих файлов между несколькими устройствами. [96] Для использования DropBox на компьютер устанавливается клиентское приложение, обеспечивающее пользователю доступ к общим файлам.[97]

По окончанию установки DropBox в список «Избранного» добавляется ярлык к общей папке, как это показано на Изображение 6. Пользователь может просто перетащить файлы или папки со своего компьютера в общую папку, синхронизируя, таким образом, их с DropBox.

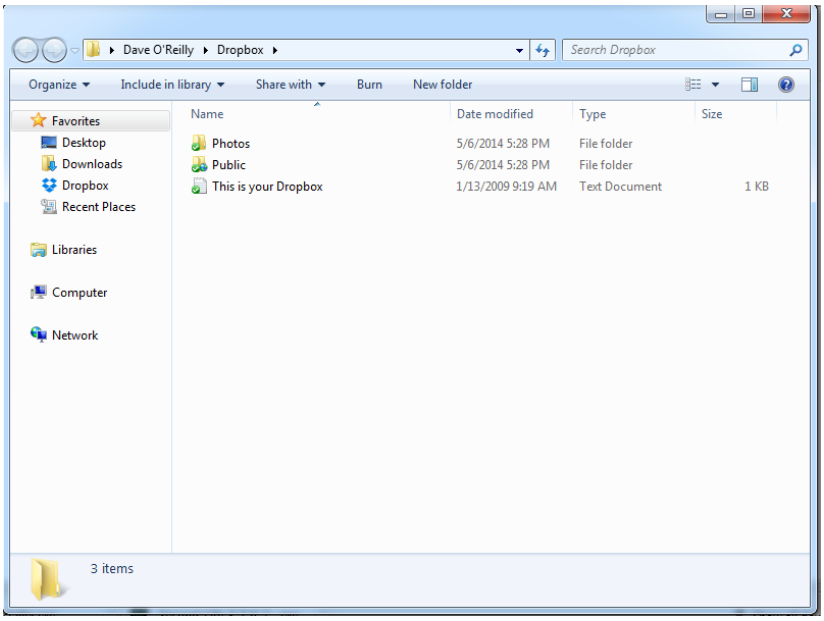
С помощью DropBox можно получить доступ к общим файлам, используя различные способы, в том числе через вэб-браузер, как показано на Изображение 7.

Что касается виртуальных валют, то и учетные данные, и цифровое выражение стоимости может храниться в текстовом или любом другом формате (электронные таблицы Excel, документы Word и пр.) в Dropbox. Доступ к данным может осуществляться непосредственно с компьютера или удаленно с помощью мобильных устройств или через вэб-браузер.

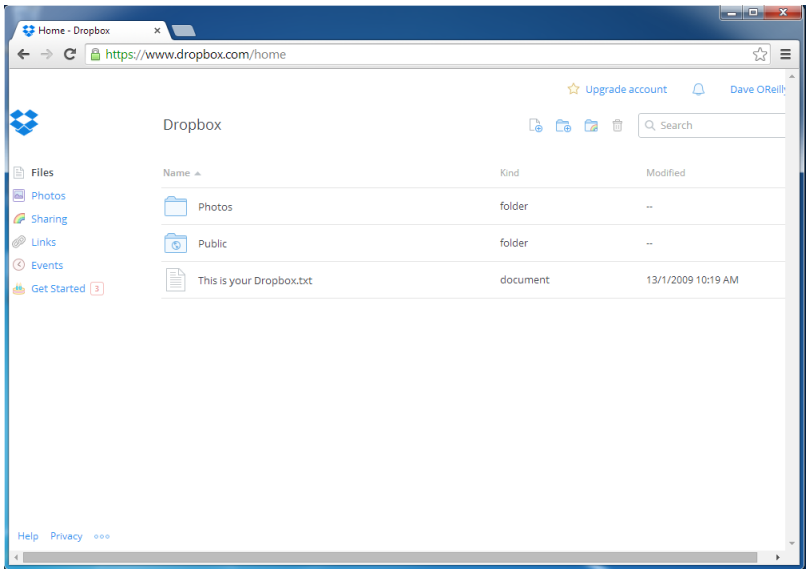
[96] https://www.dropbox.com/

[97] Для данного примера использовалась версия DropBox 2.6.31 на базе Windows 7 Professional 64-bit.

Изображение 6: Dropbox добавлен в «Избранное»



Изображение 7: Веб-интерфейс Dropbox



4.3.3 Исследование сети

Получив и проанализировав данные сетевого (входящего и исходящего) трафика компьютера подозреваемого, можно найти данные, указывающие на использование виртуальных валют. В частности, можно определить:

- Связь с распределенной приринговой сетью виртуальной валюты.
- Связь компьютера, подозреваемого с администратором или обменником (биржей) виртуальных валют.
- Использование облачных сервисов, как описано в подглаве 4.3.2.

Соответствующим специалистам предстоит провести анализ сети, во время которого они могут столкнуться с целым рядом трудностей, способных осложнить сбор доказательств.

Во-первых, канал связи между компьютером подозреваемого и компьютером, с которым он находится в контакте, скорее всего, будет зашифрован. Это практически не вызывает сомнений применительно к рассматриваемым в данном пособии случаям, связанных с проведением финансовых операций. Однако, проблема состоит в том, что с помощью анализа сетевого трафика невозможно узнать содержание имевшей место коммуникации. Тем не менее, даже если канал связи шифруется, существует возможность установить факт связи между двумя конкретными IP-адресами, например, между IP-адресом компьютера подозреваемого и IP адресом, связанным с обменником виртуальной валюты.

Во-вторых, существуют онлайновые возможности, позволяющие пользователям скрывать тот факт, что они учувствуют в коммуникации. Речь идет о специальных прокси-программах, позволяющих установить анонимное сетевое соединение. Их существует несколько видов, из которых самая известная – это, пожалуй, Tor, ранее известная как «The Onion Router»[98]. Tor осуществляет шифрование и передачу трафика через серию промежуточных узлов. Трафик, проходящий через систему Tor, представляется другим серверам в сети Интернет как таковой, который будто бы берет начало из какой-то условной точки, а не из истинного источника (то есть, компьютера, подозреваемого). Отследить трафик и выйти на истинный источник чрезвычайно трудно, если не невозможно.

Другой альтернативой является использование онлайновых прокси-программ, позволяющих скрыть личность пользователя.[99] Они работают следующим образом: пользователь входит на вэб-сайт, который они хочет посетить, через вэб-сайт скрывающих личность пользователя прокси, а не

[98] https://www.torproject.org/
[99] http://www.hidemyass.com/

через браузер. Если известно, что используются такие сервисы, то можно установить личность истинного источника трафика [100], например, посредством:

- Обращения непосредственно к прокси-сервису с официальным запросом о предоставлении необходимой информации, если Условия предоставления услуг или Политика конфиденциальности прямо не запрещают этого;[101]
- Использования полицейских каналов, таких как контактные центры 24/7 (для государств-участниц Конвенции Совета Европы о компьютерных преступлениях) или G8 Сеть подразделений в сфере высокотехнологичных преступлений, или национальные бюро Интерпол, если ни один из первых двух каналов не может быть использован. Возможности и оперативность предоставления ответа полностью зависит от адресата такого запроса, но это будет все равно гораздо быстрее, чем использование официальных процедур взаимной правовой помощи;
- Процедура взаимной правовой помощи, осуществляемая Генеральной прокуратурой или Министерством юстиции. Оперативность является главной проблемой такой процедуры.

4.4 Взаимодействие с администраторами / биржами виртуальных валют

Используя процессуальные полномочия и следственные инструменты, рассмотренные в предыдущих главах данного модуля, правоохранительным органам необходимо устанавливать и развивать сотрудничество с администраторами централизованных виртуальных валют по примеру сотрудничества государственных органов с представителями частного сектора для целей расследования киберпреступлений. Более подробно такое государственно-частное сотрудничество рассматривается в главе 5.7.

Прежде всего, необходимо попытаться установить прямой контакт с администратором виртуальной валюты на основе Условий предоставления услуг или Правил конфиденциальности, которые часто содержат положения о сотрудничестве с правоохранительными органами, оговорки в отношении гарантий конфиденциальности и/ или сохранения определенных данных (о счетах, операциях и пр.) в течение определенного промежутка времени. Юридические отделы администраторов виртуальных валют могут быть готовы напрямую сотрудничать с иностранными правоохранительными органами, если не существует специальных положений, запрещающих подобную практику.

---

[100] Например, http://www.theinquirer.net/inquirer/news/2112002/hidemyass-hide-ass
[101] http://hidemyass.com/legal/privacy/

Являясь юридическими лицами в своих национальных юрисдикциях, центральные администраторы виртуальных валют, так или иначе, будут обязаны сотрудничать с местными правоохранительными органами при расследовании уголовных преступлений. Именно по этой причине международное сотрудничество между органами полиции является предпочтительным решением во многих случаях, когда прямое неформальное сотрудничество маловероятно или потребует слишком много времени. Вопросы сотрудничества органов полиции уже многократно подымались в данном пособии, при этом обращая особое внимание на возможности, предоставляемые контактными центрами 24/7 (для государств-участниц Конвенции Совета Европы о компьютерных преступлениях), G8 Сетью подразделений в сфере высокотехнологичных преступлений или национальными бюро Интерпол, которые имеют право предпринимать конкретные действия от имени иностранных правоохранительных органов, как например, осуществлять меры по неотложному сохранению компьютерных данных или другие следственные действия, разрешенные в рамках двусторонних соглашений.

Взаимная правовая помощь (ВПП) представляет собой наиболее формализованную процедуру, основанную на традиционных процедурах сотрудничества по уголовным делам в рамках двусторонних или многосторонних договоров. Запросы об оказании взаимной правовой в отношении центральных администраторов и следственных действий, которые необходимо предпринять, должны направляться через центральные органы по вопросам ВПП, а это чаще всего главные (Генеральные) прокуратуры или Министерства юстиции.

Подход к обменникам (биржам) централизованных или децентрализованных виртуальных валют не будет отличаться от подхода в отношении центральных администраторов. Даже если такие учреждения включены в традиционные финансовые системы стран, услуги по обмену виртуальных валют не регулируются действующими нормами финансового законодательства. Поэтому с точки зрения развития государственно-частного сотрудничества обменники виртуальных валют должны рассматриваться как обычные юридические лица в соответствующих юрисдикциях. И, таким образом, ордера на предоставление информации могут быть применены в отношении таких лиц либо же могут использоваться механизмы международного сотрудничества между органами полиции (где это разрешено) или, что всегда реально, использоваться процедура взаимной правовой помощи.

5 Контрмеры

Некоторые меры противодействия и хорошие практики уже рассматривались в предыдущих исследованиях, проведенных в рамках изучения проблематики виртуальных валют. Многие из контрмер, которые будут рассмотрены в этом разделе, рассматривались в контексте более широких вопросов киберпреступности, отмывания денег, финансирования терроризма, а также выявления, ареста и конфискации доходов от преступлений в сети Интернет. Тем не менее, эти контрмеры также применимы к виртуальным валютам, что и будет продемонстрировано в следующих ниже главах.

5.1 Имплементация Рекомендаций ФАТФ

Рекомендации ФАТФ устанавливает комплексную и последовательную структуру мер, которые используются для противодействия отмыванию денег и финансированию терроризма, а также финансированию распространения оружия массового уничтожения. [102] Многие из этих рекомендаций либо непосредственно применимы, либо могут интерпретироваться в контексте виртуальных валют.

Рекомендации ФАТФ являются международными стандартами, которые странам следует адаптировать к своим конкретным условиям. Рекомендации устанавливают необходимые меры, которые странам следует иметь для того, чтобы:

- определять риски, разрабатывать политику и осуществлять координацию внутри страны;
- преследовать отмывание денег, финансирование терроризма и финансирование распространения оружия массового уничтожения;
- применять превентивные меры для финансового сектора и других установленных секторов;
- устанавливать полномочия и ответственность компетентных органов (например, следственных, правоохранительных и надзорных органов) и иные институциональные меры;
- укреплять прозрачность и доступность информации о бенефициарной собственности юридических лиц и образований;
- обеспечивать международное сотрудничество.

[102] «Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения – Рекомендации ФАТФ», ФАТФ-ГАФИ, Февраль 2012. (Источник: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

Полный текст каждой рекомендации, их интерпретацию и другие важные ссылки можно найти в сборнике Рекомендаций ФАТФ.

5.2 Предоставление сообщений

Махинации и отмывание денег в сети Интернет часто предполагают использование большого количества мелких операций с умышленным или неумышленным участием денежных мулов. Такой прием представляет собой вызов для следствия, так как каждая отдельная транзакция очень незначительна и понимание следственными органами того, что такие незначительные операции могут быть частью большой преступной схемы, зачастую сравнительно слабое. Даже если подозрительные сделки будут установлены, анализ большого объема мелких операций и последующее расследование истинной природы преступной деятельности может быть крайне затрудненным.

Что касается виртуальных валют, отсутствие регулирования в отношении провайдеров услуг виртуальных валют означает, что обязательства по предоставлению сообщений о подозрительных операциях часто либо ограничены, либо вовсе отсутствуют. А в отношении децентрализованных виртуальных валют, не имеющих центральных администраторов, на которые возлагались бы такие обязательства, существуют значительные технические препятствия для установления формальной структуры предоставления сообщений о подозрительных операциях.

Несколько исследований характеризуют предоставление сообщений о подозрительных операциях или другие методы повышения осведомленности о преступных средствах и методах отмывания в качестве примера хорошей практики.[103], [104] К ним также относится сбор оперативных данных, позволяющих выявлять и расследовать преступления в сети Интернет.

Существуют многочисленные примеры сотрудничества для целей сбора и анализа информации, непосредственно относящейся к использованию Интернет-услуг с целью совершения преступлений, в том числе для отмывания денег. К ним относятся:

---

[103] Раздел 8 Комплексное исследование по киберпреступности, Управление ООН по наркотикам и преступности, Февраль 2013 (проект).

[104] Глава 4.1 «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», Международного проекта Совета Европы по борьбе с киберпреступностью и МАНИВЕЛ, Март 2012. (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

- Центр по сообщениям о преступлениях в сети Интернет (IC3) в США[105]
- MELANI в Швейцарии[106]
- Национальный центр по сообщениям о мошенничестве в Великобритании[107]

Эти инициативы позволяют аккумулировать в одном месте (ведомстве) сообщения от различных заинтересованных сторон, будь то представители общественности, бизнеса или жертвы преступлений в сети Интернет. Затем эти сообщения анализируются на предмет выявления однотипных моделей или установления другой оперативной информации, которая может быть полезной для проведения расследований.

Разведданные, которые можно получить посредством таких инициатив, по большому счету, могут быть полезными для выявления и расследования отмывания преступных средств в сети Интернет, в том числе совершенного с помощью виртуальных валют.

Пример, когда такие сообщения могут оказаться полезными, – когда известно, что счета подозреваемого в традиционных финансовых учреждениях используются для финансирования счетов в виртуальных валютах. В таких случаях знание того, какие счета в виртуальных валютах финансировались и на что эти виртуальные валюты расходовались, может помочь закрыть пробелы в знаниях о целях использования виртуальных валют.

5.3 Повышение осведомленности общественности

Существует много способов, с помощью которых преступники используют в преступных целях слабую осведомленность простых людей. Вот некоторые примеры:

- Фишинговые сайты/ электронные письма от якобы финансового учреждения, обманным путем побуждающие доверчивого клиента предоставить преступникам свои конфиденциальные банковские данные. В этом случае преступники используют недостаточную осведомленность людей о том, что банки таким образом не общаются со своими клиентами.
- Путем рассылки спам-сообщений, содержащих вредоносные программы, эксплуатируется недостаточная осведомленность клиентов, что они не должны открывать вложения от неизвестных им людей.

105 http://www.ic3.gov/
106 http://www.melani.admin.ch
107 http://www.actionfraud.org.uk/home

- Предложения работы и другие стимулы, привлекающие денежных мулов, эксплуатируют наивность потенциальных жертв возможностями по трудоустройству, которые слишком хороши, чтобы быть правдой.

В этих и других случаях эффективные программы по информированию общественности могут помочь в борьбе с такими криминальными техниками.

В случае виртуальных валют осведомленность об отсутствии защиты, в том числе об опасностях невозвратного характера операций с виртуальной валютой, будет иметь важное значение. Аналогичным образом можно бороться с деятельностью по вербовке денежных мулов для проведения операций с виртуальными валютами.

5.4 Гармонизированная законодательная база

Гармонизированное национальное законодательство, в которое имплементированы соответствующие международные инструменты, является важной контрмерой против многих форм преступности, в том числе преступлений в сети Интернет.[108, 109]

В этом контексте, учитывая трансграничную природу большинства виртуальных валют, важно понимать значение международного сотрудничества в расследованиях по отмыванию преступных доходов.

Гармонизованное законодательство важно по целому ряду причин. Оно, среди прочего, способствует проведению трансграничных расследований и, таким образом, является важной контрмерой против незаконного использования виртуальных валют.

Но прежде всего гармонизованное законодательство важно для международного сотрудничества, будь то сотрудничество между органами полиции или оказание взаимной правовой помощи, основывающееся на принципе обоюдного признания деяния уголовным преступлением. Этот принцип стремится обеспечить, чтобы содеянное было признано уголовным преступлением как в запрашивающей, так и в запрашиваемой

---

[108] Рекомендация 36, «Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения – Рекомендации ФАТФ», ФАТФ-ГАФИ, Февраль 2012. (Источник: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

[109] Глава 4.4 «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», Международного проекта Совета Европы по борьбе с киберпреступностью и МАНИВЕЛ, Март 2012. (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

юрисдикциях и является необходимым условием предоставления взаимной правовой помощи.

Во-вторых, гармонизованное законодательство способствует профилактике преступности. Криминализация преступных деяний в равной степени всеми юрисдикциях предотвращает появление «убежищ» для преступников. Такие опасения особенно справедливы в отношении незаконного использования виртуальных валют как для совершения киберпреступлений, так и для совершения отмывания денег, так как онлайновая среда является весьма благоприятной почвой для развития транснациональной преступности.

Наконец, гармонизованное законодательство является важным требованием организаций, борющихся как с отмыванием денег (например, FATF, MONEYVAL), так и с киберпреступлениями (например, Комитет Конвенции Совета Европы компьютерных преступлениях). Гармонизация имеет важное значение для дальнейшего развития законодательства в указанных сферах, что в долгосрочной перспективе позволит повысить эффективность национальных компетентных ведомств в вопросах предупреждения и борьбы с соответствующими преступлениями.

5.5 Специальные подразделения

5.5.1 Специальные подразделения по финансовым расследованиям

Под финансовыми расследованиями понимается исследование финансовых аспектов преступной деятельности, целью которых является выявление и документирование фактов движения денежных средств в ходе осуществления преступной деятельности. Финансовое расследование включает в себя сбор, сопоставление и анализ всей имеющейся информации в целях оказания содействия уголовному преследованию и лишения преступников их доходов и средств совершения преступления. Финансовое расследование может служить орудием выявления неизвестных ранее предикатных преступлений и позволяет выявить других причастных лиц и групп.[110]

В соответствии с ФАТФ Рекомендацией 30 должны быть определены уполномоченные правоохранительные органы, отвечающие за обеспечение должного расследования путем проведения финансового расследования по отмыванию денег, предикатным преступлениям и финансированию терроризма. Пояснительная записка к Рекомендации 30

[110] Параграфы 14 и 15, «Руководство по финансовым расследованиям: оперативные вопросы», ФАТФ/ОЭСР, Июнь 2012 (Источник: http://www.fatf-gafi.org/media/fatf/documents/reports/Operational Issues_Financial investigations Guidance.pdf)

требует «параллельного финансового расследования», означающего проведение финансового расследования наряду или в рамках (традиционного) уголовного расследования отмывания денег, финансирования терроризма и/или предикатного преступления (преступлений). Следователи правоохранительных органов при расследовании предикатных преступлений должны быть уполномочены параллельно проводить расследование связанных преступлений по отмыванию денег и финансирования терроризма либо иметь возможность передать дело в другой орган, который провел бы такие расследования.

Таким образом, возможны многочисленные модели организации специальных подразделений по вопросам финансовых расследований. При этом они могут и не быть правоохранительными органами *per se*. Как правило, центральная роль в проведении финансовых расследований отводится подразделению финансовой разведки (ПФР), которое служит национальным центром для сбора и анализа (а) сообщений о подозрительных операциях (сделках) и (б) иной информации, относящейся к отмыванию денег, предикатным преступлениям и финансированию терроризма, и для передачи результатов анализа в соответствующие компетентные органы.

Рекомендация 30 также предписывает использовать для проведения финансовых расследований многопрофильные группы, что является общепризнанной лучшей практикой[111]. Такие группы могут состоять из разного рода специалистов, включая следователей по финансовым преступлениям, финансовых аналитиков, специалистов по бухгалтерии, специалистов по информационным технологиям, прокурорских работников и специалистов по управлению активами. Эксперты могут быть прикомандированы или привлечены из других ведомств, таких как регулирующие органы, ПФР, налоговые ведомства, аудиторские агентства, генеральной прокуратуры, или даже привлечены из частного сектора. Более детальное рассмотрение межведомственных механизмов сотрудничества представлено в главе 5.6.

В случае с виртуальными валютами специальные подразделения по вопросам финансовых расследований могут опираться на опыт проведения расследований отмывания преступных доходов, совершенного более традиционными методами. Эти знания и опыт в сочетании со знаниями и опытом специальных подразделений по борьбе с киберпреступлениями (рассматриваются в следующей подглаве) могут предложить эффективное решение угроз, связанных с виртуальными валютами.

---

111 Отчет ФАТФ «Руководство по финансовым расследованиям: оперативные вопросы», ФАТФ/ОЭСР, Июнь 2012. (Источник: http://www.fatf-gafi.org/media/fatf/documents/reports/Operational Issues_Financial investigations Guidance.pdf)

5.5.2 Специальные подразделения по вопросам киберпреступлений

Специальные подразделения по вопросам киберпреступлений являются ключевым элементом в борьбе с киберпреступностью. В состав таких подразделений входят как спецподразделения правоохранительных органов, так и специализированные прокуроры [112].

Специальные подразделения по вопросам киберпреступлений могут различаться по типам и функциям, но, как правило, они все:

- Расследуют и/ или преследуют в судебном порядке преступления против компьютерных систем и данных.
- Расследуют и/ или преследуют в судебном порядке преступления, совершенные посредством компьютерных систем и данных.
- Проводят компьютерную криминалистическую экспертизу в отношении электронных доказательств.

В последние годы обозначилась тенденция к разделению функций по расследованию компьютерных и других связанных с применением технологий преступлений от функций по сбору и анализу электронных доказательств. Это обуславливается тем, что в ряде стран возникло огромное количество нерасследованных дел, требующих анализа электронных доказательств небольшим количеством следователей, ответственных за расследование киберпреступлений. Такое положение вещей привело к признанию того факта, что все большее количество любых видов преступлений включают в себя определенный элемент электронных доказательств и поэтому криминалистический анализ электронных доказательств в настоящее время все чаще становиться частью обязанностей основных структур по вопросам криминалистической экспертизы.

Функции специального подразделения по вопросам киберпреступлений зависят от законодательства, обеспечивающего правовую основу для деятельности такого подразделения, а также департамента, в состав которого оно входит, внутренней структуры ведомства и многих других факторов. В то же время наблюдаются некоторые общие закономерности.

---

[112] Глава 5 Комплексного исследования УНП ООН по киберпреступности; см. также «Специализированные подразделения по вопросам киберпреступлений – хорошая практика», подготовленное совместно Советом Европы и Европейским союзом, Глобальным проектом Совета Европы по киберпреступности - CyberCrime@IPA и и Целевой группой Европейского Союза по вопросам киберпреступности, Ноябрь 2011. (Источник: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf)

- это – подразделения, которые расследуют преступления, совершенные против компьютерных систем и данных или с помощью компьютерных данных и систем. Такие подразделения также могут иметь возможности по проведению компьютерной криминалистической экспертизы.
- это – подразделения, которые отвечают только за сбор и анализ электронных доказательств.
- это – подразделения, которые координируют розыскную деятельность или проводят сбор оперативных данных, но не имеют следственной функции.
- это – подразделения, уполномоченные расследовать конкретные преступления.

Расследования, связанные с использованием виртуальных валют, имеют много общего с расследованиями киберпреступлений. И поэтому технические знания следователей по вопросам киберпреступлений и экспертов по криминалистической экспертизе окажутся несомненно полезными для осуществления корректного сбора электронных доказательств.

5.6 Межведомственное сотрудничество между государственными органами

В зависимости от специфики в каждой конкретной стране ответственность за проведение финансовых расследований, криминалистической экспертизы, конфискации доходов, мер по борьбе с отмыванием денег, киберпреступностью и так далее может быть возложено на различные государственные органы и ведомства. Эффективное сотрудничество между этими учреждениями с целью выявления и расследования дел, связанных с отмыванием преступных доходов в сети Интернет, является важным условием успеха.

Для расследований преступлений посредством виртуальных валют, имеющих сходство как с расследованиями киберпреступлений, так и расследованиями отмывания преступных доходов в сети Интернет с использованием других методов и средств, межведомственное сотрудничество также будет иметь важное значение.

Механизмы такого межведомственного сотрудничества могут быть разделены на формальные или неформальные. Официальные договоренности как, например, меморандум о взаимопонимании, призваны повысить эффективности такого сотрудничества. В то же время не менее важны неформальные механизмы сотрудничества между ведомствами, которому, к сожалению, уделяется меньшее внимание и придается меньшее значение.

Ниже приведены некоторые примеры организации межведомственного сотрудничества, реализованного в некоторых странах:

- Создание на базе нескольких ведомств единого «мозгового центра» для выявления и анализа следственных вызовов.
- Привлечение представителей полиции к проведению проверок и анализу полученных результатов.
- Пересмотр используемых в работе подходов с учетом подходов, используемых полицией и надзорными органами.
- Создание единой информационной системы, позволяющей разным компетентным ведомствам иметь доступ к информации о прошлых или текущих расследованиях в отношении конкретного физического и/ или юридического лица. Это помогает избежать дублирования и содействует кооперации.
- Установление политик и процедур, способствующих обмену информацией / разведданными.
- Установление процедур, позволяющих решать спорные вопросы в интересах следствия.
- Подписание письменных соглашений, как, например, меморандума о взаимопонимании или подобного ему с целью формализации процессов сотрудничества.

Пример: Создание контактных центров по сообщениям о преступлениях

Рассмотрим в качестве примера формального сотрудничества создание контактного центра по сообщениям о преступлениях. Важность таких сообщений как контрмеры уже обсуждалась в главе 5.2.

Представители общественности часто не знают, куда и как сообщать о преступлениях. В то время как такие сообщения могут иметь важное значение для выявления масштабных преступлений в сети Интернет. Часто это происходит потому, что в соответствии с типологией отмывания денег, рассмотренной в Модуле 2 (когда осуществляется большое количество переводов на небольшие суммы через счета денежных мулов), сумма, связанная с каждым отдельно взятым преступлением, может быть незначительной.

После того, как о преступлениях становиться известно, можно определить закономерности преступной деятельности, которые невозможно было выявить другим способом. Эту информацию можно

направить в соответствующий правоохранительный орган для проведения расследования.

Несколько примеров такой модели взаимодействия существуют на практике.

Один из таких примеров – вэб-страница Департамента юстиции США, содержащая ссылки на соответствующие ведомства, которым необходимо адресовать сообщения о компьютерном взломе, мошенничестве и других видах Интернет-преступлений [113].

Другим таким примером является Центр по сообщениям о преступлениях в сети Интернет (IC3) [114], являющийся результатом партнерства между Федеральным бюро расследований (ФБР) и Национальный центром борьбы с должностными преступлениями (NW3C). Миссия IC3 заключается в том, чтобы получать, обрабатывать и передавать жалобы об Интернет-преступлениях, предоставляемые представителями общественности. IC3 является единым механизмом, обеспечивающим предоставление такой информации правоохранительным и регулирующим органам на федеральном, областном и местном уровнях.

Пример: Откомандирование сотрудников в ПФР

В *Корее* несколько ведомств командировали своих сотрудников в подразделение финансовой разведки. В обязанности таких командированных сотрудников входило проведение анализа отчетов о подозрительных сделках, относящихся к сфере их специализации, а также выявление вопросов, которые должны были быть расследованы правоохранительными органами. В 2012 году было командировано девять сотрудников из органов прокуратуры, восемь сотрудников из органов полиции, семи сотрудников из налоговой администрации, семь сотрудников из таможенной администрации, один сотрудник из Службы финансового надзора и один сотрудник из Банка Кореи. В период их командирования в подразделение финансовой разведки указанные сотрудники не имели прямого доступа к информации, которая находилась в распоряжении командировавших их ведомств, но должны были получать информацию через обычный интерфейс подразделения финансовой разведки.

113 http://www.justice.gov/criminal/cybercrime/reporting.html
114 http://www.ic3.gov/default.aspx

Налоговая администрация *Испании* также командировала шесть своих сотрудников в подразделение финансовой разведки, чтобы помочь в проведении анализа Отчетов о подозрительных сделках. Как и в Корее, командированные сотрудники в Испании могли обмениваться своими навыками и опытом, но не имели доступа к налоговой информации, которую, в случае необходимости, они могли получить, используя обычные каналы подразделения финансовой разведки через уполномоченных лиц в налоговой администрации.

Налоговая администрация *Голландии* командировала ряд своих сотрудников на работу в подразделение финансовой разведки в качестве контактных лиц. Указанные сотрудники работали вместе с персоналом подразделения финансовой разведки над анализом отчетов о необычных сделках, но для этого у них был прямой доступ к базам данных налоговой администрации.

В *Греции* сотрудники были командированы в подразделение финансовой разведки из каждого ведомства, представленного в Совете подразделения финансовой разведки. Эти обученные и опытные специалисты проводили анализ отчетов о подозрительных сделках, имея доступ к базам данных соответствующих ведомств.

Налоговая и таможенная администрации *Португалии* командировали своих сотрудников в группу по взаимодействию в рамках подразделения финансовой разведки.

В *США* все крупные федеральные ведомства, включая налоговую администрацию, командировали своих сотрудников в подразделение финансовой разведки, чтобы они выполняли роль контактных лиц, содействующих процессу обмена информацией, типологиями и тенденциям.

Налоговая администрация *Великобритании* командировала небольшую группу сотрудников в подразделение финансовой разведки в середине 1990-х, чтобы в полном объеме использовать данные отчетов о подозрительных сделках в процессе налогового администрирования, правоприменения и выполнения иных функций.

В *Бельгии* три сотрудника органов полиции работали в подразделении финансовой разведки в качестве контактных лиц.

В *Финляндии* Служба по возврату активов функционирует в рамках подразделения финансовой разведки. Служба по возврату активов в основном состоит из сотрудников финской полиции, но также включает в себя одного сотрудника из налоговой администрации и одного сотрудника из Службы судебных приставов. В дополнение к этому в Финляндии было создано 17 межведомственных региональных групп

для отслеживания доходов, полученных преступным путем, состоящих из 38 сотрудников полиции, 20 сотрудников налоговой администрации и 19 сотрудников Службы судебных приставов.[115]

Пример: Межведомственное сотрудничество на национальном уровне

Центр финансовой экспертизы (FEC) *Голландии* является совместным проектом регуляторных, следственных, разведывательных органов и органов прокуратуры, причастных к регулированию или надзору в финансовом секторе. Партнерами-участниками в FEC являются Национальная налогово-таможенная администрация, Служба фискальной разведки и расследований (FIOD, структурно входящий в NTCA), Национальная полиция, Генеральная Служба информации и безопасности, прокуратура, Служба финансовых рынков Голландии и Национальный банк Голландии, при участии Министерства финансов и Министерства безопасности и правосудия, участвующих в качестве наблюдателей. Миссия FEC – мониторинг и обеспечение целостности финансового сектора посредством межведомственного взаимодействия и сотрудничества. Это предполагает обмен информацией и создание единого центра знаний, который функционирует в интересах участвующих ведомств и аккумулирует знания и опыт, необходимые для сохранения целостности финансового сектора. В фокусе внимания FEC – риски, связанные с отмыванием денег, имущественным мошенничеством, мошенничеством с личными данными, включая скимминг, ипотечным мошенничеством, инвестиционным мошенничеством и киберпреступлениями, включая фишинг-атаки.[116]

[115] Стр. 72 «Эффективное межведомственное сотрудничество в борьбе с налоговыми и другими финансовыми преступлениями», ОЭСР, Второй Ежегодный Форум по Налогам и Преступлениям, Июнь 2012.

[116] Стр. 25 of «Эффективное межведомственное сотрудничество в борьбе с налоговыми и другими финансовыми преступлениями», ОЭСР, Издание Второе, 2013.

Пример: Международная координация и анализ

В 2013 году официально начал свою деятельность Европейский центр борьбы с киберпреступностью (EC3) на базе Европол [117]. Он призван действовать в качестве координационного центра в борьбе европейского сообщества против киберпреступности, способствуя более быстрому реагированию в случае совершения онлайновых преступлений. EC3 содействует государствам-участникам и институтам Европейского Союза в развитии оперативного и аналитического потенциала для проведения расследований и развития сотрудничества с международными партнерами.

Миссия EC3 – эффективное противодействие кибепреступлениям, которые:

- совершаются организованными группами с целью получения больших преступных доходов, например, Интернет-мошенничество.
- причиняют серьезный вред жертве, как, например, сексуальная эксплуатация детей, транслирующаяся онлайн.
- оказывают критическое влияние на информационные инфраструктуру и системы Европейского Союза.

Расследование онлайновых преступлений часто может касаться в одном единственном случае сразу сотен жертв и подозреваемых в различных частях мира. Это требует от правоохранительных органов использование согласованного подхода, который бы мог обеспечить трансграничное сотрудничество с государственными и частными заинтересованными сторонами:

- государствами-участницами ЕС
- основными партнерами ЕС
- странами, не входящих в ЕС
- международными организациями
- управляющими компаниями и провайдерами услуг Интернет
- компаниями, занимающиеся вопросами Интернет-безопасности и безопасности финансового сектора
- научными кругами
- общественными организациями

[117] https://www.europol.europa.eu/ec3

- центрами по реагированию на инциденты в области компьютерной безопасности (CSIRTs)[118] , а также CERT-EU.

5.7 Сотрудничество государственных органов с частным сектором и обмен информацией

Государственно-частное сотрудничество и обмен информацией является, возможно, наиболее эффективной мерой по профилактике и борьбе с криминальными потоками денег в сети Интернет. Такое сотрудничество призвано решить проблему недостаточного использования информации, находящейся в распоряжении национальных финансовых учреждений и правоохранительных органов. Существуют также определенные вопросы в контексте государственно-частного сотрудничества и обмена информацией, когда частные организации являются международными провайдерами услуг.

Есть много примеров государственно-частного сотрудничества и обмена информацией, многие их которых касаются сотрудничества и обмена информацией на национальном уровне.[119] Но государственно-частное сотрудничество может рассматриваться и гораздо шире.

В первую очередь, нужно понимать, что подразумевается под понятиями «государственное», «частное» и «сотрудничество».

Есть много различных компонентов в системе государственной службы, которые могут быть заинтересованы в сотрудничестве с частным сектором. Например, правоохранительные органы, органы прокуратуры, суды, финансовые регуляторы, надзорные органы, ПФР, другие контролирующие органы, таможенные чиновники, военные учреждения, спецслужбы и так далее. Характер и степень взаимодействия, а также предъявляемые к нему формальные требования будут зависеть от типа государственного органа, заинтересованного в таком сотрудничестве.

Точно так же есть много организаций частного сектора, в сотрудничестве с которыми государственные органы могут быть заинтересованы, в

---

[118] CSIRTs (Центры по реагированию на инциденты в области компьютерной безопасности) – это специализированные группы экспертов, играющие ключевую роль в обеспечении защиты национальных информационных систем и данных, деятельность которых в основном сосредоточена на предупреждении, управлении и минимизации последствий инцидентов в сфере кибернетической безопасности.

[119] Глава 4.7 «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками», Международного проекта Совета Европы по борьбе с киберпреступностью и МАНИВЕЛ, Март 2012. (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf)

частности, в контексте борьбы с киберпреступностью и использованием виртуальных валют в незаконных целях. В широком смысле они могут быть разделены на две категории: национальные компании и международные корпорации. Учитывая международную природу Интернета, киберпреступности и преступлений по отмыванию доходов в сети Интернет, международные корпорации могут оказаться источниками информации, имеющие критическое значение для расследования отмывания преступных средств. Примерами таких организаций могут быть облачные сервисы и другие провайдеры Интернет-услуг (Microsoft, Amazon, Yahoo!, Facebook, Skype, Google и пр.), провайдеры услуг Интернет-платежей (PayPal и пр.), международные финансовые организации (Visa, Mastercard, Amex и пр.).

В национальном контексте также существуют частные организации, которые могут предложить важную для расследования информацию. Типичными примерами этой категории являются финансовые учреждения, провайдеры телекоммуникационных и Интернет-услуг.

Характер сотрудничества также будет зависеть от сторон, намеревающихся сотрудничать. Как правило, такое сотрудничество предполагает оказание оперативной поддержки, обмен техническими знаниями и оперативными данными, предоставление сообщений и оказание помощи в проведении расследований.

Для того, чтобы государственно-частное сотрудничество было эффективным, должно наличествовать убедительный стимул для всех заинтересованных сторон. Для государственных органов таким стимулом может быть увеличение количества успешно завершенных гражданских и уголовных дел или же расширение возможностей по сбору оперативных данных. Для организаций частного сектора стимулом к сотрудничеству с государственными органами может быть уменьшение количества случаев мошенничества, распределение нагрузки по вопросу предотвращения мошенничества на отраслевом уровне, защита бренда и корпоративная ответственность.

Пример: Взаимодействие с финансовыми учреждениями

Ирландская Банковская Федерация (IBF) является представительским органом для всех финансовых учреждений Ирландии. IBF учредила Форум по вопросам высокотехнологичных преступлений в качестве национальной инициативы государственно-частного сотрудничества с целью устранения угроз, которые представляют собой розничному банковскому сектору компьютерные и высокотехнологичные преступления. Форум по вопросам высокотехнологичных преступлений собирается четыре раза в год для обмена информацией, обсуждения текущих и возникающих угроз, определения проектов, которые будут осуществляться на уровне отрасли и выделения ассигнований на проведение исследований и других инициатив.

Членами Форума являются представители:

- всех розничных банков Ирландии, предоставляющие онлайновые услуги.
- правоохранительных органов по вопросам киберпреступности
- правоохранительных органов по вопросам мошенничества с кредитными картами
- Ирландской Ассоциации Интернет-провайдеров (ISPAI)
- Ирландской Организации платежных услуг (IPSO)
- научных кругов (Центр по расследованиям киберпреступлений (CCI) Университетского Колледжа Дублина (USD))

В рамках Форума было реализовано ряд успешных инициатив, некоторые из которых кратко изложены ниже:

- *Обмен информацией*:
  - каждый банк сообщает о количестве и видах киберпреступлений, зафиксированных ним с момента последней встречи.
  - Интернет-провайдеры предоставляют информацию о наблюдаемых ними угрозах, тенденциях и других схожих инцидентах.
  - организации, предоставляющие платежные услуги, делятся информацией о преступлениях с платежными картами.
  - правоохранительные органы информируют о новых международных тенденциях в данной области.

- *Центра по сообщению и реагированию на инциденты*: Члены Форума по вопросам высокотехнологичных преступлений отмечали, что это было очень трудно получить доступ к точной информации о масштабах угроз киберпреступлений, с которыми сталкиваются финансовые учреждения в Ирландии. Члены Форума инициировали проект по изучению данного вопроса и, основываясь на выводах проекта, договорились совместно инвестировать в создание инфраструктуры, куда бы анонимно передавались данные об инцидентах в сфере киберпреступности. Эта информация собирается и обрабатывается, чтобы предоставить членам Форума данные об установленных тенденциях, а также точную статистику о количестве и размере инцидентов, включая понесенные убытки.
- *Моделирование инцидентов:* Члены Форума договорились провести несколько тренингов по имитации крупных инцидентов сфере киберпреступности. Целью этих упражнений было изучение эффективности внутренних процедур по реагированию финансовых учреждений на такие инциденты, а также определения потребностей по обеспечению наиболее эффективной координации на отраслевом уровне, если в ней возникнет необходимость.
- *Оперативная поддержка:* Форум по вопросам высокотехнологичных преступлений оказывал экспертную поддержку отдельным финансовым учреждениям и правоохранительным органам в технически сложных случаях.[120]

Пример: Сотрудничество с Интернет-провайдерами

В январе 2010 года ведущие грузинские Интернет-провайдеры, представляющие абсолютное большинство на телекоммуникационном рынке, заключили с Министерством внутренних дел «Меморандум о взаимопонимании между правоохранительными органами и Интернет-провайдерами, основанный на принципах сотрудничества в области борьбы с киберпреступностью». Документ стал результатом годичных переговоров между Интернет-индустрией и Правительством Грузии в рамках проекта по борьбе с киберпреступностью, реализуемого Советом Европы. Выполнение Меморандума обеспечивается

[120] «Банки объединяются в борьбе с высокотехнологичными преступлениями», Silicon Republic, Август 2006. (Источник: http://www.siliconrepublic.com/business/item/6595-banks-band-together-to-tack)

Национальной комиссией по коммуникациям Грузии, являющейся официальным регистратором соглашения.

Заключению Меморандума предшествовали дискуссии между сторонами о необходимости внесения изменений в законодательство, в том числе касательно обеспечения сохранности компьютерных данных, а также изменений в Закон об электронных коммуникациях, в результате которых принцип абсолютной конфиденциальности абонента был упразднен.

Меморандум признает необходимость обеспечения баланса конфиденциальности пользователей и угроз информационной безопасности, в также неизбежности сотрудничества для достижения такого баланса. Интернет-провайдеры считаются партнерами в области борьбы с киберпреступностью на ровне с правоохранительными органами.

Меморандум устанавливает ряд важных принципов сотрудничества, таких как:

- Принцип минимального вмешательства, означающий, что любая деятельность в рамках сотрудничества должна оказывать минимальное влияние на качество Интернет-услуг и приводила бы к перебоями в предоставлении Интернет-услуг только в исключительных случаях.
- С целью укрепления сотрудничества определялись контактные центры, доступные в режиме 24/7, как со стороны правоохранительных органов, так и со стороны провайдеров Интернет-услуг.
- Регулярный обмен информацией и опытом (в основном, на базе ежегодного Форума по кибербезопасности).
- Сотрудничество осуществляется только посредством письменных запросов.
- Все стороны признают и уважают конфиденциальность такого сотрудничества.
- Разумное время для предоставления ответов на запросы. На практике редко превышает 3 дней.
- Если запрашиваемая информация не может быть предоставлена Интернет-провайдером, правоохранительным органам представляются письменные объяснения с изложением соответствующих причин.[121]

[121] С текстом Меморандума можно ознакомиться на веб-сайте Совета Европы: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy project balkan/June 11_Duress_Cooperation_LEA_ISP/2215_MoU_Cooperation LEA-ISP_eng.pdf.

Меморандум о взаимопонимании является юридически обязательным документом, который активно применяется в контексте расследований киберпреступлений.

5.8 Обучение

Обучение и повышение осведомленности необходимо на всех уровнях в рамках системы уголовного правосудия, в том числе для правоохранительных органов, прокуроров и судей. Различные проекты, в том числе и это учебное пособие, имплементируются с целью обеспечения и укрепления необходимой учебно-материальной базы для организации обучения и повышения уровня осведомленности.

Одними из главных проблем в этой связи являются отсутствие опытных практиков, которые могли бы выступать в качестве тренеров, а также интеграция необходимой подготовки любо в рамки первичного обучения, либо в обучение по месту работы соответствующих специалистов.

Пример: Обмен знаниями

В *Австрии* проводятся регулярные встречи и обучающие семинары с участием сотрудников различных ведомств, что позволяет сотрудникам устанавливать и поддерживать личные контакты. Такие встречи и семинары также доказали свою актуальность в повышении эффективности совместной работы и обмена информацией. Межведомственные встречи по обмену стратегической информацией о тенденциях в сфере финансовой преступности, методологическим принципам проведения расследований и передовой практике ведения дел, а также межведомственные обучающие семинары и конференции аналогичным образом проводятся в Чехии, Люксембурге, Голландии, Новой Зеландии и Словакии.[122]

[122] Стр. 74 «Эффективное межведомственное сотрудничество в борьбе с налоговыми и другими финансовыми преступлениями», ОЭСР, Второй Ежегодный Форум по Налогам и Преступлениям, Июнь 2012.

Пример: Обучение вопросам борьбы с киберпреступностью

В 2007 году в Европоле была создана Европейская Группа по вопросам обучения и образования в сфере борьбы с киберпреступностью[123], призванная обеспечить координацию инициатив по обучению вопросам киберпреступности и администрирование учебного материала, который был разработан в рамках ряда европейских проектов. Целями Группы являются:

- Поддержка международных мероприятий, направленных на гармонизацию подготовки в сфере борьбы с киберпреступлениями в глобальном масштабе.
- Обмен знаниями, опытом и поиск образовательных решений выявленных проблем.
- Содействие стандартизации методов и процедур учебных программ и сотрудничеству с другими международными организациями.
- Сотрудничество с научными кругами по учреждению признанной научной квалификации в области проблем киберпреступности и сотрудничество с университетами, которые уже учредили подобные звания, способствуя, таким образом, распространению этого процесса в международном масштабе.
- Сотрудничество с отраслевыми партнерами по созданию механизма поддержки правоохранительных органов в вопросах обучения, проводящегося в рамках единой гармонизированной программы, которая бы обеспечила наиболее эффективное использование имеющихся ресурсов.
- Оказание содействия международным партнерам путем предоставления им учебных материалов и тренеров с целью поддержки их усилий по подготовке сотрудников правоохранительных органов в сфере борьбы с киберпреступностью глобально.

Было подготовлено большое количество технических курсов исключительно для использования правоохранительными органами:

- Linux как следственный инструмент (часть 1)
- Linux как следственный инструмент (часть 2)
- Криминалистическая экспертиза NTFS

123 http://www.ecteg.eu/index.html

- Основные навыки криминалистической экспертизы мобильных телефонов
- Расследования в сети Интернет
- Сетевые расследования
- Анализ и проведение расследований вредоносных программ
- Программирование для целей криминалистической экспертизы с использованием BASH
- Вступительный курс по криминалистической экспертизе информационных технологий с открытым исходным кодом и курс по сетевым расследованиям
- Криминалистическая экспертиза текущих данных
- Курс по криминалистической экспертизе Macintosh
- Сетевые расследования (курс средней сложности)
- Курс по криминалистической экспертизе твердотельных накопителей и других средств хранения данных
- Криминалистическая экспертиза Vista и Windows 7
- Добыча данных и базы данных
- Криминалистическая экспертиза мобильных телефонов (курс средней сложности)

Вопросы для самооценки

Вопрос 1: Опишите с точки зрения материального уголовного права взаимосвязи между отмыванием денег и киберпреступлениями в случаях, когда используются виртуальные валюты.

Вопрос 2: Приведите пример преступления по незаконному доступу в контексте виртуальных валют?

Вопрос 3: Опишите, как использование позволяющих скрывать личность онлайновых (прокси) программ может быть представлено в качестве элемента преступления по вмешательству в данные на примере, когда речь идет о вмешательстве в персональные данные пользователей виртуальных валют.

Вопрос 4: Объясните, как использование децентрализованных виртуальных валют может быть использовано, чтобы доказать элемент «расслоения» преступления по отмыванию денег?

Вопрос 5: Объясните возможные взаимосвязи между компьютерным мошенничеством и отмыванием денег посредством виртуальных валют.

Вопрос 6: Какие данные, которыми располагает CSIRT, могут быть использованы для финансовых расследований по отмыванию денег, совершенных посредством виртуальных валют?

Вопрос 7: Какова правовая основа и требования, предъявляемые к перехвату данных контента, в делах, связанных с использованием виртуальных валют?

Вопрос 8: Объясните процедурные различия (с точки зрения законодательства и практики) между оперативным обеспечением сохранности компьютерных данных и обыском, и изъятием компьютерных данных.

Вопрос 9: Назовите, как минимум, три элемента обеспечения последовательности электронных доказательств.

Вопрос 10: Назовите национальные ведомства, чей экспертный потенциал может быть полезен в расследованиях, связанных с виртуальными валютами.

Вопрос 11: Опишите следственные индикаторы, которые могут указывать на использование виртуальных валют для отмывания преступных доходов.

Вопрос 12: Расскажите о видах доказательств, которые могут быть собраны с помощью криминалистической экспертизы компьютера подозреваемого и которые могут свидетельствовать об отмывании

преступных доходов посредством виртуальных валют. В качестве примера используйте Bitcoin-кошелек.

Вопрос 13: Расскажите, какую информацию можно получить от центрального администратора виртуальной валюты и/ или биржи виртуальных валют, а также о возможных способах получения такой информации.

Вопрос 14: Расскажите, как государственно-частное партнерство может стать эффективной контрмерой в отношении отмывания преступных доходов посредством виртуальных валют. Аргументируя свой ответ, используйте примеры.

Вопрос 15: Расскажите, как межведомственное сотрудничество государственных органов может стать эффективной контрмерой в отношении отмывания преступных доходов посредством виртуальных валют. Аргументируя свой ответ, используйте примеры.

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Модуль 4
Арест виртуальных валют

1 Краткое изложение

В этом модуле рассматриваются правовые требования, процедуры, инструменты и способы ареста виртуальных валют.

2 Цели обучения

По окончанию данного модуля Вы будете знать о:

- правовых и институциональных основах, необходимых для осуществления ареста виртуальных валют как доходов или инструментов преступлений на национальном и международном уровнях.

- ведомствах, имеющих отношение к аресту активов в делах, связанных с виртуальными валютами, как на национальном, так и международном уровнях, а также об их процессуальных полномочиях и компетенции.

- способах ареста виртуальных валют и некоторых вопросах, связанных с их предполагаемой конфискацией.

3 Вступление

В отличие от предыдущих частей данного пособия, в которых изучались различные аспекты использования виртуальных валют для отмывания денег и совершения компьютерных преступлений, а также рассматривались возможные решения в борьбе с преступлениями, совершенных посредством виртуальных валют, в рамках традиционной системы уголовного правосудия, другими словами, для расследования и уголовного преследования за соответствующие преступления, этот раздел пособия фокусируется на рассмотрении практических возможностей ареста доходов и орудий таких преступлений с целью их последующей конфискации в пользу государства.

Арест доходов или орудий преступлений означает применение процедур, которые запрещают передачу, преобразование, отчуждение или передвижение имущества, полученного преступным путем, и позволяющие компетентному органу или суду осуществлять контроль в отношении соответствующего имущества. [1] Арест преступных доходов и орудий преступлений является эффективным средством, в равной степени полезным для профилактики (препятствование использованию имущества в незаконных целях), расследования (имущество находится под контролем и не может быть перемещено или преобразовано в другое имущество) и отправления правосудия (косвенная компенсация усилий по борьбе с организованной преступностью [2] и общее сдерживающее воздействие на организованную преступность). Арест доходов/ орудий преступлений может быть также эффективным и при расследовании преступлений, связанных с отмыванием денежных средств посредством виртуальных валют, органично объединяя в себе все три элемента – профилактику, расследование и отправление правосудия.

Арест, замораживание или конфискация доходов или орудий преступлений являются сложными процедурами и с точки зрения права, и с точки зрения их практической реализации. Вполне естественно, что применение этих процедур к виртуальным валютам делают их еще более сложными, учитывая особенности таких валют (анонимность, сложность отслеживания и трансграничная природа транзакций – лишь часть примеров, детально рассмотренных в данном пособии). Поэтому, изучая вопросы ареста доходов или орудий преступлений, совершенных с помощью виртуальных валют, в этом модуле будут рассматриваться только те доходы или орудия, которые являются централизованными или децентрализованными виртуальными валютами. К примеру, особенности

[1] Группа разработки финансовых мер борьбы с отмыванием денег, Глоссарий Рекомендаций ФАТФ (Источник: http://www.fatf-gafi.org/pages/glossary/s-t/).
[2] ФАТФ Рекомендация 38.

ареста вредоносного ПО, использованного для взлома Bitcoin-кошельков отдельных пользователей, рассматриваться не будут.

Не в последнюю очередь обращаем внимание на то, что данный модуль не предназначен для использования в качестве пошагового руководства по конфискации доходов от преступлений, совершенных посредством виртуальных валют, или конфискации последних как орудий преступлений, а нацелен на рассмотрение исключительно вопросов ареста таких активов. На самом деле можно утверждать, что после осуществления ареста конфискация виртуальной валюты или ее относительной стоимости мало чем будет отличаться от конфискации других форм собственности, особенно денежно-кредитных инструментов. Поэтому в качестве практического пособия по конфискации уже арестованных активов или их стоимости рекомендуем использовать соответствующие разделы Руководства по международному сотрудничеству в целях конфискации доходов, полученных преступным путем, опубликованные Управлением Организации Объединенных Наций по наркотикам и преступности в 2012 году[3].

4 Терминология

Арест доходов или орудий преступлений может определяться как запрещение передачи, преобразования, отчуждения или передвижения имущества по решению компетентного органа или суда в рамках механизма «замораживания». Но в отличие от «замораживания», означающего временное запрещение передачи, преобразования, отчуждения или передвижения имущества, [4] арест позволяет компетентному органу или суду **осуществлять контроль** в отношении такого имущества. Арестованное имущество остается собственностью физического или юридического лица (лиц), которые имеют долю в указанном имуществе на момент ареста, в то время как компетентный орган или суд имеют право на владение, администрирование или управление арестованным имуществом. [5]

Есть также еще несколько важных понятий, особенно актуальных в контексте ареста доходов, полученных преступным путем, а именно:

[3] https://www.unodc.org/documents/organized-crime/Publications/Confiscation_Manual_Ebook_E.pdf.

[4] УНП ООН, «Руководство по международному сотрудничеству в целях конфискации доходов, полученных преступным путем», стр. 2.

[5] Группа разработки финансовых мер борьбы с отмыванием денег, Глоссарий Рекомендаций ФАТФ (Источник: http://www.fatf-gafi.org/pages/glossary/s-t/).

- **«Доходы»** означают любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения какого-либо преступления. Доходы могут состоять из любого имущества, будь то материального или нематериального, движимого или недвижимого, выраженного в вещах или в правах, а также юридических документах или актах, подтверждающих право на такие активы или интерес в них; [6]
- **«Орудия»** означают любое имущество, использованное или предназначенное для использования любым способом, целиком или частично для совершения преступления или преступлений.[7]

Эти два понятия имеют непосредственное отношение к природе виртуальных валют, будь то централизованных или децентрализованных, в связи с их использованием в качестве средства электронного платежа. Виртуальные валюты, учитывая присущую анонимность транзакций с их использованием (более характерно для децентрализованных виртуальных валют), могут использоваться для сокрытия преступного происхождения денег, используемых для покупки/ обмена на такие валюты. А покупка bitcoin может еще и принести доходы в виде дополнительных bitcoin, полученных в процессе майнинга, или в результате увеличения стоимости самого bitcoin. [8] Таким образом, в ходе проведения расследований и судебных слушаний о преступлениях с использованием виртуальных валют, в особенности по отмыванию денег, будет достаточно сложным провести разграничительную линию между доходами и орудиями преступлений. Однако, с практической точки зрения, это не будет иметь существенного влияния на процедуры или способы ареста, так как, в сущности, они будут одинаковыми.

[6] Статья 1 (d, e) Конвенции Организации Объединенных Наций против транснациональной организованной преступности.
[7] Статья 1 (c) Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма
[8] http://www.coindesk.com/price/.

5 Юридические требования и процедуры

Выявление, замораживание/ арест и конфискация доходов от преступлений являются юридическими процедурами, которые все чаще признаются в качестве особо эффективных мер в борьбе с организованной преступностью. Применение любой из этих процедур потребует твердых правовых оснований. Главная задача данного раздела – дать краткий обзор международных и национальных норм и стандартов, которые должны применяться для ареста преступных доходов и орудий преступлений.

5.1 Международные стандарты

В этой главе будет представлен обзор международных нормативных документов, актуальных в контексте ареста преступных доходов. Понимание этих инструментов, помимо чисто теоретического значения, важно для понимания основ и базовых принципов международного сотрудничества.

Подход к вопросам предупреждения преступности и отправления правосудия в виде мер, предусматривающих конфискацию доходов от преступной деятельности, впервые был внедрен Конвенцией Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (1988), которая предусматривала арест, замораживание и конфискацию доходов или другого имущества эквивалентной стоимости, полученного от наркопреступности, а также перенос бремени доказывания законности приобретения такого имущества. [9]

Эти принципы нашли свое дальнейшее развитие в Конвенции Организации Объединенных Наций против организованной преступности (2000) и Протоколах к ней, которые не только распространили вышеуказанные возможности по аресту и конфискации на наиболее распространенные формы организованной преступности, но и установили правила для стран-участниц Конвенции в вопросах международного сотрудничества с целью ареста и конфискации, а также управления арестованными активами. [10]

Принятая в 2003 г. Конвенция Организации Объединенных Наций против коррупции содержит аналогичные по объему и содержанию положения, касающиеся ареста, замораживания и конфискации, применимые к преступлениям, связанных с коррупцией (в понимании и объеме,

[9] Статья 5 Конвенции Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ.
[10] Статьи 12-14 Конвенции Организации Объединенных Наций против транснациональной организованной преступности.

определенном Конвенцией), а также содержит отдельную главу о возвращении активов. [11]

Необходимость внедрения эффективных процедур ареста, замораживания и конфискации преступных доходов и орудий преступлений также признается Стандартами Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ). В частности, стандарты ФАТФ требуют конфискации «отмытого» имущества, доходов, полученных от отмывания денег или предикатных преступлений, инструментов, использованных или предназначавшихся для использования для отмывания денег или совершения предикатных преступлений, или имущества эквивалентной стоимости без ущемления прав добросовестных третьих лиц. Такие меры должны включать предоставление полномочий на: (а) выявление, отслеживание и оценку имущества, подлежащего конфискации; (б) принятие обеспечительных мер, таких, как замораживание и арест в целях предотвращения любых операций (сделок), передачи или распоряжения таким имуществом; (в) принятие мер с целью предотвратить или нейтрализовать любые действия, которые подрывают способность государства замораживать или арестовывать имущество, подлежащее конфискации; и (г) принятие любых надлежащих следственных мер. [12] Наиболее важным является то, что такие меры (включая конфискацию) могут быть предприняты в отсутствие обвинительного приговора, то есть, еще до того, как компетентный суд вынесет окончательное решение по сути уголовного дела. [13]

На региональном уровне к странам ГУАМ применяются также положения Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности 1990 г., с дополнениями, внесенными в 2005 г. Конвенцией Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма, которые предусматривают инструменты и требования, аналогичные описанным выше. [14]

---

[11] Статья 31 и Раздел V Конвенции Организации Объединенных Наций против коррупции.

[12] Стандарты ФАТФ, Рекомендация 4 « Обеспечительные меры и конфискация» (Источник: http://www.fatf-gafi.org).

[13] Больше информации о международных стандартах и инструментах, касающихся ареста преступных доходов и орудий преступлений, можно найти в сборнике УНП ООН "Обзор Конвенций ООН и других международных стандартов, касающихся борьбы с отмыванием денег и противодействия финансированию терроризма" (Источник: https://www.imolin.org/pdf/overview_of_UN_conventions_2013.pdf).

[14] Разделы 3 и 4 указанных Конвенций.

5.2 Национальное законодательство и компетентные органы

Для того, чтобы обеспечить арест и конфискацию доходов от преступлений, странам нужно не только установить нормы и требования к соответствующим процедурам согласно их внутреннего законодательства, но и определить компетентные органы, которые будут эффективно реализовывать эти полномочия.

С точки зрения материально права во всех станах ГУАМ предусмотрена уголовная ответственность за легализацию доходов, полученных преступным путем. [15] Во всех странах, за исключением Украины, [16] применяется подход, предусматривающий включение всех уголовных преступлений в категорию предикатных по отношению к отмыванию денег. Это означает, что доходы и орудия любого уголовного преступления могут быть предметом замораживания, ареста и конфискации.

В странах ГУАМ порядок ареста преступных доходов или орудий преступлений рассматривается преимущественно в контексте уголовно-процессуального законодательства. [17] И хотя ни одно из этих положений не содержит никаких запретительных или иных критериев, которые могли бы ограничить их применение к виртуальным валютам как доходам или орудиям преступлений, несколько важных моментов обращают на себя внимание:

- В свете изменяющихся условий, в которых применяется арест имущества, а также различных определений самого имущества для осуществления ареста необходимо учитывать природу виртуальных валют. Другими словами, во всех указанных юрисдикциях предусмотрен арест орудий преступлений. Но арест доходов от преступлений может быть обусловлен конкретными преступлениями или критериями тяжести содеянного;
- Существуют различные степени вовлеченности судебных инстанций в процедуры ареста имущества, в том числе утверждение уже произведенного ареста в неотложных обстоятельствах, имеющие непосредственное влияние на оперативность данной

[15] Статья 193[1] Уголовного кодекса Азербайджанской Республики; Статьи 194 и 194[1] Уголовного кодекса Грузии; Статья 243 Уголовного кодекса Республики Молдова; и статья 209 Уголовного кодекса Украины.

[16] Статья 209 Уголовного кодекса Украины предусматривает минимальный порог наказания (наказание в виде лишения свободы или штраф свыше 3000 минимальных размеров оплаты труда), а также исключение – преступление об уклонении от уплаты налогов (статьи 212 и 212[1] Уголовного кодекса).

[17] Статья 249 Уголовно-процессуального кодекса Азербайджанской Республики; Статья 151 Уголовно-процессуального кодекса Грузии; Статья 203-204 Уголовно-процессуального кодекса Республики Молдова; Статья 100 Уголовно-процессуального кодекса Украины.

процедуры и важное значение с точки зрения обеспечения сохранности электронных доказательств;

- В некоторых странах предусмотрено применение гражданской процедуры наложения ареста на имущество, что обуславливает необходимость специальных знаний, которые не всегда могут иметься у правоохранительных органов, уполномоченных проводить такой арест;
- Во всех странах ГУАМ предусмотрена возможность ареста до вынесения обвинительного приговора, что означает, что стандарт доказывания, необходимый для осуществления ареста преступных доходов ниже стандарта, необходимого для вынесения судебного решения, по сути дела.

Еще одним важным вопросом является то, какие ведомства уполномочены осуществлять арест в уголовных делах, связанных с использованием виртуальных валют. На сегодняшний момент соответствующими функциями в странах ГУАМ наделены правоохранительные органы, уполномоченные использовать любые предусмотренные уголовно-процессуальным законодательством процедуры при условии, что они обладают подследственной юрисдикцией в отношении данного уголовного дела. В контексте данного пособия это – подразделения, уполномоченные расследовать легализацию преступных доходов.[18]

Тем не менее, пожалуй, не требует доказательств, что различные вопросы доходов и орудий преступлений требуют наличия специальных знаний, а использование виртуальных валют может потребовать еще большей специализации, которой могут не располагать правоохранительные органы. В таких случаях для осуществления ареста преступных доходов и орудий преступлений могут потребоваться проведение экспертиз и предоставление экспертных отчетов[19], особенно в случаях, когда ходатайства о таких процессуальных действиях должны санкционироваться судьей.

[18] Департамент по борьбе с коррупцией при Генеральной прокуратуре Азербайджана; Антикоррупционный департамент Офиса Главного прокурора Грузии; Служба по предупреждению и борьбе с отмыванием денег Национального антикоррупционного центра Республики Молдова; Департамента финансовых расследований при Министерстве доходов и сборов Украины. На ряду с последним следственные действия также осуществляют Министерство внутренних дел и/ или Служба безопасности Украины.

[19] Глава XXXV Уголовно-процессуального кодекса Азербайджанской Республики; Статья 144-146 Уголовно-процессуального кодекса Грузии; Статьи 142-153 Уголовно-процессуального кодекса Республики Молдова; Статьи 242-245 Уголовно-процессуального кодекса Украины.

5.3 Вопросы юрисдикции

Виртуальные валюты функционируют и находят свое развитие в онлайновой среде, которая не имеет национальных границ и делает электронную торговлю международным феноменом. В этом свете не удивительно, что одним из наиболее проблематичных вопросов для репатриации доходов, полученных в результате совершения преступлений, связанных с виртуальными валютами, является вопрос юрисдикции и выдвигаемых нею требований к международному сотрудничеству.

Следует с самого начала отметить, что на сегодняшний день нет известных случаев международного сотрудничества с целью ареста или конфискации виртуальных валют. Таким образом, следующие ниже предложения основываются на общих принципах установления юрисдикции с целью ареста виртуальных валют как доходов/ орудий преступлений.

В первую очередь, юрисдикционные аспекты ареста доходов, полученных преступным путем, и орудий преступлений выявляют различия между централизованными и децентрализованными виртуальными валютами. В случае с централизованными виртуальными валютами, например, валютами, использующихся в онлайновых играх, обмен валют рассматривается как разрешение на доступ к некоторым функциям или услугам, предлагаемых администратором, и, таким образом, остается, как технически, так и юридически, под контролем компании-эмитента виртуальных валют. [20] С точки зрения ареста активов это означает, что юрисдикция, где находится администратор виртуальной валюты, является, если специально не установлено иначе, юрисдикцией для целей ареста и конфискации преступных доходов.

Децентрализованные виртуальные валюты, т.е. криптовалюты, в этом смысле демонстрируют совсем иную картину. Например, bitcoin сами по себе не существуют в любой форме, даже в виде цифрового файла. На практике существует только реестр операций между разными адресами с балансами, которые увеличиваются или уменьшаются. [21] Поэтому, если рассматривать в качестве доходов или орудий преступления, bitcoin не может рассматриваться как физически находящиеся в той или иной среде или даже в определенном месте. Однако, учитывая, что они bitcoin-транзакции обозначают сделки между Bitcoin-адресами отдельных пользователей, bitcoin имеют непосредственную связь с определенными адресами, в отношении которых соответствующие пользователи осуществляют контроль. Таким образом, в случае с криптовалютами юрисдикционный подход будет выглядеть так: в соответствии с

[20] http://lindenlab.com/tos#tos4
[21] http://www.coindesk.com/information/how-do-bitcoin-transactions-work/

международным публичным правом территориальная юрисдикция над доходами или орудиями преступлений, совершенных с использованием криптовалют, будет определяться местом нахождения кошелька. Другими словами, физическое расположение оборудования, на котором хранится кошелек с виртуальной валютой, следует рассматривать как юрисдикцию для целей замораживания, ареста и конфискации преступных доходов и орудий преступления.

Особой сложностью для установления юрисдикции в связанных виртуальными валютами случаях являются облачные сервисы (рассматривались в Модуле 2). Данные кошельков с виртуальными валютами, хранящихся в «облаке», могут регулярно мигрировать с одного сервера на другой, с легкостью «пересекая» национальные границы. В терминологии, используемой при расследовании компьютерных преступлений, это часто называется «потерей места».[22] Однако, до тех пор, пока не случится значительного пересмотра международного публичного права, принцип территориальности остается отправной точкой для установления юрисдикции. Поэтому, используя все доступные механизмы международного сотрудничества, нужно приложить все усилия для определения местоположения кошелька – данных, хранящихся на определенном сервере в конкретной юрисдикции.

[22] См., например, Совет Европы, «Документ для обсуждения "Облачные вычисления и расследования киберпреступлений: территориальность против распорядительной власти?"», стр. 5 (Источник: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf).

6 Процедуры и инструменты ареста

Внимание в данном разделе сконцентрировано на существующих подходах и методах ареста преступных доходов и орудий преступлений, которые могут быть актуальными в контексте виртуальных валют. С этой целью мы рассмотрим некоторые практические процедуры и умозаключения, связанные с их арестом и последующей конфискацией.

Подобно используемому в данном пособии подходу процедурные возможности осуществления ареста преступных доходов и орудий преступлений включают в себя мероприятия по установлению таких доходов (выявление активов) и собственно их арест посредством существующих правовых процедур. И хотя это деление на первый взгляд может показаться условным, практическое позиционирование виртуальных валют как преступных доходов и орудий преступлений выявляют различия между этими подходами, не в последнюю очередь с институциональной точки зрения.

Подходы и процедуры, представленные в этом разделе, выстроены в определенном порядке, который отражает попытку применения логики следственных действий в рамках уголовного расследования к контексту виртуальных валют. Однако, учитывая новизну и неизученность вопросов, связанных с этим контекстом, последовательность перечисленных здесь действий и техник, представлена только для целей общего ознакомления.

6.1 Шаг 1: Инициирование финансовых расследований

Финансовое расследование включает в себя сбор, сопоставление и анализ всей имеющейся информации для оказания помощи уголовному расследованию и лишения преступников их доходов и орудий совершения преступлений. [23] Главной целью финансового расследования является выявление и документирование фактов движения денежных средств в ходе осуществления преступной деятельности. Связь между источником происхождения денежных средств, получателями средств, и тем, когда они были получены и где хранятся, может быть источником информации о преступной деятельности и служить ее доказательством. [24] С этой точки зрения финансовое расследование – это процесс, который, как правило, идет параллельно уголовному расследованию, будь то расследование киберпреступлений, мошенничества или отмывания денег, и позволяет

[23] Отчет ФАТФ, «Руководство по финансовым расследованиям: оперативные вопросы», ФАТФ/ОЭСР 2012, стр. 6.
[24] Отчет ФАТФ, «Руководство по финансовым расследованиям: оперативные вопросы», ФАТФ/ОЭСР 2012, стр. 3.

следователям сосредоточиться исключительно на доходах и орудиях преступлений.

Финансовые расследования, таким образом, требуют специальных знаний, которыми не всегда могут располагать правоохранительные органы. Для решения этой проблемы национальные власти могут прибегнуть к таким действиям:

- Создать совместную следственную группу по решению прокурора и при его общей координации, в том числе в вопросах распределения обязанностей;
- Привлечь к текущему расследованию финансовых экспертов при сохранении полного контроля над расследованием уголовного дела у заинтересованного правоохранительного органа;
- Отделить расследование по поиску преступных активов от основного уголовного расследования и обеспечить обратную связь между следственными органами.

На какой бы из этих вариантов не пал выбор, необходимо учитывать характерные особенности финансовых расследований. Одной из таких особенностей является менее высокий стандарт доказывания по сравнению с уголовным делом (об отмывании денег). Доказательство преступного происхождения имущества и доходов не требует подхода «вне разумного сомнения», что кардинальным образом отличает финансовые расследования от традиционных уголовных расследований.

Финансовые расследования в отношении виртуальных валют как доходов и орудий преступлений по-прежнему остаются относительной новизной. По этой причине не существует никаких опробованных подходов к вопросам о том, как проводить расследования в делах, связанных с виртуальными валютами. Последующие главы представляют собой попытку предложить некое руководство, в основе которого лежат наиболее актуальные методы расследования, подходящие для выявления, контроля и управления виртуальными валютами.

6.2 Шаг 2: Выявление активов

Выявление активов или, иными словами, установление «денежного следа» является важной частью финансовых расследований, нацеленных на установление преступного происхождения доходов или орудий преступлений. В расследованиях в отношении виртуальных валют это может считаться предварительным этапом, на котором необходимо определить объект замораживания или ареста, после чего последует сам арест таких объектов.

Выявление активов, как и любая другая разведывательная деятельность в уголовном или финансовом расследовании полагается на определенные индикаторы – «красные флажки», которые могут помочь следователю установить преступный характер доходов/ имущества. На самом деле, красные флажки, о которых идет речь здесь и которые были детально рассмотрены в Модуле 3 данного пособия, являются актуальными не только для фактических расследований, но и вообще для отслеживания транзакций, совершенных при помощи виртуальных валют. Это:

- Большое количество банковских счетов, принадлежащих одному администратору виртуальной валюты или компании, занимающейся обменом виртуальных валют (иногда находятся в разных странах), которые, по всей видимости, используются как транзитные счета (что может свидетельствовать о деятельности, характерной для второго этапа процесса отмывания денег – «расслоения») без разумного обоснования такой бизнес-схемы;
- Администратор виртуальной валюты или компания, занимающейся обменом виртуальных валют, находятся в одной стране, но имеют счета в других странах, в которых нет большой клиентской базы (нелогичное обоснование такой бизнес-деятельности, что может быть подозрительным);
- Круговое движение денежных средств между банковскими счетами, находящихся в разных странах и принадлежащих разным администраторам виртуальной валюты или компаниям, которые занимаются обменом виртуальных валют (может свидетельствовать о деятельности, характерной для второго этапа процесса отмывания денег – «расслоения», если такая деятельность не является обычной бизнес-активностью компании);
- Объем и частота операций с наличностью (иногда разбиты на суммы, меньшие порога предоставления отчетности), проводимые собственником администратора виртуальной валюты или компании, занимающейся обменом виртуальных валют, и не имеющие экономического смысла;
- Системы виртуальных валют, не имеющие соответствующей регистрации и/ или прозрачности или, известно, что они пользуются популярностью у известных преступных групп.

Как следует из анализа этих индикаторов, они сфокусированы на точках контакта виртуальных валют с финансовыми учреждениями, включая центральных администраторов, валютные биржи, операторов платежных услуг в виртуальных валютах, услуг хостинга, торговые компании и т.д. Однако следует иметь в виду, что транзакции с виртуальными валютами проходят вне финансовых учреждений, а анонимный характер таких операций, использование криптографии и отсутствие какой-либо официальной документации делают выявление криптовалют

чрезвычайно трудной, если не невыполнимой, задачей. Даже если для таких валют, как, например, bitcoin, существует общедоступный открытый и прозрачный реестр всех проведенных транзакций (известный как цепочка блоков), [25] для установления связи между конкретной транзакцией и соответствующим пользователем (кошельком) потребуется информация из других источников.

В этой связи существует несколько возможных вариантов установления фактов использования виртуальных валют:

6.2.1 Вариант 1: Финансовые разведданные

Подразделение финансовой разведки (ПФР) следует рассматривать в качестве основного партнера правоохранительных органов в вопросах выявления и отслеживания преступных доходов и орудий преступлений, учитывая наличие у ПФР прямого доступа к финансовой информации, имеющей отношение к предполагаемым доходам от преступлений и потенциальному финансированию терроризма. Предоставляемая ПФР разведывательная информация является ключевой для эффективного расследования и конфискации преступных доходов. [26]

Одной из основных функций национального ПФР является обработка и предоставление информации, которая может быть использована для целей финансовой разведки. СПО (сообщения о подозрительных операциях) вместе с результатами проведенного ПФР анализа таких отчетов имеют особое значение и ценность.

В случае централизованных виртуальных валют управление валютными токенами или игорными активами осуществляется в основном администратором по внутренним каналам, отделенных от традиционной финансовой системы государства. Таким образом, наличие и ценность СПО от центральных администраторов будут определяться степенью государственного регулирования виртуальных валют и установленными требованиями по предоставлению СПО национальному ПФР.

В случае с децентрализованными виртуальными валютами, т.е. криптовалютами, СПО о транзакциях, совершенных биржами виртуальных валют, являлись бы особенно полезным источником информации для выявления преступных доходов и орудий преступлений.

---

[25] https://blockchain.info/

[26] Руководство УНП ООН по международному сотрудничеству для целей конфискации доходов, полученных преступным путем, стр. 24.

В общем, правоохранительные органы должны быть знакомы со структурой, ролью и полномочиями службы финансовой разведки в своей стране. [27] В дополнение к сообщениям о подозрительных операциях, многие подразделения финансовой разведки имеют право получать и анализировать сообщения об операциях, превышающие определенный порог, как в наличной, так и безналичной формах, что делает подразделения финансовой разведки держателями важной финансовой информации.[28]

6.2.2 Вариант 2: Мониторинг операций

Информация и разведданные, необходимые для финансовых расследований, могут быть также получены посредством мониторингового ордера или ордера на предоставление информации.

«Мониторинговый ордер» означает выданный компетентным органом приказ финансовому учреждению, требующей от последнего раскрытия уполномоченному лицу информации об операциях по счету, открытом в этом учреждении, или по счету, который принадлежит указанному в ордере лицу. Такой приказ может предусматривать обязательство для финансового учреждения сообщить об операции сразу после ее проведения или при попытке ее проведения. Помимо этого, мониторинговый ордер может обязать финансовое учреждение воздержатся от совершения или завершения операции в течение определенного периода времени.[29]

Что касается стран ГУАМ, мониторинговые ордеры могут быть выданы как правоохранительными органами, так и ПФР (за исключением Азербайджана). В соответствии с положениями уголовно-процессуального законодательства правоохранительные органы имеют право мониторинга любого счета, в отношении которого есть подозрения в его причастности к отмыванию денег, финансированию терроризма, предикатным преступлениям, а также к любому другому уголовно наказуемому деянию. [30] ПФР также имеют право мониторить банковские счета при наличии подозрений в причастности, как правило, ко всем видам преступлений. Правовые основания таких полномочий закреплены либо специальным

---

[27] Дополнительную информацию касательно компетенции, функциях и полномочиях ПФР Вы сможете найти в публикации Международного Валютного Фонда/ Всемирного Банка "Подразделения финансовой разведки: обзор" (Источник: http://www.imf.org/external/pubs/ft/FIU/fiu.pdf)

[28] Руководство УНП ООН по международному сотрудничеству для целей конфискации доходов, полученных преступным путем, стр. 44.

[29] Руководство УНП ООН по международному сотрудничеству для целей конфискации доходов, полученных преступным путем, стр. 3.

[30] Исследование МАНИВЕЛ "Замораживание финансовых транзакций и мониторинг банковских счетов", Совет Европы, 2013, стр. 40-41 (Источник: http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2013)8_Postponement.pdf)

законодательством по борьбе с отмыванием денег, либо законом об оперативно-розыскной деятельности. [31] Факторами, являющимися основанием для инициирования мониторинговых ордеров, являются: запрос иностранного компетентного органа (в том числе ПФР), результаты своего анализа, СПО, полученные от субъекта мониторинга, или запрос прокуратуры.

Ордер на предоставление информации означает санкционированный судом приказ, обязывающий конкретное лицо предоставить для проверки уполномоченному лицу документ, связанный с или указывающий на местонахождение имущества, подлежащее аресту или конфискации, или который может помочь определить стоимость имущества или выгоду, полученную обвиняемым вследствие совершения уголовного деяния. [32]

Иными словами, цель таких ордеров – принудить указанное в них физическое или юридическое лицо предоставить информацию/ документы или их копии в течение определенного времени. Такие ордеры будут иметь существенные отличия с точки зрения их применения к централизованным и децентрализованным виртуальным валютам:

- Администраторы централизованных виртуальных валют могут получать и выполнять такие ордеры непосредственно;
- Принимая во внимание отсутствие центральных административных органов у систем децентрализованных виртуальных валют, мониторинговые ордеры и ордеры на предоставление информации с указанием имен конкретных клиентов и/ или их счетов, подлежащих проверке и мониторингу, могут быть направлены лицам, занимающиеся конвертацией виртуальных валют.

[31] Исследование МАНИВЕЛ "Замораживание финансовых транзакций и мониторинг банковских счетов", Совет Европы, 2013, стр. 38-39 (Источник: http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2013)8_Postponement.pdf).

[32] Руководство УНП ООН по международному сотрудничеству для целей конфискации доходов, полученных преступным путем, стр. 4.

Пример: Преследование bitcoin-обменника за отмывание денег

В январе 2014 года в международном аэропорту Джона Ф. Кеннеди в Нью-Йорке американские прокуроры арестовали Чарли Шрема, известного 24-летнего защитника Bitcoin. Он обвинялся в сговоре с целью отмывания доходов на сумму более $ 1 млн., принадлежащих пользователям онлайнового черного рынка Silk Road (Шелковый Путь). Другой подозреваемый – Роберт Файелла – был также арестован по выдвинутому Офисом прокурора Манхэттена обвинению в преступном сговоре, направленном на оказание помощи клиентам сайта Silk Road анонимно приобретать все желаемое от наркотиков до поддельных паспортов.

Чарли Шрем управлял Bitinstant, Нью-Йоркским bitcoin-обменником, который был одним из первых зарегистрированным в Департаменте казначейства США. В 2013 г. компания привлекла $ 1,5 млн. инвестиций от Winklevoss Capital.

По утверждению прокуроров, Шрем и Файелла продали пользователям сайта Silk Road более 1 млн. долл. США электронных денег. Так, 52-летний Файелла осуществлял на сайте Silk Road управление «подпольным» bitcoin-обменником, через который продавалась валюта для пользователей сайта с декабря 2011 до октября 2013 года. После подтверждения заказа Файелла получал валюту от базирующейся в Нью-Йорке компании, в которой Шрем являлся главным исполнительным директором, а затем продавал ее пользователям с наценкой.

Другая компания, не названная в иске, предоставляла пользователям возможности по анонимному обмену наличных денег на bitcoin. Шрем также являлся комплаенс-менеджером этой компании, ответственным за соблюдение законодательства в сфере противодействия отмыванию денег.

Согласно иску, в обмен на вознаграждение Шрем удовлетворял заказы Файеллы, зная, что валюта предназначалась для пользователей Silk Road, которые могли использовать ее для покупки наркотиков и оплаты контрабанды. Кроме того, Шрем делал скидки Файелле за оптовые заказы, маскируя таким образом, заказы, поступавшие от другого соучредителя его компании, и не подавал в уполномоченные органы отчеты о подозрительной деятельности в соответствии с требованиями

федерального законодательства. По заявлениям прокуроров, Шрем также лично покупал наркотики на Silk Road.

«Сами по себе bitcoin не являются незаконными и известны случаи их законного использования. Но, принимая во внимание ту легкость, с которой bitcoin позволяют перемещать деньги, соблюдая при этом анонимность, хорошо известны и случаи их незаконного использования, в том числе с целью отмывания преступных доходов», – заявил в иске агент Службы внутренних доходов США, расследовавший дело.

Оба мужчины обвиняются в преступном сговоре с целью совершения отмывания денег и оказания нелицензированных услуг по переводу денег. В дополнение к этому Шрем также обвиняется в умышленном непредоставлении сообщений о подозрительной деятельности. Как результат, Файеллу грозит срок до 25 лет, а Шрему – до 30 лет лишения свободы. [33]

6.2.3 Вариант 3: Раскрытие финансовой информации

Раскрытие финансовой информации – еще одна возможность для использования ордеров на предоставление информации, что представляет собой особенно важный источник данных для выявления преступных доходов и орудий преступлений. Требования по борьбе с отмыванием денег для банковских и небанковских учреждений предписывают им хранить определенную информацию о счетах и деятельности своих клиентов, которую можно истребовать и использовать для поиска интересующих активов.

С точки зрения виртуальных валют такие запросы, как уже отмечалось ранее, нужно направлять компаниям, занимающимся обменом виртуальных валют, и которые, как предполагается, соблюдают требования в сфере противодействия отмыванию денег, в том числе касательно хранения документации. Информацию о клиентах и их операциях по конвертации виртуальных валют следует истребовать, не нарушая действующие нормы по защите данных, и использовать такую информацию исключительно для целей расследований.

Денежные переводы часто используются для обмена фиатных денег на децентрализованные виртуальные валюты, такие как bitcoin, и наоборот.[34] Этот, равно как и другие используемые обменниками способы оплаты

[33] The Wall Street Journal, «Двое обвиняемых в причастности к схеме по отмыванию денег с использованием bitcoin» (Источник: http://online.wsj.com/article/BT-CO-20140127-709257.html)

[34] http://www.coindesk.com/information/how-can-i-buy-bitcoins/

является еще одним потенциально ценным задокументированным источником информации, который не следует упускать из внимания, проводя поиски преступных доходов и орудий совершения преступления.

6.3 Шаг 3: Взятие активов под контроль

После того, как преступные доходы или орудия преступления установлены, их можно арестовать. Арест, как отмечалось выше, означает взятие компетентным органом под контроль установленного имущества и осуществление в отношении него функций владения, распоряжения или управления.

И хотя есть соответствующий опыт ареста и конфискации электронных денег или счетов (нематериальные активы), которые могут быть использованы по аналогии, виртуальные валюты в отсутствие государственного регулирования обращаются вне установленных финансовых учреждений и каналов. Говоря об аресте виртуальных валют, как доходов или орудий преступлений, различия между централизованными и децентрализованными валютами определяют разницу в подходах, используемые в таких случаях.

6.3.1 Вариант 1: Арест централизованных виртуальных валют

В случае централизованных виртуальных валют активы в виде виртуальной валюты остаются под полным контролем администратора. Поэтому арест таких активов может применяться в отношении юридических лиц, занимающиеся их администрированием, что позволит обеспечить выполнение законных требований правоохранительных органов.

В это же время существуют некоторые особенности ареста централизованных виртуальных активов. Если, к примеру, WebMoney или уже не существующая E-Gold сами осуществляют администрирование виртуальной валютой, которую можно арестовать и конвертировать в фиатные деньги, то арест предметов амуниции или боевых кораблей компьютерной игры будет иметь мало практической пользы для правоохранительных органов и государства. В таких случаях можно использовать стоимостную конфискацию, означающей наложение денежного обязательства (например, штрафа, значительно превышающего прибыль или полученную от преступления выгоду). Такая конфискация применима в отношении любого актива лица[35] и позволяет избежать

[35] Руководство УНП ООН по международному сотрудничеству для целей конфискации доходов, полученных преступным путем, стр. 5.

указанных выше и других потенциальных трудностей, связанных с управлением специфического рода активами.

Пример: Предметы многопользовательских онлайновых игр

Китайская компания Shanda Interactive была вынуждена выплатить 5000 юаней и извиниться перед геймером разработанной нею игры «The World of Legend» («Мир Легенд») из-за изъятия его виртуальных активов.

22 ноября 2006 года геймер по фамилии Жанг обнаружил пропажу с его игрового счета шести виртуальных предметов стоимостью более 1 500 юаней, в связи с чем и обратился в компанию Shanda Interactive. Компания заявила, что предметы были изъяты нею в связи с полицейским расследованием в отношении продажи краденых виртуальных предметов. Как сообщается, Shanda Interactive не выполнила предписания полиции и возвратила предметы после окончания расследования. [36]

И хотя этот пример совершенно не связан с отмыванием денег и получением доходов от преступлений, он демонстрирует, что правоохранительные органы и судебная система имеет в распоряжении соответствующие инструменты для ареста и конфискации виртуальных активов, а также, что в интересах эффективности расследований может применяться стоимостная конфискация.

6.3.2 Вариант 2: Арест криптовалют

Криптовалюты в отличие от централизованных виртуальных валют не имеют координирующего или центрального органа. Это означает, что процедуры ареста таких валют должны применяться в отношении отдельных пользователей, а объектом ареста будет являться виртуальная валюта, которая находится в их кошельках/ адресах.

Теоретически взятие кошелька с виртуальной валютой под контроль может осуществляться двумя разными способами. Первый – заставить пользователя предоставить компетентному органу пароль доступа к кошельку. Плюсы такого подхода включают в себя возможности дальнейшего проведения разведывательных и следственных действий, так

[36] MMOsite, «Игровую компанию обязали уплатить штраф за изъятые виртуальные предметы» (Источник: http://news.mmosite.com/content/2007-12-30/20071230222432466.1.shtml).

как в силу присущей криптовалютам анонимности нельзя установить, кто именно осуществляет фактическое владение кошельком. Однако минусы этого подхода значительно перевешивают плюсы:

- Наличие правовых полномочий принудить пользователя представить его/ ее конфиденциальные данные во многом будет зависеть от правовой системы государства. В контексте стран ГУАМ отказ от предоставления данных доступа к кошельку может быть истолкован как манипулирование доказательствами, что повлечет за собой дополнительные уголовные обвинения. Но невысокая оперативность, характерная для такого подхода, в купе с волатильностью электронных доказательств могут работать против интересов следствия;
- Отсутствие гарантий, что даже при условии предоставления следствию данных доступа к кошельку преступником или его соратниками не были сделаны копии, позволяющие восстановить контроль над арестованными активами.

Поэтому на данный момент самым приемлемым вариантом представляется взятие виртуальных валют под контроль путем передачи их на счет (кошелек) правоохранительного органа. Этот процесс состоит из нескольких этапов:

- Определение количества виртуальной валюты или кошельков, или и того и другого, подлежащих аресту;
- Обеспечение сотрудничества со стороны подозреваемого или установление контроля над кошельком с помощью других разрешенных законом средств, чтобы необходимая сумма была переведена на контролируемый правительством кошелек с целью последующей конфискации и ликвидации;
- Документирование должным образом получения активов; или
- Если сотрудничество или контроль над кошельком невозможны:
    - определить на основе обменного курса стоимость виртуальной валюты, подлежащей аресту, в местной валюте;
    - применить процедуру стоимостной конфискации.

Разумеется, к стоимостной конфискации можно прибегнуть и изначально, особенно в случаях, когда традиционный арест и контроль над виртуальными валютами невозможны в силу либо соображений безопасности, либо с точки зрения обременительного управления такими активами.

Одним из дополнительных аргументов в пользу передачи виртуальных валют или их стоимостного эквивалента на счета, контролируемые государством, является то, что это, по-видимому, было самым

предпочтительным способом в очень немногочисленных случаях применения ареста и конфискации к виртуальным валютам. В частности, как уже отмечалось, в случае с Silk Road правительство США управляло набольшим в мире bitcoin-кошельком, в котором хранилась изъятая у Silk Road виртуальная валюта. [37]

Пример: Арест bitcoin в деле по наркотикам

Администрация по борьбе с наркотиками США (DEA) опубликовала официальное сообщение об изъятии bitcoin у физического лица, виновного в покупке подконтрольных веществ. По данным Let's Talk Bitcoin, это – пожалуй, первый случай изъятия bitcoin правоохранительными органами.

Согласно сообщению DEA, среди прочих других г-н Эрик Даниэль Хьюз (также известный как Кейси Джоунс) владел 11.02 BTC стоимостью, рваной на 12 апреля с.г. 814,22 USD. Цифровая валюта была изъята в округе Южная Каролина по причине нарушения виновным Акта о контролируемых веществах (21 U.S.C. §§ 801 и послед.).

Сообщение содержит обобщенные данные, рассказывающее обо всех случаях конфискации у граждан США, нарушивших Акт о подконтрольных веществах, где случай Хьюз является одним из многих. В то же время не сообщается о деталях ареста bitcoin. Сообщение также не содержит информации о взломе Bitcoin-протокола. Под «арестом», вероятнее всего, понимается, что активы были получены в результате тайной операции в отношении Silk Road, а не в результате фактического ареста bitcoin, находящихся в кошельках пользователей», – заявил Андреас М. Антонопулос, эксперт по вопросам безопасности и спонсор Let's Talk Bitcoin.

Свидетельствующий о получении 12 апреля 2013 года 11.02 BTC Bitcoin-адрес 1ETDwGUC1QcjYuehFr3u1FD3MvDaUs7SFy можно увидеть в цепочке блоков. Он совпадает с адресом, указанным в сообщении DEA.[38].

[37] International Business Times, «Американское правительство владеет наибольшим в мире bitcoin-кошельком» (Источник: http://www.ibtimes.com/worlds-biggest-bitcoin-wallet-owned-us-government-1514100).

[38] CoinDesk, «Агентство по борьбе с наркотиками арестовало bitcoin» (Источник: http://www.coindesk.com/bitcoins-seized-by-drug-enforcement-agency/).

6.4 Шаг 4: Управление активами

Одной из главных проблем для правоохранительных органов является управление изъятыми активами, переданных под контроль государства. Учитывая, что право собственности на имущество, ожидающее решения о конфискации, принадлежит его изначальному владельцу, необходимо бережно обращаться с изъятыми активами.

С этой точки зрения виртуальные валюты, будь то централизованные или децентрализованные, представляют собой наименьшую из таких проблем, поскольку, обладая цифровой природой, они физически не портятся. Тем не менее, виртуальные валюты, особенно криптовалюты, подвержены значительным колебаниям обменного курса, [39] что может стать для правоохранительных органов проблемой в контексте предполагаемой конфискации виртуальных валют в пользу государства. Различия в стоимости на момент выявления и фактического ареста может потребовать пересмотра количества и стоимости виртуальных валют, подлежащих изъятию, хотя, с учетом широкой доступности данных обменного курса для этого не потребуется привлечения экспертов и экспертного анализа.

В контексте ареста активов как орудий преступлений одним из ключевых вопросов является профилактический характер ареста, который означает, что орудия совершения преступления должны быть изъяты из обращения. И хотя неизвестно ни об одном зарегистрированном случае ареста централизованных или децентрализованных виртуальных валют в качестве орудий преступлений, может возникнуть необходимость поместить изъятую виртуальную валюту (содержимое кошелька) на съемный носитель с целью обеспечения ее изоляции от виртуальной среды.

Подобная логика будет также применяться к bitcoin, изъятых в качестве доходов от преступлений и помещенных в кошелек под управлением компетентного органа. В таких случаях было бы целесообразно изолировать от виртуальной среды и кошелек, и его содержимое путем создания локальных файлов и их хранения на съемном носителе. [40] Причины этого, кроме желания защитить конфискованные активы от манипуляций транзакциями и майнинга, кроются в том, что виртуальные валюты, обладая цифровой природой, могут быть непреднамеренно изменены или утрачены вследствие ненадлежащего обращения, перебоев в обслуживании или стать целью кибератак. Эти и другие рекомендации по вопросам безопасности можно найти и в самой сети Bitcoin. [41]

---

39 http://www.coindesk.com/price/ http://dogepay.com/ http://www.ltc-charts.com/
40 https://en.bitcoin.it/wiki/How_to_set_up_a_secure_offline_savings_wallet
41 http://www.coindesk.com/information/how-to-store-your-bitcoins/

6.5 Особенности международных расследований

Финансовые расследования часто выходят за рамки национальных границ. Поэтому важно, чтобы компетентные органы могли своевременно использовать возможности формального и неформального международного сотрудничества в ходе всего расследования. Установление контактов на ранних стадиях поможет следователям понять особенности иностранной правовой системы и связанные с этим потенциальные проблемы для целей получения дополнительных данных, а также для формирования общей стратегии расследования. Это также поможет иностранному государству подготовиться к своей участи в сотрудничестве. [42]

Учитывая трансграничную природу сети Интернет, являющегося уникальной средой функционирования виртуальных валют, международное сотрудничество представляет собой важный элемент финансовых расследований преступлений, совершенных с использованием виртуальных валют. Поэтому как формальные, так и неформальные механизмы сотрудничества должны быть использованы эффективно и, самое главное, без промедлений, учитывая волатильность, присущую электронным доказательствам и следам онлайновой преступной деятельности.

Финансовые следователи могут воспользоваться различными механизмами сотрудничества, среди которых:

- Сотрудничество через сети по международному сотрудничеству, специально созданные для выявления доходов от преступлений: Камденская межучрежденческая сеть возвращения активов (CARIN),[43] Инициатива по возвращению похищенных активов (StAR), являющаяся результатом партнерства между Мировым Банком и Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН), [44] или более специализированные сети по возвращению активов, такие как Глобальная сеть координаторов по возвращению активов – совместный проект StAR и Интерпол с акентом на доходах от коррупции;[45]

[42] Отчет ФАТФ, «Руководство по финансовым расследованиям: оперативные вопросы», ФАТФ/ОЭСР 2012, стр. 31.
[43] http://www.assetrecovery.org/kc/node/baf520a5-fe6d-11dd-a6ca-f1120cbf9dd3.6
[44] http://star.worldbank.org/star/
[45] http://www.interpol.int/Crime-areas/Corruption/International-asset-recovery

- Использование механизмов сотрудничества между органами полиции, в особенности, такие как контактные центры 24/7 в соответствии с Конвенцией Совета Европы о компьютерных преступлениях, G8 Сеть подразделений в сфере высокотехнологичных преступлений или национальные бюро Интерпол, которые могут предоставить данные разведывательного характера, выполнить запросы по обеспечению сохранности данных, а также другие следственные запросы непрямую в обход трудоемкой процедуры взаимной правовой помощи;

- Установление посредством национального ПФР контактов с ПФР иностранных государств, запрашивая по защищенному каналу Egmont Secure Web[46] данные о СПО или другую разведывательную информацию, включая результаты проведенного анализа, а также использование других, в том числе двусторонних, механизмов сотрудничества; и

- Использование формальных процедур обмена информацией с Центральным органом (прокуратурой) – механизм обмена запросами в рамках взаимной правовой помощи.

Что касается последнего варианта, не вдаваясь в излишние подробности о юридически сложных аспектах предоставления взаимной правовой помощи, отметим, что, выполнение запросов об аресте централизованных или децентрализованных виртуальных валют натолкнется на дополнительную проблему, связанную с отсутствием должного правового регулирования таких валют (данный вопрос уже рассматривался в Модуле 1 данного пособия) и, таким образом, ставит вопрос определения статуса виртуальных валют в финансовой системе запрашиваемого государства на усмотрение этого государства. Следует иметь в виду, что взаимная правовая помощь является весьма формализованным процессом, зависящим от точных определений и четких процедур. Достаточно часто эффективность такого механизма сотрудничества определяется наличием понимания/ желания у запрашиваемого государства иметь дело с вопросами, которые могут быть чужды ее правовой системе.

46 http://www.egmontgroup.org/membership

Вопросы по самооценке

Вопрос 1: Каковы различия между преступными доходами и орудиями преступлений?

Вопрос 2: Каковы различия между замораживанием и арестом преступных доходов и орудий преступлений?

Вопрос 3: Объясните необходимость экспертной помощи для выявления и ареста преступных доходов и орудий преступлений.

Вопрос 4: Объясните, как нужно определять соответствующую юрисдикцию для процессуальных действий в отношении децентрализованных виртуальных валют как доходов преступления?

Вопрос 5: Назовите, по крайней мере, два «красных флажка», применимых для выявления преступных доходов, связанных с обменниками виртуальных валют.

Вопрос 6: Объясните значение сообщений о подозрительных операциях (СПО) для целей выявления преступных доходов и орудий преступлений, совершенных с использованием виртуальных валют.

Вопрос 7: Опишите процесс ареста (взятия под контроль) децентрализованной виртуальной валюты.

Вопрос 8: Назовите, по крайней мере, два механизма международного сотрудничества в финансовых расследованиях.

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Приложение 1
Библиография

В этом приложении приведен перечень всех информационных источников, на которые делались ссылки в тексте настоящего пособия.

Национальное законодательство

- **Азербайджан**
    - «Уголовный кодекс Азербайджанской Республики»
    - «Уголовно-процессуальный кодекс Азербайджанской Республики»
    - «Закон Азербайджанской Республики Об оперативно-розыскной деятельности»
    - «Закон Азербайджанской Республики О предотвращении легализации денежных средств или другого имущества, полученного преступным путем, или финансирования терроризма»
- **Грузия**
    - «Уголовный кодекс Грузии»
    - «Уголовно-процессуальный кодекс Грузии»
    - «Закон Грузии О содействии предотвращению легализации преступных доходов»
- **Молдова**
    - «Уголовный кодекс Республики Молдова»
    - «Уголовно-процессуальный Республики Молдова»
    - «Закон Республики Молдова о борьбе с киберпреступностью»
    - «Закон Республики Молдова о специальной розыскной деятельности»
    - «Закон Республики Молдова О предупреждении и борьбе с отмыванием денег и финансированием терроризма»
- **Украина**
    - «Уголовный кодекс Украины»
    - «Уголовно-процессуальный кодекс Украины»
    - «Закон Украины О предотвращении и противодействии легализации (отмыванию) доходов, полученных преступным путем или финансированию терроризма»

Организация Объединенных Наций

- «Международная конвенция о борьбе с финансированием терроризма»
  - http://www.un.org/law/cod/finterr.htm

- «Типовой закон ЮНСИТРАЛ об электронной торговле»
  - https://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

- «Типовой закон ЮНСИТРАЛ о международных кредитовых переводах»
  - https://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf

- «Конвенция Организации Объединенных Наций против коррупции»
  - http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

- «Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ»
  - http://www.unodc.org/pdf/convention_1988_en.pdf

- «Конвенция Организации Объединенных Наций против транснациональной организованной преступности»
  - http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

- «Комплексное исследование УНП ООН по киберпреступности»
  - Подготовлено УНП ООН для рассмотрения Межправительственной экспертной группой по проведению всестороннего исследования проблем киберпреступности в соответствии с методологией, согласованной в рамках этой экспертной группы.
  - http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

- «Руководство УНП ООН по международному сотрудничеству с целью конфискации доходов, полученных преступным путем»
  - https://www.unodc.org/documents/organized-crime/Publications/Confiscation_Manual_Ebook_E.pdf

- «Инструментарий УНП ООН по борьбе с торговлей людьми»
  - http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf

- «Обзор конвенций ООН и других международных стандартов, касающихся борьбы с отмыванием денег и противодействия финансированию терроризма»
  - http://www.imolin.org/pdf/overview_of_UN_conventions_2013.pdf

Международные, региональные и национальные источники

- **Азиатский банк развития**

  - «Руководство по противодействию легализации преступных доходов и финансированию терроризма»
    - https://www.unodc.org/tldb/pdf/Asian-bank-guide.pdf

- **Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ)**

  - «Виртуальные валюты – ключевые определения и потенциальные риски в сфере ПОД/ФТ»
    - http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html

  - «Руководство по финансовым расследованиям: оперативные вопросы»
    - http://www.fatf-gafi.org/media/fatf/documents/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf

- «Руководство по риск-ориентированному подходу к предоплаченным картам, мобильным платежам и платежным услугам посредством Интернет»
  - http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

- «Новые способы платежей, используемые для отмывания денег»
  - http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

- «Отчет о новых способах платежей»
  - http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf

- **Европейский парламент**

  - «Директива 1999/93/ЕС Европейского парламента и Совета от 13 декабря 1999 года об основах законодательства Сообщества об электронных подписях»
    - http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31999L0093

  - «Директива 2000/31/ЕС Европейского парламента и Совета от 8 июня 2000 года о некоторых правовых аспектах услуг информационного общества, в частности, электронной торговли на внутреннем рынке»
    - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML

  - «Директива 2009/110/ЕС Европейского Парламента и Совета от 16 сентября 2009 г. об учреждении, деятельности и надзоре за деятельностью организаций, занимающихся электронными деньгами»
    - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN

- «Директива 2011/83/ЕС о правах потребителей»
  - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1

- **Европейский Центральный Банк**
  - «Схемы с использованием виртуальных валют»
    - http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

- **Комиссия по борьбе с финансовыми преступлениями (FinCEN), Министерство финансов США**
  - «Руководство: Применение предписаний FinCEN в отношении лиц, занимающихся управлением, обменом или использованием виртуальных валют»
    - http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

- **Лига арабских государств**
  - «Конвенция о преступлениях в области информационных технологий»
    - https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd

- **Международный валютный фонд**
  - «Подразделения финансовой разведки: обзор»
    - http://www.imf.org/external/pubs/ft/FIU/fiu.pdf

- **Международный союз электросвязи (МСЭ)**
  - «Инструментарий МСЭ в вопросах законодательства о борьбе с киберпреступностью»
    - http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf

- **Организация экономического сотрудничества и развития (ОЭСР)**

  - «Эффективное межведомственное сотрудничество в борьбе с налоговыми и другими финансовыми преступлениями»
    - http://www.oecd.org/ctp/crime/EffectiveInterAgencyCooperationinFightingTaxCrimes.pdf
    - http://www.oecd.org/tax/crime/effective-inter-%20agency-cooperation-report.pdf (издание второе)

- **Совет Европы**

  - «Конвенция о компьютерных преступлениях»
    - http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

  - «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками»
    - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/MONEYVAL_2012_6_Reptyp_flows_en.pdf

  - «Обучение судей и прокуроров в вопросах компьютерных преступлений: концепция»
    - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf

  - «Документ для обсуждения «Облачные вычисления и расследования киберпреступлений: территориальность против распорядительной власти?»«
    - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

  - «Электронные доказательства: базовое руководство для сотрудников полиции, прокуроров и судей»
    - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp

- «Пояснительная записка к Конвенции Совета Европы о компьютерных преступлениях»
  - http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

- «Финансовые расследования и конфискация доходов от преступной деятельности»
  - http://www.coe.int/t/dghl/cooperation/economiccrime/specialfiles/CARPO-ManualFinInv_eng.pdf

- «Судебная подготовка: вводный курс по киберпреступности и электронным доказательствам для судей и прокуроров»
  - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/basic%20training%20for%20judges/Cyber_JudTrain_Basic_course_Manual_V_1_0.pdf

- «Трудности правоохранительных органов в трансграничном получении электронных доказательств от «поставщиков облачных вычислений»»
  - http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

- «Исследование МАНИВЕЛ «Замораживание финансовых транзакций и мониторинг банковских счетов»
  - http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2013)8_Postponement.pdf

- «Специализированные подразделения по вопросам киберпреступлений – хорошая практика»
  - http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

- «Стратегические приоритеты сотрудничества в сфере борьбы с киберпреступностью в регионе Восточного партнерства»
  - http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@EAP/2523_EAP_Strat_Priorities_V7%20ENG.pdf

- «Конвенция об отмывании, выявлении, изъятии, конфискации доходов от преступной деятельности и финансировании терроризма»
  - http://conventions.coe.int/Treaty/en/Treaties/Html/141.htm

- **Содружество Независимых Государств (СНГ)**

- «Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации»
  - https://cms.unov.org/documentrepositoryindexer/GetDocInOriginalFormat.drsx?DocID=5b7de69a-730e-43ce-9623-9a103f5cabc0

- **Шанхайская организация сотрудничества**

- «Соглашение о сотрудничестве в области обеспечения международной информационной безопасности»
  - http://www.fidh.org/en/Terrorism/Agreement-Between-the-Member (неофициальный перевод)

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Приложение 2
Глоссарий

1 Глоссарий

Обращаем Ваше внимание на то, что приведенные в глоссарии определения терминов не являются официальными и применимы только в контексте данного пособия.

Административный орган/ Администратор
См. Централизованная виртуальная валюта

Арест
Применение процедур, которые запрещают передачу, преобразование, отчуждение или передвижение полученного преступным путем имущества и позволяют компетентному органу или суду осуществлять контроль в отношении такого имущества.

Биржа виртуальной валюты
Организация, предлагающая услуги по покупке или продаже, или выступающая посредником при покупке и продаже виртуальной валюты в обмен на фиатную или другие виртуальные валюты.

Виртуальная валюта
– это цифровое выражение стоимости, которое может быть предметом торгов в Интернете и функционирует в качестве (1) средства обмена; и/или (2) расчетной денежной единицы; и/или (3) средства хранения стоимости, но не обладает статусом законного платежного средства ни в одной юрисдикции.

Виртуальная машина
Программное обеспечение, позволяющее пользователю использовать операционную систему в качестве приложения на своем компьютере.

Вмешательство в данные
Криминализация вмешательства в данные преследует целью защитить целостность и надлежащее функционирование или использование данных или программ, хранящихся на компьютерах, от неправомерного повреждения, удаления, порчи, изменения или блокирования.

Вмешательство в систему
Преступление, связанное с умышленным воспрепятствованием законному использованию компьютерных систем, включая телекоммуникационное оборудование, используя или воздействуя на компьютерных данные.

Децентрализованные виртуальные валюты
– это распределенные, основанные на математических принципах пиринговые виртуальные валюты с открытым исходным кодом, которые не имеют центрального администратора и отсутствует централизованный контроль или надзор.

Дискреционное уголовное преследование
Понятие, обозначающее применение стандартов государственных интересов к конкретным уголовным делам для того, чтобы принять решение о возбуждении или продолжении уголовного преследования, или применить к преступнику альтернативные виды наказания.

Linden Dollars
Конвертируемая централизованная виртуальная валюта, предназначенная для использования онлайн в виртуальном мире Second Life.

Доходы от преступлений
Обозначают любую собственность, приобретенную или полученную прямо или косвенно в результате совершения какого-либо преступления.

Закрытая виртуальная валюта
См. Неконвертируемая виртуальная валюта

Замораживание
Временное запрещение передачи, преобразования, отчуждения или передвижения имущества. Отличается от ареста, который позволяет компетентному органу или суду осуществлять контроль в отношении соответствующего имущества.

Защита потребителей
Набор правил, направленных на защиту прав потребителей и предоставляющие им право на товары и услуги приемлемого стандарта, а также защищающие их от нечестных и несправедливых деловых практик.

Интеграция
Заключительный этап процесса отмывания денег, который представляет собой интеграцию «отмытых» средств в легальную экономику. См. также Отмывание денег, Размещение и Расслоение.

Киберпреступления
Понятие, обозначающее преступления против компьютерных данных и систем, таких как преступления против конфиденциальности, целостности и доступности данных и систем, а также преступления, совершенных с помощью компьютерных данных и систем.

Компьютерное мошенничество
Ассимилирующее преступление, которому характерны признаки традиционного мошенничества, совершенного посредством информационно-коммуникационных технологий.

Конвертируемая виртуальная валюта
Конвертируемая виртуальная валюта имеет эквивалентное значение в фиатной валюте и может быть обменена на фиатную валюту и обратно.

Криптовалюта
См. Децентрализованная виртуальная валюта

Мониторинговый ордер
Выданный компетентным органом приказ финансовому учреждению, требующей от последнего раскрытия уполномоченному лицу информации об операциях по счету, открытом в этом учреждении, или по счету, который принадлежит указанному в ордере лицу.

Неконвертируемая виртуальная валюта
Неконвертируемая виртуальная валюта предназначена для использования только в конкретном виртуальном домене или мире, таком как глобальные многопользовательские онлайновые ролевые игры (MMORPG) или Amazon, и в соответствии с регулирующими ее использование правилами не подлежит обмену на фиатные валюты.

Несанкционированный доступ
Базовое преступление, представляющее собой угрозы и атаки в отношении безопасности (то есть, конфиденциальности, целостности и доступности) компьютерных систем и данных.

Новые способы платежей
Используемое ФАТФ выражение, обозначающие предоплаченные карты, мобильные платежи и платежные услуги посредством сети Интернет.

Обмениики валют
См. Биржа виртуальной валюты

Ордер на предоставление информации
Используется правоохранительными органами, чтобы обязать лицо предоставить хранящиеся на компьютере данные или сервис-провайдера представить информацию об абоненте.

Орудия
Любое имущество, используемое или предназначенное для использования в любой форме, полностью или частично, для совершения любого уголовного преступления(-ий).

Открытая виртуальная валюта
См. конвертируемая виртуальная валюта

Отмывание денег
Процесс, посредством которого преступники маскируют происхождение и контроль над доходами от преступной деятельности, представляя такие доходы как такие, которые имеют законное происхождение.

Подразделение финансовой разведки
Специализированное ведомство государственной власти, которое получает от финансовых учреждений и других физических и юридических лиц сообщения о подозрительных операциях, анализирует их и передает результаты своего анализа в национальные правоохранительные органы и иностранные подразделения финансовой разведки с целью борьбы с отмыванием денег.

Предикатное преступление
Преступление, доходы от которого могут стать предметом преступления по отмыванию денег.

Противозаконное использование устройств
Преднамеренное совершение определенных правовых актов в отношении определенных устройств или доступ к данным с целью совершения преступлений против конфиденциальности, целостности и доступности компьютерных систем или данных.

ПФР
См. Подразделение финансовой разведки

Размещение
Первый этап процесса отмывания денег, на котором «грязные» деньги впервые размещаются в финансовой системе. См. также Отмывание денег, Расслоение и Интеграция.

Расслоение
Второй этап процесса отмывания денег, как правило, включает в себя ряд операций, цель которых – скрыть незаконное происхождение средств. См. также Отмывание денег, Размещение и Интеграция.

Данные контента
Содержание коммуникации, другими словами, суть или смысл передаваемого сообщения, или информации.

Обеспечение сохранности
Понятие, обозначающее защиту имеющихся данных от всего, что может вызывать ухудшение их текущего качества или может привести к изменению или разрушению данных. Сохранение вовсе не означает, что данные будут недоступными. Законные пользователи в зависимости от условий ордера могут иметь доступ к данным.

Технологическая нейтральность
Понятие, обозначающее, что технологии могут быть использованы как в законных, так и незаконных целях и, следовательно, основная технология не может считаться незаконной только в силу ее потенциального использования в преступных целях.

Фиатная валюта
Используемые как законное платежное средство монеты и бумажные деньги страны, которые находятся в обращении, используются и принимаются в эмитирующей их стране в качестве законного средства расчетов.

Центр по реагированию на инциденты в области компьютерной безопасности (CSIRT)
Группа специалистов, деятельность которых в основном сосредоточена на предупреждении, управлении и минимизации последствий инцидентов в сфере кибернетической безопасности.

Централизованная виртуальная валюта
Централизованные виртуальные валюты имеют единый административный орган (администратора), т.е. третью сторону, которая управляет системой. Администратор эмитирует валюту, устанавливает правила ее использования, ведет центральный платежный реестр и имеет право возврата валюты (изъятия ее из обращения). Обменный курс для конвертируемой валюты может быть либо плавающим, то есть определяться рыночным спросом и предложением на виртуальную валюту, либо твердым, то есть установленным администратором как фиксированное значение, выраженное в фиатной валюте или другом средстве сбережения из реального мира, таком как золото или валютная корзина.

Цепочка блоков
Центральный платежный реестр, используемый некоторыми типами децентрализованных виртуальных валют (например, bitcoin).

Цифровая валюта
Цифровая валюта может выступать как средство цифрового выражения либо виртуальной валюты (нефиатной валюты), либо электронных денег (фиатной валюты).

Цифровое выражение
Выражение чего-либо в виде цифровых данных. Физический объект, например, флэш-накопитель или жесткий диск компьютера могут содержать цифровое выражение виртуальной валюты, но, в конечном счете, именно цифровые данные, а не носитель, на котором они хранятся, являются виртуальной валютой.

Электронная торговля
Любая форма коммерческой операции между физическими и юридическими лицами, использующих электронную коммуникацию вместо физического обмена товаров или услуг.

Электронные деньги
являются цифровым средством выражения фиатной валюты и используются для электронного перевода стоимости (выраженной) в фиатной валюте. Электронные деньги представляют собой механизм цифрового перевода фиатной валюты, т.е. они используются для электронного перевода валюты, и обладают статусом законного платежного средства.

Электронные доказательства
Созданная, хранящаяся или передаваемая с использованием электронных устройств информация, которая может быть использована в суде.

Bitcoin
Децентрализованная пиринговая платежная система, не имеющая центрального органа или посредников, функционирование которой обеспечивается ее же пользователями.

CSIRT
См. Центр по реагированию на инциденты в области компьютерной безопасности

E-Gold
Созданная в 1996 году система виртуальной валюты, позволяющая пользователям открывать счета, деноминированные в граммах золота (или других ценных металлах) и совершать мгновенные переводы между счетами E-Gold. В 2007 ликвидирована судом США.

Е-деньги
См. Электронные деньги

Liberty Reserve
Созданная в 2006 г. и прекратившая существование в 2013 г. система виртуальной валюты, которая предоставляла своим пользователям возможность регистрироваться и переводить деньги другим пользователям, требуя для этого только имя, электронной адрес и дату рождения.

WebMoney
Созданная в 1998 г. система виртуальной валюты, которая предоставляет своим пользователям возможность контролировать имущественные права, хранящиеся другими участниками системы. На момент подготовки данного пособия WebMoney насчитывала почти 25 миллионов пользователей.

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Приложение 3
Примеры и анализ для стран ГУАМ

Данное приложение содержит краткий обзор правовых аспектов виртуальных валют в странах-участницах ГУАМ, в частности вопросов, связанных с нормативной и институциональной основами борьбы с отмыванием денег и компьютерными преступлениями. Эти вопросы организованы по соответствующим темам – общего регулирования виртуальных валют, противодействия отмыванию денег и борьбы с киберпреступностью.

1 Регулирование виртуальных валют

Ни в одном из государств ГУАМ нет нормативных актов, непосредственно регулирующих вопросы использования и обращения централизованной или децентрализованной виртуальных валют. В этом нет ничего удивительного, так как на момент подготовки данного пособия лишь небольшое количество стран во всем мире сделали первые шаги в попытке решить вопросы, поднятые виртуальными валютами. Это, однако, не означает, что отсутствие регулирования виртуальных валют освобождает от ответственности за их использование в незаконных целях, в том числе для отмывания денег. Как уже неоднократно обсуждалось в данном пособии, принципы аналогии и должная интерпретация действующих норм в сфере борьбы с отмыванием денег и киберпреступностью могут и должны быть использованы для решения проблем, связанных с использованием виртуальных валют для легализации преступных доходов.

Подобно мировым тенденциям в этой области необходимость регулирования виртуальных валют в государствах ГУАМ станет важным вопросом на повестки дня, когда число пользователей и количество транзакций с использованием виртуальных валют достигнет некого критического порога, вызывающего обеспокоенность. Однако, как видно из следующего примера, виртуальные валюты могут привлечь внимание политиков и финансовых регуляторов даже в тех случаях, когда такие условно-гипотетические пороги еще не достигнуты.

Пример: Статус bitcoin и регулирование виртуальных валют в Украине

В ответ на запрос украинского новостного ресурса AIN.UA [1] Национальный банк Украины (НБУ) опубликовал свои первые официальные рекомендации для украинского Bitcoin-сообщества.

В частности, НБУ указал, что платежная система Bitcoin и услуги платежной инфраструктуры должны быть зарегистрированы в Национальном банке Украины и должны придерживаться действующего законодательства касательно эмиссии и использования электронных денег. Вопрос о том, существует ли необходимость принимать отдельные законы для регулирования вопросов, связанных с использованием bitcoin, активно дискутируется во всем мире. Таким образом, решение использовать существующее законодательство демонстрирует индивидуальный подход Украины к проблематике bitcoin.

AIN.UA опубликовала полный текст комментария НБУ, который состоит из нескольких пунктов и содержит ссылки на действующий закон «О платежных системах и переводе средств в Украине» – основу данных рекомендаций. [2]

Согласно НБУ, ссылающегося на статью 9 вышеупомянутого закона, участники платежной системы Bitcoin, и операторы услуг Bitcoin имеют право совершать деятельность в Украине исключительно после их регистрации Национальным банком Украины.

Статья 9 также требует от провайдеров платежных услуг:

- Установить процедуру урегулирования случаев, когда они не в состоянии предоставлять услуги;
- Определить организационную структуру и порядок разрешения споров между участниками платежной системы;
- Предоставлять информацию о переводах денег с целью обеспечения защиты прав потребителей.

Также в своих рекомендациях НБУ ссылается на статью 15 этого же закона, в которой говорится, что организация, имеющая «намерение

[1] http://ain.ua/

[2] Полный текст рекомендаций в ответ на запрос AIN.UA можно найти по следующему адресу: http://ain.ua/ (только на русском).

осуществлять эмиссию электронных денег»[3], обязана до начала их эмиссии согласовать с ним правила использования электронных денег в соответствии с действующими нормативными положениями.

Предоставляя определенные правовые разъяснения для растущего сообщества операторов и пользователей виртуальных валют, чиновники НБУ следуют примеру других европейских стран, которые опубликовали официальные предупреждения для своих граждан относительно волатильности ценности bitcoin и недостаточности мер по защите потребителей. Как говорится в сообщении НБУ: «Мы подчеркиваем, что все риски, связанные с использованием так называемых криптовалют ... несет участник расчетов». Тем самым Украина присоединилась к другим европейским и азиатским странам, которые приняли решение повышать осведомленность пользователей о рисках виртуальных валют.[4]

2 Нормативно-правовая база противодействия отмыванию денег

Все государства ГУАМ являются участниками основных международных документов, требующих от стран предпринять усилия по предупреждению и борьбе с отмыванием денег, в том числе Конвенции ООН против организованной преступности, Конвенции ООН против коррупции, Конвенции ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ, а в региональном контексте – Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма. Страны ГУАМ также являются частью глобальной сети ФАТФ, в отношении которых осуществляется мониторинг за соблюдением международных стандартов по борьбе с отмыванием денег, финансированием терроризма и распространением оружия массового уничтожения (Стандарты ФАТФ). Аналогичным образом в европейском контексте соблюдение странами ГУАМ стандартов по борьбе с отмыванием денег обеспечивается Комитетом экспертов Совета Европы по оценке мер борьбы с отмыванием денег мер и финансированием терроризма (МАНИВЕЛ).

[3] Исходя из определений, приведенных в Модуле 1, электронные деньги в данном контексте следует понимать как такие, которые подразумевают цифровые валюты.
[4] CoinDesk, «Украина применяет действующее законодательство для регулирования операций с bitcoin» (Источник: http://www.coindesk.com/)

2.1 Материальное право

Определения термину «отмывание денег» в странах ГУАМ дано в специальных законодательных актах, принятых с целью предотвращения легализации незаконных доходов. Определения, содержащиеся в Законе Азербайджанской Республики «О предотвращении легализации денежных средств или другого имущества, полученного преступным путем, или финансирования терроризма», Законе Грузии «О содействии предотвращению легализации преступных доходов», Законе Республики Молдова «О предупреждении и борьбе с отмыванием денег и финансированием терроризма» и Законе Украины «О предотвращении и противодействии легализации (отмыванию) доходов, полученных преступным путем или финансированию терроризма», соответствуют международно-признанным определениям «отмывания денег» и могут быть использованы в случаях, связанных с незаконным использованием виртуальных валют.

С точки зрения материального уголовного права во всех станах ГУАМ криминализирована легализация доходов и средств, полученных преступным путем. Статьи 193[1] «Легализация денежных средств или другого имущества, если известно, что такие средства или другое имущество представляют собой доходы от преступлений» и 194 «Приобретение, владение, использование или распоряжение денежными средствами или иным имуществом, зная, что такие средства или иное имущество представляют собой доходы от преступлений» Уголовного кодекса Азербайджана, статьи 194 «Легализация незаконных доходов» и 194[1] «Использование, приобретение, владение или распоряжение имуществом, полученным вследствие легализации незаконных доходов» Уголовного кодекса Грузии, статья 243 «Отмывание денег» Уголовного кодекса Республики Молдова и статья 209 «Легализация (отмывание) доходов, полученных преступным денег» Уголовного кодекса Украины обеспечивают материально-правовую основу для противодействия таким преступлениям как с точки зрения необходимых элементов преступлений, так и с точки зрения применения санкций.

Ситуация разнится в отношении предикатных преступлений. Во всех странах, за исключением Украины, применяется подход, предусматривающий включение всех уголовных преступлений в категорию предикатных по отношению к отмыванию денег. Это означает, что доходы и орудия любого уголовного преступления могут быть предметом замораживания, ареста и конфискации. В случае с Украиной статья 209 Уголовного кодекса предусматривает минимальный порог санкций (преступления, наказание за которые предусматривает лишение свободы или штраф более 3000 минимальных размеров оплаты труда), а также исключения из категории предикатных преступление по уклонению от уплаты налогов (статьи 212 и 212[1] Уголовного кодекса). Если смотреть

на эту ситуацию через призму компьютерных преступлений, которые часто могут являться предикатными к отмыванию денег, совершенного посредством виртуальных валют, это не является большой проблемой, поскольку все противоправные акты, попадающие под действие Главы 16 «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи» Уголовного кодекса Украины предусматривает лишение свободы как возможной вариант наказания.

2.2 Процессуальное законодательство

Помимо общей уголовно-процессуальной основы, применяемой в расследованиях всех типов уголовных преступлений, равно как и связанные с ней процессуальные действия (такие как свидетельские показания, обыск и арест, ордер на предоставление документов и т.д.) для целей финансовых расследований отмывания денег, а также выявления и ареста незаконных доходов и орудий преступлений, используются специфические процессуальные полномочия, которые также могут быть полезными в расследованиях, связанных с использованием виртуальных валют.

В данном пособии уже рассматривался вопрос актуальности, предоставляемой национальным ПФР информации из сообщений о подозрительных операциях для целей сбора оперативных данных в уголовных расследованиях по отмыванию денег, совершенного посредством виртуальных валют. Определения «подозрительной операции» дано соответственно в статье 7 Закона Азербайджанской Республики «О предотвращении легализации денежных средств или другого имущества, полученного преступным путем, или финансирования терроризма», статье 2 (h) Закона Грузии «О содействии предотвращению легализации преступных доходов», статье 5 Закона Республики Молдова «О предупреждении и борьбе с отмыванием денег и финансированием терроризма» и статье 11 Закона Украины «О предотвращении и противодействии легализации (отмыванию) доходов, полученных преступным путем или финансированию терроризма».

Мониторинг операций как инструмент финансовых расследований в отношении отмывания денег регламентируется статьями 2-9 Закона Азербайджанской Республики «О предотвращении легализации денежных средств или другого имущества, полученного преступным путем, или финансирования терроризма», статьями 5-10 Закона Грузии «О содействии предотвращению легализации преступных доходов», статьями 4-6 Закона Республики Молдова «О предупреждении и борьбе с отмыванием денег и финансированием терроризма» и Разделом II Закона Украины «О предотвращении и противодействии легализации (отмыванию) доходов,

полученных преступным путем или финансированию терроризма». Такие процессуальные полномочия имеются у всех национальных ПФР.

Мониторинговые ордера также могут быть изданы правоохранительными органами. Статья 124^1 Уголовно-процессуального кодекса Грузии, и статья 132^4 Уголовно-процессуального кодекса Республики Молдова обеспечивают следственные органы правом мониторить финансовые операции в ходе проведения расследований. В то же время уголовно-процессуальное законодательство Украины и Азербайджана не содержит схожих возможностей для правоохранительных органов.

Требовать предоставления и раскрытия финансовой информации относится к общим полномочиям правоохранительных органов запрашивать и получать доказательства в виде документов или информации от любого государственного органа, частного или физического лица. В контексте расследований, связанных с виртуальными валютами, для получения финансовой информации могут использоваться либо специальные ордера в отношении электронных доказательств (статья 136 Уголовно-процессуального кодекса Грузии и Главы 15 Уголовно-процессуального кодекса Украины), либо общие ордера на предоставление информации (Глава XXXI Уголовно-процессуального кодекса Азербайджанской Республики, и статья 126 Уголовно-процессуального кодекса Республики Молдова).

Процедуры ареста преступных доходов или орудий преступлений в странах ГУАМ регламентируются преимущественно уголовно-процессуальным законодательством.

Статья 249 Уголовно-процессуального кодекса Азербайджанской Республики содержит перечень оснований для применения ареста незаконно полученного имущества. И хотя такой арест обычно предусматривает вовлечение судебной инстанции, в случае неотложных обстоятельств, таких как неминуемое уничтожение или потеря контроля над имуществом, обоснованное ходатайство следователя может являться правовым основания для осуществления ареста.

Статья 151 Уголовно-процессуального кодекса Грузии предусматривает исключительно судебный порядок ареста незаконно полученного имущества. Этим положением предусматривается также особая возможность применения гражданских процедур осуществления ареста при условии, что эти процедуры в целом соответствуют требованиям Уголовно-процессуального кодекса.
Статьи 203-209 Уголовно-процессуального кодекса Республики Молдова содержат перечень оснований и порядок ареста имущества, полученного незаконным путем. С этой целью в равной степени могут применяться и

судебные ордера, и процедуры ареста, осуществляемые «ex officio». Существуют также подробные положения, связанные с исполнением ордеров и управлением арестованным имуществом.

Арест незаконных доходов в Украине регламентируется Главой 17 Уголовно-процессуального кодекса в рамках общих правил, касающихся ареста имущества в рамках уголовного судопроизводства.

В случае, если для надлежащего осуществления вышеуказанных процессуальных действий возникнет необходимость в проведении экспертизы, Глава XXXV Уголовно-процессуального кодекса Азербайджанской Республики, статьи 144-146 Уголовно-процессуального кодекса Грузии, статьи 142-153 Уголовно-процессуального кодекса Республики Молдова и статьи 242-245 Уголовно-процессуального кодекса Украины могут использоваться в качестве правового основания для привлечения экспертной поддержки в рамках расследований, связанных с использованием виртуальных валют.

2.3 Институциональная основа

С точки зрения проведения расследований отмывания денег и в особенности получения доступа к финансовым разведданным ключевыми партнерами в этой связи являются подразделения финансовой разведки. Служба финансового мониторинга при Центральном банке Азербайджанской Республики, Служба финансового мониторинга Грузии, Служба по предупреждению и борьбе с отмыванием денег Национального центра по борьбе с коррупцией Республики Молдова и Служба государственного финансового мониторинга Украины располагают специальными экспертными знаниями и практическим опытом в вопросах предупреждения и (финансового) расследования отмывания денег.

Что касается ареста доходов и орудий преступлений, то соответствующими полномочиями в странах ГУАМ наделены правоохранительные органы, к компетенции которых относится проведение расследований легализации преступных доходов, а именно: Управление по борьбе с коррупцией при Генеральной прокуратуре Азербайджана, Антикоррупционный департамент Офиса главного прокурора Грузии, Служба по предупреждению и борьбе с отмыванием денег Национального центра по борьбе с коррупцией Республики Молдова и Департамент финансовых расследований Министерства налогов и сборов Украины при содействии Министерства внутренних дел и/ или Службы безопасности Украины, которые также осуществляют следственные действия.

Касательно международного сотрудничества в борьбе с отмыванием денег необходимо отметить, что ПФР всех государств-участников ГУАМ

являются членами Эгмонтской группы подразделений финансовой разведки и, следовательно, пользуются каналами обмена данными и иными возможностями по содействию проведению расследований, предоставляемой этой сетью. С другой стороны, правоохранительные органы, занимающиеся уголовными расследованиями легализации незаконных доходов, могут воспользоваться возможностями контактных пунктов 24/7 для целей сотрудничества между органами полиции в борьбе с компьютерными преступлениями, а также контактными пунктами Интерпол для получения подобной и другой помощи от органов полиции. В случаях, когда потребуется международно-правовое сотрудничество, центральные органы власти по оказанию взаимной правовой помощи в уголовных делах (в странах ГУАМ – международные отделы министерств юстиции или генеральных/ главных прокуратур в зависимости от стадии уголовного разбирательства) помогут с получением и обработкой соответствующих запросов.

3 Нормативно-правовая база противодействия компьютерным преступлениям

Все страны ГУАМ являются участницами Конвенции Совета Европы о компьютерных преступлениях 2001 г., которая является региональным договором, охватывающим вопросы криминализации компьютерных преступлений, процессуальных действий по их расследованию, институциональной основы и форм международного сотрудничества, необходимых для транснациональной борьбы с киберпреступностью. Мониторинг соответствия стран ГУАМ требованиям этой конвенции осуществляется Комитетом Конвенции Совета Европы по киберпреступности (T-CY) путем опубликования регулярных тематических отчетов.

3.1 Материальное право

Киберпреступления, которые могут являться предикатными или вспомогательными по отношению к отмыванию денег, совершенного посредством виртуальных валют, по большей части инкорпорированы в уголовное законодательство стран ГУАМ. Тем не менее, существуют некоторые различия в том, как и в какой степени в странах ГУАМ криминализированы отдельные преступления.

Преступление по несанкционированному доступу как основное преступление, несущее в себе угрозы для и атаки против безопасности (т.е. конфиденциальности, целостности и доступности) компьютерных систем и данных, полностью криминализировано в Азербайджане, Грузии и Молдове. Неправомерный доступ криминализирован статьей 271

Уголовного кодекса Азербайджанской Республики, статьей 284 Уголовного кодекса Грузии и статьей 259 Уголовного кодекса Республики Молдова соответственно. Материальное уголовное право Украины не содержит прямых аналогий.

Вмешательство в данные, преступление против целостности и надлежащего функционирования или использования компьютерных данных или компьютерных программ, такие как разрушение, удаление, порча, изменение или блокирование компьютерных данных, включены в диспозиции статьи 286 Уголовного кодекса Грузии, статьи 260^2 Уголовного кодекса Республики Молдовы и статьей 361 и 362 Уголовного кодекса Украины. В уголовном законодательстве Азербайджана не предусмотрено такого отдельного преступления как вмешательство в данные.

Аналогичным образом преступление по вмешательству в системы, означающее умышленное препятствование законному использованию компьютерных систем, включая телекоммуникационные объекты, путем использования или воздействия на компьютерные данные, является уголовным преступлением в соответствии с п.2 статьи 286 Уголовного кодекса Грузии, статьей 260^3 Уголовного кодекса Республики Молдовы и статьями 361 и 363^1 Уголовного кодекса Украины. В настоящее время уголовное законодательство Азербайджана не квалифицирует вмешательство в системы как отдельное преступление.

Неправомерное использование устройств, то есть, незаконное деяние по использованию устройств и данных для совершения преступлений против конфиденциальности, целостности и доступности компьютерных систем или данных, должным образом криминализировано во всех государствах ГУАМ. Соответствующие положения можно найти в статье 271^6 Уголовного кодекса Азербайджана, статье 285 Уголовного кодекса Грузии, статье 260^4 Уголовного кодекса Молдовы и статье 361^1 Уголовного кодекса Украины.

3.2 Процессуальные действия

Электронные доказательства являются ключевым понятием для расследования преступлений, связанных с компьютерными системами и данными, и, таким образом, представляются важными для целей расследований об отмывании денег, совершенного посредством виртуальных валют. В странах ГУАМ уголовно-процессуальное законодательство не выводит электронные доказательства в отдельную самостоятельную категорию, а рассматривает их в качестве «документов» или «информации», которые могут использоваться в качестве допустимых доказательств в уголовном судопроизводстве.

Что касается конкретных процессуальных действий в отношении расследования киберпреступлений, возможность сбора данных трафика в

режиме реального времени обеспечивается статьей 137 Уголовно-процессуального кодекса Грузии и статей 263 Уголовно-процессуального кодекса Украины. Примечательно, что такая возможность не предусмотрена уголовно-процессуальным законодательством Азербайджана и Молдовы.

Перехват данных контента направлен на ассимилирование традиционных способов снятия данных контента со средств телекоммуникации (например, телефонных переговоров) к среде информационных технологий. В странах ГУАМ процедуры перехвата данных обеспечиваются либо законами об оперативно-розыскной деятельности (Раздел 10 Закона Азербайджанской Республики «Об оперативно-розыскной деятельности» и статья 18 Закона Республики Молдова «О специальной розыскной деятельности»), либо инкорпорированы в основное уголовно-процессуальное законодательство (статья 138 Уголовно-процессуального кодекса Грузии и статьи 258 и 264 Уголовно-процессуального кодекса Украины).

В отличие от этого положения об обеспечении сохранности компьютерных данных, а также о частичном раскрытии таких данных наличествует только Молдове (статья 7 Закона Республики Молдова по борьбе с киберпреступностью) и отсутствует в законодательстве других стран ГУАМ. Однако, на практике процедуры по обеспечению сохранности могут быть замещены процедурами обыска и ареста электронных доказательств в неотложных обстоятельствах, что возможно в большинстве странах ГУАМ (п.3 статьи 243 Уголовно-процессуального кодекса Азербайджанской Республики, статья 120 Уголовно-процессуального кодекса Грузии и п.4 статьи 125 Уголовно-процессуального кодекса Республики Молдова). В Украине обыск и арест возможен только на основании санкционированных судом ордеров (статья 234 Уголовно-процессуального кодекса Украины).

Ордера на предоставление информации, используемые в контексте борьбы с киберпреступностью с целью принуждения человека предоставить требуемые компьютерные данные или с целью обязать провайдера, предлагающего свои услуги на территории страны-участницы Конвенции Совета Европы о компьютерных преступлениях, представить информацию об абоненте, могут применяться в соответствии со статьей 136 Уголовно-процессуального кодекса Грузии и Главой 15 Уголовно-процессуального кодекса Украины. В Азербайджане и Молдове с тем же успехом применяются общие положения уголовно-процессуального законодательства, обязывающие лицо предоставить документы и другие доказательства (Глава XXXI Уголовно-процессуального кодекса Азербайджанской Республики, и статья 126 Уголовно-процессуального кодекса Республики Молдова).

3.3 Институциональная основа

В соответствии с требованиями Конвенции Совета Европы о борьбе с киберпреступностью расследование киберпреступлений возложено на центральные специализированные следственные подразделения по выявлению и расследованию киберпреступлений, которые среди прочего проводят предварительный анализ электронных доказательств. Во всех государствах ГУАМ такие подразделения функционируют в составе полиции.

В Азербайджане расследованием киберпреступлений занимается Департамент борьбы с преступлениями в сфере коммуникаций и информационных технологий Министерства национальной безопасности Азербайджанской Республики; в Грузии – Отдел по борьбе с киберпреступностью Главного управления уголовной полиции Министерства внутренних дел Грузии; в Молдове – Дирекция по предотвращению и борьбе с кибернетическими, информационными и транснациональными преступлениями Министерства внутренних дел Молдовы. В Украине расследование киберпреступлений отнесено к следственной компетенции Департамента по борьбе с киберпреступностью Министерства внутренних дел Украины.

Что касается международного сотрудничества по вопросам киберпреступности, то в соответствии с требованиями Конвенции Совета Европы о компьютерных преступлениях все вышеуказанные следственные подразделения имеют в своем составе контактный пункт 24/7, который и обеспечивает такое сотрудничество между органами полиции. В случаях, когда потребуется международно-правовое сотрудничество, центральные органы власти по оказанию взаимной правовой помощи в уголовных делах (в странах ГУАМ – международные отделы министерств юстиции или генеральных / главных прокуратур в зависимости от стадии уголовного разбирательства) помогут с подготовкой, получением и обработкой соответствующих запросов.

4 Выводы

В отсутствие нормативных актов, непосредственно направленных на решение вопросов незаконного использования виртуальных валют, в частности, для целей отмывания денег, государства-участницы ГУАМ должны опираться на существующие положения национального законодательства по борьбе с отмыванием денег и киберпреступностью, адаптируя их к среде виртуальных валют. Справедливости ради следует отметить, что и другие государства пока что не ввели в свое национальное законодательство такие прямые нормы в отношении виртуальных валют. Очень важно, чтобы существующие нормативные положения по борьбе с

отмыванием денег и киберпреступностью в странах ГУАМ, по крайней мере, теоретически могли применяться для решения вызовов и угроз, связанных с виртуальными валютами.

Так или иначе, на сегодняшний момент есть ряд вопросов, касающихся имплементации международных положений о борьбе с киберпреступностью в уголовное законодательство стран ГУАМ, которые необходимо решить, как с точки зрения материального, так с точки зрения и процессуального права. Несмотря на то, что киберпреступления могут быть автономными уголовными деяниями, которые не имеют отношения к отмыванию денег, актуальность проведения расследований киберпреступлений как таких, которые могут быть предикатными или вспомогательными по отношению к отмыванию денег, не раз подчеркивалось в данном пособии. Даже если такой подход остается в значительной степени нехарактерным для следственной практики в государствах ГУАМ, нельзя недооценивать наличие согласованных правовых норм, которые могут применяться для решения проблем, вызванных развитием информационных технологий.

Правильная интерпретация юридических терминов очень важна. Однако, в контексте виртуальных валют еще более важным представляется правильное понимание всеми в той или иной форме причастными государственными учреждениями и ведомствами перекрестных вопросов отмывания денег и киберпреступности. Как и в любом другом случае возникновения технически и юридически сложных ситуаций, ключом к пониманию и решению проблем, вызванных виртуальными валютами, является сотрудничество между национальными заинтересованными органами. Кроме того, принимая во внимание, что виртуальные валюты функционируют в онлайновой среде, не ограниченной национальными границами, международное сотрудничество играет и будет играть все более важную роль при расследовании отмывания денег, совершенного посредством виртуальных валют. Имея в наличии национальные ведомства, уполномоченные расследовать отмывание денег и киберпреступления, а также создав национальные контактные центры для международного сотрудничества следственных органов и предоставления взаимной правовой помощи, с институциональной точки зрения государства-участники ГУАМ имеют все предпосылки для достижения высоких результатов в результате такого сотрудничества.

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Приложение 4
Список компетентных органов в странах ГУАМ

В этом приложении представлен список соответствующих органов в странах ГУАМ, компетентных в вопросах выявления и расследования отмывания преступных доходов, совершенного посредством виртуальных валют. Список контактов приводится по странам ГУАМ в алфавитном порядке.

1 Азербайджан

Подразделение финансовой разведки

Служба финансового мониторинга при
Центральном банке Азербайджанской Республики
Пр. Бюль-Бюль, 40, AZ1014,
Баку, Азербайджан
Тел.: +994 12 598 19 46;.
Факс: +994 12 493 03 88; +994 12 493 03 67;
Эл. почта: office@fiu.az

Уголовные расследования по отмыванию денег

Департамент по борьбе с коррупцией
Генеральная прокуратура Азербайджанской Республики
Ул. Каверочкина, 30A, AZ1007
Баку, Азербайджан
Тел.: +994 12 441 92 52
Факс: н/д
Эл. почта: kaliyev@prosecutor.gov.az

Подразделение по изъятию преступных доходов / орудий преступлений

Департамент по борьбе с коррупцией
Генеральная прокуратура Азербайджанской Республики
Ул. Каверочкина, 30A, AZ1007
Баку, Азербайджан
Тел.: +994 12 441 92 52
Факс: н/д
Эл. почта: kaliyev@prosecutor.gov.az

Прокуратура

Генеральная прокуратура Азербайджанской Республики
Ул. Нигяр Рафибейли, 7, AZ1001
Баку, Азербайджан

Тел.: +994 12 492 55 40
Факс: н/д
Эл. почта: info@prosecutor.gov.az

Национальный контакт в вопросах взаимной правовой помощи

На стадии досудебного рассмотрения дел:
Международно-правовой департамент
Генеральная прокуратура Азербайджанской Республики
Ул. Нигяр Рафибейли, 7, AZ1001
Баку, Азербайджан
Тел.: + 99 41) 492 61 98; + 994 12 492 17 70; + 994 12 492 87 51
Факс: + 99 412 493 00 20
Эл. почта: intlaw@azeri.com

На стадии судебного рассмотрения дел:
Департамент международного сотрудничества
Министерство юстиции Азербайджанской Республики
Пр. Иншаатчылар, 1, AZ1073
Баку, Азербайджан
Тел.: +994 12 430 01 67
Факс: +994 12 510 29 40
Эл. почта: international@justice.gov.az

Подразделение по вопросам киберпреступлений / высокотехнологичных преступлений

Департамент по борьбе с преступлениями в сфере коммуникации и информационных технологий
Министерство национальной безопасности Азербайджанской Республики
Парламентский пр., 2, AZ1006
Баку, Азербайджан
Тел.: +994 12 493 76 22
Факс: +994 12 493 76 22
Эл. почта: secretoffice@mns.gov.az

Контактный пункт 24/7 в соответствии с Конвенцией о компьютерных преступлениях

Департамент по борьбе с преступлениями в сфере коммуникации и информационных технологий
Министерство национальной безопасности Азербайджанской Республики
Парламентский пр., 2, AZ1006
Баку, Азербайджан
Тел.: +99 412 493 76 22

Факс: +99 412 493 76 22
Эл. почта: secretoffice@mns.gov.az

Контактный пункт Интерпол

Бюро Интерпол в Азербайджанской Республике
Фирдоуси Мамедов, 4, Нариманов, AZ1008
Баку, Азербайджан
Тел.: +994 12 498 09 23, +994 12 590 99 26
Факс: +994 12 598 37 77
Эл. почта: н/д

Центр по реагированию на инциденты в области компьютерной безопасности (CSIRT)

CERT-AZ
Переулок Дрогал, Блок 702, AZ1010
Тел.: +994 12 493 20 57
Эл. почта: reports@cert.az

Служба по защите персональных данных

Уполномоченный по правам человека (омбудсмен)
Ул. У. Гаджибекова, 40, Дом Правительства, дверь II, AZ 1000
Баку, Азербайджан
Тел.: +994 12 498 23 65
Факс: +994 12 498 23 65
Эл. почта: ombudsman@ombudsman.gov.az

2 Грузия

Подразделение финансовой разведки

Служба финансового мониторинга Грузии
Ул. Санапиро, 2, 0105 Тбилиси, Грузия
Тел.: +995 32 229 67 00
Факс: +995 32 229 67 00
Эл. почта: info@fms.gov.ge

Уголовные расследования по отмыванию денег

Антикоррупционный департамент
Офис главного прокурора Грузии
Ул. Горгасали, 24, 0114 Тбилиси, Грузия
Тел.: +995 32 240 51 36
Факс: н/д
Эл. почта: btkhelidze@justice.gov.ge

Подразделение по изъятию преступных доходов / орудий преступлений

Антикоррупционный департамент
Офис главного прокурора Грузии
Ул. Горгасали, 24, 0114 Тбилиси, Грузия
Тел.: +995 32 240 51 36
Факс: н/д
Эл. почта: btkhelidze@justice.gov.ge

Прокуратура

Антикоррупционный департамент
Офис главного прокурора Грузии
Ул. Горгасали, 24, 0114 Тбилиси, Грузия
Тел.: +995 32 240 51 36
Факс: н/д
Эл. почта: presscenter@pog.gov.ge

Национальный контакт в вопросах взаимной правовой помощи

На стадии досудебного и судебного рассмотрения дел:
Международно-правовой департамент
Офис главного прокурора, по делегированным полномочиям
Министерства юстиции Грузии
Ул. Горгасали, 24, 0114 Тбилиси, Грузия

Тел: + 995 32 240 51 43
Факс: + 995 32 240 51 42
Эл. почта: ichilingarashvili@justice.gov.ge

Подразделение по вопросам киберпреступлений / высокотехнологичных преступлений

Отдел по борьбе с киберпреступностью
Главное управление уголовной полиции
Министерство внутренних дел Грузии
Кахетинское шоссе, 38, 0135 Тбилиси, Грузия
Тел.: +995 32 241 87 59
Факс: +995 32 241 87 76
Эл. почта: international@mia.gov.ge

Контактный пункт 24/7 в соответствии с Конвенцией о компьютерных преступлениях

Отдел по борьбе с киберпреступностью
Главное управление уголовной полиции
Министерство внутренних дел Грузии
Кахетинское шоссе, 38, 0135 Тбилиси, Грузия
Тел.: +995 32 241 87 59
Факс: +995 32 241 87 76
Эл. почта: datogabekhadze@mia.gov.ge

Контактный пункт Интерпол

Национальное центральное бюро Интерпол
Министерство внутренних дел Грузии
Кахетинское шоссе, 38, 0135 Тбилиси, Грузия
Тел.: +995 32 241 13 98
Факс: +995 32 241 13 98
Эл. почта: interpol@mia.gov.ge

Центр по реагированию на инциденты в области компьютерной безопасности (CSIRT)

CERT-GOV-GE
Агентство по обмену данными
Министерство юстиции Грузии
Ул. Св. Николая, 2, 0102 Тбилиси, Грузия
Тел.: +995 32 291 51 40
Факс: +995 32 291 51 40
Эл. почта: cert@dea.gov.ge

Служба по защите персональных данных

Бюро по защите персональных данных
Ул. Апакидзе, 15, 0102 Тбилиси, Грузия
Тел.: +995 32 242 1000
Факс: н/д
Эл. почта: office@pdp.ge

3 Молдова

Подразделение финансовой разведки

Служба по предупреждению и борьбе с отмыванием денег
Национальный центр по борьбе с коррупцией
Ул. Штефан чел Маре, 198,
2004 Кишинев, Молдова
Тел.: +373 22 257 317
Факс: +373 22 257 317
Эл. почта: spcsb@cna.md

Уголовные расследования по отмыванию денег

Служба по предупреждению и борьбе с отмыванием денег
Национальный центр по борьбе с коррупцией
Ул. Штефан чел Маре, 198,
2004 Кишинев, Молдова
Тел.: +373 22 257 317
Факс: +373 22 257 317
Эл. почта: spcsb@cna.md

Подразделение по изъятию преступных доходов / орудий преступлений

Служба по предупреждению и борьбе с отмыванием денег
Национальный центр по борьбе с коррупцией
Ул. Штефан чел Маре, 198,
2004 Кишинев, Молдова
Тел.: +373 22 257 317
Факс: +373 22 257 317
Эл. почта: spcsb@cna.md

Прокуратура

Генеральная прокуратура Республики Молдова
Ул. Банулеску-Бодони, 26,
2005 Кишинев, Молдова
Тел.: +373 212 042, +373 212 348
Факс: н/д
Эл. почта: proc-gen@gov.md

Национальный контакт в вопросах взаимной правовой помощи

На стадии досудебного рассмотрения дел:
Международно-правовой департамент
Генеральная прокуратура Республики Молдова
Ул. Банулеску-Бодони, 26
2005 Кишинев, Молдова
Тел: +373 22 221 470; + 373 22 225 589; + 373 22 221 335
Факс: + 373 22 221 335
Эл. почта: proc-gen@gov.md

На стадии судебного рассмотрения дел:
Международно-правовой департамент
Министерство юстиции Республики Молдова
Ул. 31 августа 1989, 82,
2012 Кишинев, Молдова
Тел: + 373 22 201 438; +373 22 201 455
Факс: + 373 22 201 410
Эл. почта: sirku@justice.gov.md

Подразделение по вопросам киберпреступлений / высокотехнологичных преступлений

Дирекция по предотвращению и борьбе с кибернетическими, информационными и транснациональными преступлениями
Министерство внутренних дел Молдовы
Ул. Букурией, 14
2004 Кишинев, Молдова
Тел: +373 22 577 216
Факс: н/д
Эл. почта: lurdan-ana@mail.ru

Контактный пункт 24/7 в соответствии с Конвенцией о компьютерных преступлениях

Дирекция по предотвращению и борьбе с кибернетическими, информационными и транснациональными преступлениями
Министерство внутренних дел Молдовы
Ул. Букурией, 14
2004 Кишинев, Молдова
Тел: +373 22 577 216
Факс: н/д
Эл. почта: Iurdan-ana@mail.ru

Контактный пункт Интерпол

Национальное центральное бюро Интерпол
Центр международного сотрудничества органов полиции
Министерство внутренних дел Молдовы
Ул. Штефан чел Маре, 75
2004 Кишинев, Молдова
Тел: +373 22 255 404
Факс: н/д
Эл. почта: igp@mai.gov.md

Центр по реагированию на инциденты в области компьютерной безопасности (CSIRT)

Центр компьютерной безопасности CERT-GOV-MD
Центр специальных телекоммуникаций
Государственная канцелярия Республики Молдова
Пл. Великого Национального Собрания, 1
2033 Кишинев, Молдова
Тел: +373 22 820 900
Факс: +373 22 250 522
Эл. почта: info@cert.gov.md

Служба по защите персональных данных

Национальный центр по защите персональных данных
Ул. Сергея Лазо, 48
2004 Кишинев, Молдова
Тел: +373 22 820 801
Факс: +373 22 820 807
Эл. почта: centru@datepersonale.md

4 Украина

Подразделение финансовой разведки

Государственная служба финансового мониторинга Украины
Министерство финансов Украины
Ул. Белорусская, 24
04655 Киев, Украина
Тел: +38 044 594 16 52
Факс: +38 044 594 16 52
Эл. почта: sdfm@sdfm.gov.ua

Уголовные расследования по отмыванию денег

Главное управление финансовых расследований
Министерство доходов и сборов Украины
Львовская пл., 8
04655 Киев, Украина
Тел: +38 044 247 34 99
Факс: +38 044 247 36 03
Эл. почта: Kabmin_doc@minrd.gov.ua

Отдел по борьбе с легализацией доходов организованных групп и преступных организаций
Министерство внутренних дел Украины
Ул. Богомольца, 10
01601 Киев, Украина
Тел: +38 044 256 03 33
Факс: +38 044 256 16 33
Эл. почта: н/д

Подразделение по изъятию преступных доходов / орудий преступлений

Главное управление финансовых расследований
Министерство доходов и сборов Украины
Львовская пл., 8
04655 Киев, Украина
Тел: +38 044 247 34 99
Факс: +38 044 247 36 03
Эл. почта: Kabmin_doc@minrd.gov.ua

Прокуратура

Генеральная прокуратура Украины
Ул. Ризницкая, 13/15
01011 Киев, Украина
Тел.: +38 044 200 78 49
Факс: н/д
Эл. почта: jnt@gp.gov.ua

Национальный контакт в вопросах взаимной правовой помощи

На стадии досудебного рассмотрения дел:
Международно-правовой департамент
Ул. Ризницкая, 13/15
01011 Киев, Украина
Тел.: +38 044 200 78 84
Факс: +38 044 280 28 51
Эл. почта: indep@gp.gov.ua

На стадии судебного рассмотрения дел:
Департамент международного сотрудничества
Министерство юстиции Украины
Ул. Городецкого, 13
01001 Киев, Украина
Тел.: +38 044 279 68 79
Факс: +38 044 270 54 53
Эл. почта: itex@minjust.gov.ua

Подразделение по вопросам киберпреступлений / высокотехнологичных преступлений

Департамент по борьбе с киберпреступностью
Министерство внутренних дел Украины
Ул. Богомольца, 10
01601 Киев, Украина
Тел.: +38 044 374 37 13
Факс: +38 044 374 37 00
Эл. почта: request@cybercrime.gov.ua

Контактный пункт 24/7 в соответствии с Конвенцией о компьютерных преступлениях

Департамент по борьбе с киберпреступностью
Министерство внутренних дел Украины
Ул. Богомольца, 10

01601 Киев, Украина
Тел.: +38 044 374 37 13
Факс: +38 044 374 37 00
Эл. почта: request@cybercrime.gov.ua

Контактный пункт Интерпол

Украинское бюро Интерпол
Министерство внутренних дел Украины
Ул. Богомольца, 10
01601 Киев, Украина
Тел.: +380 44 256 12 53
Факс: +380 44 226 20 57
Эл. почта: interpol@mvs.gov.ua

Центр по реагированию на инциденты в области компьютерной безопасности (CSIRT)

CERT-UA
Государственная служба специальной связи и защиты информации Украины
Ул. Мельникова, 83б, корп. 2
04119 Киев, Украина
Тел: +380 44 281 88 25
Факс: +380 44 489 31 33
Эл. почта: cert@cert.gov.ua

Служба по защите персональных данных

Государственная служба по защите персональных данных
Ул. Марины Расковой, 15
02660 Киев, Украина
Тел.: +38 044 517 68 00
Факс: +38 044 517 68 00
Эл. почта: info@zpd.gov.ua

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности

Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют

Приложение 5
Примеры ответов на вопросы для самооценки

В этом приложении приведены примеры ответов на вопросы для самооценки, поставленных в конце каждого модуля настоящего пособия. Образцы ответов содержат перечень ключевых моментов, которые должны быть отражены, отвечая на вопрос.

1 Модуль 1: Знакомство с виртуальными валютами

Вопрос 1: Используя терминологию ФАТФ, дайте определение «виртуальной валюте», «электронным деньгам» и «цифровой валюте», четко объясняя разницу между ними.

- Приведенные ниже определения используются ФАТФ. Существуют и другие определения.
- Определение термина «виртуальная валюта»:
  «Виртуальная валюта представляет собой цифровое выражение стоимости, которым можно торговать в цифровой форме и которое функционирует в качестве (1) средства обмена; и/или (2) расчётной денежной единицы; и/или (3) средства хранения стоимости, но не обладает статусом законного платёжного средства ни в одной юрисдикции».
- Разъяснение термина «цифровая форма» в контексте приведенного выше определения.
- Определение термина «электронные деньги»:
  «Ее [виртуальную валюту] следует отличать от электронных денег, которые являются цифровым выражением фиатной валюты и используются для электронного перевода стоимости, выраженной в фиатной валюте. Электронные деньги представляют собой механизм цифрового перевода фиатной валюты, т.е. они используются для электронного перевода валюты, обладающей статусом законного платежного средства».
- Определение термина «цифровая валюта»:
  «Цифровая валюта может выступать цифровым выражением как виртуальной валюты (нефиатной валюты), так и электронных денег (фиатной валюты) ...»

Вопрос 2: Опишите характеристики, отличающие конвертируемую виртуальную валюту от неконвертируемой. Приведите пример для каждой категории.

- Определения конвертируемой/ открытой виртуальной валюты и неконвертируемой/закрытой виртуальной валюты.
- Приведите примеры конвертируемых и неконвертируемых виртуальных валют.

    - Конвертируемые: Bitcoin, WebMoney, Second Life Linden Dollars
    - Неконвертируемые: World of Warcraft Gold
- Обратите внимание, что вторичная торговля неконвертируемыми виртуальными валютами также существует.
- Упомяните о том, что «конвертируемые / неконвертируемые» не является главной категоризацией виртуальных валют с следственной точки зрения в связи с тем, что вторичная торговля виртуальными валютами делает многие *де-юре* неконвертируемые виртуальные валюты *де-факто* конвертируемыми виртуальными валютами.

Вопрос 3: Опишите особенности, отличающие централизованную виртуальную валюту от децентрализованной. Приведите примеры для каждой категории.

- Определения централизованной и децентрализованной виртуальной валюты.
- Дайте краткое описание особенностей, централизованных и децентрализованных виртуальных валют
    - Централизованные: центральный администратор контролирует валюту
    - Децентрализованные: распределенные, с открытым исходным кодом, на математической основе, пиринговые виртуальные валюты, не имеют центрального контроля или надзора
- Приведите примеры централизованных и децентрализованных виртуальных валют
    - Централизованные: Second Life Linden Dollars, PerfectMoney, WebMoney and World of Warcraft Gold
    - Децентрализованные: Bitcoin, LiteCoin, Ripple

Вопрос 4: Разбираясь в вопросах о виртуальных валютах важно понимать интерфейс между виртуальными валютами и традиционной финансовой системой. В этой связи расскажите о роли, которую играют биржи виртуальных валют, делая, в частности, акцент на возможных источниках финансирования (способах оплаты), которые могут быть использованы для приобретения виртуальных валют.

- Обмен фиатной валюты на виртуальную обычно происходит на бирже виртуальной валюты.
- Возможны разнообразные источники финансирования, в том числе другие виртуальные валюты, банковские и денежные переводы, кредитные карты, наличные, а также платежи посредством Интернет, например, PayPal.

- Существуют и другие современные модели покупки виртуальной валюты, такие как покупка при помощи SMS (текстовых сообщений).
- Недостаток регулирования торговли виртуальными валютами несет в себе риски ненадлежащего определения источников финансирования, используемых для их покупки.

Вопрос 5: Помимо бирж виртуальных валют приведите еще три примера интерфейса между традиционной финансовой системой и виртуальными валютами, важные с точки зрения легализации преступных доходов посредством виртуальных валют.

- Наличные деньги
    - Наличные деньги всегда были привлекательны для целей отмывания преступных доходов.
    - Растущая в последнее время популярность виртуальных валют, особенно bitcoin, означает появление новых бизнес-моделей.
    - Например, наличие в ряде стран Bitcoin-банкоматов.
    - Существуют также биржи виртуальных валют, предоставляющие возможность покупки bitcoin за наличные деньги.
- Платежные карты
    - Предоплаченные карты могут выступать в качестве альтернативы различным традиционным банковским продуктам, включая возможность совершать и принимать платежи от третьих лиц, трансграничные переводы и т.д.
    - Платежные карты могут быть источником финансирования для виртуальных валют.
    - Предоплаченные карты также могут обеспечивать абсолютную анонимность.
- Провайдеры услуг денежных переводов
    - Предыдущие исследования свидетельствуют о том, что использование провайдеров услуг денежных переводов является обычной техникой для целей отмывания преступных доходов, в частности, полученных от киберпреступлений.
    - Провайдеры услуг денежных переводов могут быть использованы для отмывания денег с использованием виртуальных валют через счета мулов.
    - Существуют также биржи виртуальных валют, непосредственно принимающие денежные переводы для покупки виртуальной валюты.

Вопрос 6: Назовите причины, почему некоторые виртуальные валюты являются привлекательным средством оплаты для законных предпринимателей.

- После подтверждения сделки с bitcoin являются невозвратными. Поэтому нет возможностей для возвратных платежей или других рисков мошенничества, которые возможны с платежными картами.
- Комиссия по операциям с bitcoin меньше комиссии по операциям с использованием платежных карт.
- Появилась и развивается целая система услуг, нацеленная на содействие бизнесу в проведении платежей с bitcoin.

Вопрос 7: Объясните, что такое криптовалюта.

- Криптовалюта – это виртуальная валюта, опирающаяся на принципы криптографии с целью обеспечения надежности и целостности.
- Например, bitcoin являются конвертируемой децентрализованной виртуальной валютой и криптовалютой в то же время.
- Криптовалюты обычно предполагают использование и распространение открытого платежного реестра. Целостность и хронологический порядок операций в реестре обеспечивается криптографией.

Вопрос 8: Объясните, как функционирует сеть Bitcoin, обращая особое внимание на цели майнинга.

- В основе функционирования сети Bitcoin лежит центральный платежный реестр, известный как цепочка блоков. Реестр содержит информацию обо всех когда-либо выполненных операциях и используется для проверки легитимности транзакций.
- Bitcoin-адрес является уникальным идентифицирующим значением, используемым для обозначения принадлежности конкретных bitcoin.
- Для перечисления bitcoin от лица «А» лицу «В» в сеть Bitcoin поступает сообщение, содержащее адрес отправителя, адрес получателя (его «получающий адрес») и сумму передаваемых bitcoin. Каждый узел сети Bitcoin, получивший такое сообщение, обновляет свою версию реестра, а затем передает сообщение об операции другим узлам.
- Транзакции собираются в группы, известные как блоки. В свою очередь блоки формируют цепочку блоков.
- Транзакции, собранные в одном блоке, считаются такими, которые происходили в одно время.

- Блоки выстраиваются так, что каждый последующий блок в цепочке связан с предыдущим.
- Процесс построения блоков и добавления их в цепочку, как описано выше, называется майнингом.
- Каждый, кто создаст блок и добавит его в цепочку, получает вознаграждение, составляющее в настоящее время 25 bitcoin.
- Каждые четыре года вознаграждение за майнинг уменьшается вполовину и так будет до тех пор, пока эмиссия bitcoin не прекратится.
- Общий объем эмиссии не превысит 21 млн. bitcoin.
- Bitcoin делятся на более мелкие части, называемые satoshi.
- Помимо вознаграждения за создание новых блоков майнеры имеют возможность получать комиссию, которая по желанию может быть включена в транзакцию.
- Как правило, майнинг осуществляется не отдельными лицами, а организованными группами майнеров, известные как пулы. Полученное вознаграждение распределяется между членами пула пропорционально количеству затраченных каждым майнером усилий по вычислению блоков.

Вопрос 9: Расскажите, каким образом в сети Bitcoin предотвращается возможность «двойной траты».

- В основе функционирования сети Bitcoin лежит центральный платежный реестр, известный как цепочка блоков. Реестр содержит информацию обо всех когда-либо выполненных операциях и используется для проверки легитимности транзакций.
- Bitcoin-адрес является уникальным идентифицирующим значением, используемым для обозначения принадлежности конкретных bitcoin.
- Двойная трата является большой проблемой для одноранговых сетей, таких как Bitcoin, потому что нет никакой гарантии, что порядок, в котором какой-либо отдельно взятый узел в сети получает уведомление о проведении транзакций, представляет собой действительный хронологический порядок, в котором они были проведены.
- Проблема может быть сформулирована следующим образом: что может помешать лицу «А», создавая сообщение об отправке bitcoin лицу «В», одновременно создать другое сообщение об отправке bitcoin кому-то еще, и, таким образом дважды потратить одни и те же bitcoin?
- Ключевым технологическим преимуществом сети Bitcoin является метод, с помощью которого эта проблема решается.
- Транзакции собираются в группы, известные как блоки. В свою очередь блоки формируют цепочку блоков.

- Транзакции, собранные в одном блоке, считаются такими, которые происходили в одно время.
- Блоки выстраиваются так, что каждый последующий блок в цепочке связан с предыдущим.
- Транзакции, которые не определены в блок, называются неподтвержденными.
- Любой узел в сети может собрать неподтвержденные транзакции, сгруппировать их и предложить в качестве следующего блока в цепочке.
- Предлагаемый блок должен содержать решение сложной математической задачи, которую трудно решить. Сеть Bitcoin динамически регулирует трудность математической задачи таким образом, чтобы каждый новый блок добавлялся в цепь в среднем раз в десять минут.
- Может случиться, хоть вероятность очень мала, что несколько узлов в сети Bitcoin предложат блоки приблизительно в одно время.
- В таком случае с добавлением различными узлами разных блоков, цепочка блоков временно разветвится.
- Эта ситуация разрешится, когда следующий блок добавится к цепочке.
- Новый блок будет, как уже говорилось ранее, содержать ссылку на предыдущий блок в цепочке.
- Таким образом, блок присоединится к одному из двух возможных ответвлений в цепочке блоков, которая, соответственно, станет длиннее.
- Правило сети Bitcoin гласит о том, что узлы должны переключаться на самую длинную из доступных ветвей. В результате очень быстро цепочка блоков стабилизируется, и все узлы согласятся по всем блокам, которые находились в стороне от конца цепочки.

Вопрос 10: Объясните, как пользователь сети Bitcoin может доказать другому пользователю свое право собственности на определенное количество bitcoin.

- В основе функционирования сети Bitcoin лежит центральный платежный реестр, известный как цепочка блоков. Реестр содержит информацию обо всех когда-либо выполненных операциях и используется для проверки легитимности транзакций.
- Bitcoin-адрес является уникальным идентифицирующим значением, используемым для обозначения принадлежности конкретных bitcoin.
- Для того чтобы сгенерировать легитимное сообщение о передаче bitcoin, отправитель bitcoin должен доказать, что он является их владельцем.

- Представьте ситуацию, когда, к примеру, лицо «A» пересылает 10 bitcoin лицу «B». Для этого лицу «A» необходимо включить в сообщение ссылки на предыдущие транзакции, вследствие которых ним было получено более 10 bitcoin. Они обозначаются как «входы» транзакции.
- Помните, что каждый пользователь сети Bitcoin имеет копию платежного реестра («цепочку блоков»), в котором содержится история всех предыдущих транзакций.
- При помощи цепочки блоков лицо «B» может легко удостовериться, что bitcoin, на которые идет ссылка в сообщении, на самом деле принадлежат лицу «A».

Вопрос 11: Опишите взаимосвязь между принципами технологической нейтральности и использованием виртуальных валют в незаконных целях.

- Принцип технологической нейтральности является одним из базовых принципов электронной торговли во всем мире. Он означает, что технологии могут использоваться как в законных, так и противозаконных целях, и что сама по себе технология безобидна. Незаконное использование технологии является результатом осуществления контроля и действий человека, а значит, ответственность лежит на человеке, а не на технологии.
- И централизованные, и децентрализованные виртуальные валюты представляют собой технологию, которая в равной степени может использоваться как в законных, так и в незаконных целях.
- Правомерное использование виртуальных валют дает пользователям преимущество с точки зрения дополнительного удобства и одновременно положительно влияет на динамику роста электронной торговли.
- С другой стороны, незаконное использование виртуальных валют может предполагать использование технологии для совершения преступлений, таких как мошенничество и отмывание денег или других преступлений аналогичного характера, а также для перемещения и сокрытия незаконных доходов.
- Исходя из принципа технологической нейтральности, виртуальные валюты «невиновны» в их незаконном использовании отдельными пользователями, что, таким образом, исключает логику запрета такой технологии из-за ее возможного использования в преступных целях.

Вопрос 12: Опишите возможную привлекательность криптовалют для целей отмывания денег.

- В сущности, необходимо учитывать отличительные особенности виртуальных валют, которые могут быть использованы в целях совершения преступлений или сокрытия доходов от преступлений.
- Криптовалюты обращаются вне финансовых учреждений. Другим словами, эти виртуальные валюты обходятся без использования общепринятых, специально созданных и, таким образом, тщательно регулируемых и контролируемых каналов финансовых операций, что обеспечивает большую степень сокрытия от внимания учреждений, осуществляющих контроль в сфере противодействия отмыванию денег.
- Криптовалюты обеспечивают анонимность операций: после того как виртуальная валюта, например, bitcoin, зачислен в определенный кошелек, дальнейшие операции с ним в цепочке блоков (единый онлайновый реестр платежей сети Bitcoin) могут быть анонимизированы, что исключает возможность отследить реальных владельцев валютных кошельков.
- Криптовалюты полагаются на криптографию – значение привязано к распределенной сети вычислений, выполняемых майнерами для решения криптографической задачи. Это также дополнительно усложняет возможность отслеживания и установления фактов незаконного использования виртуальных валют.

Вопрос 13: В чем разница между преступлениями против конфиденциальности, целостности и доступности компьютерных данных / систем и преступлениями, связанных с данными контента?

- Преступления против конфиденциальности, целостности и доступности компьютерных систем и данных обозначают действия, направленные против нормальной работы компьютерных систем или данных, хранящихся в таких системах, и включают в себя такие преступления:
    - Неправомерный доступ;
    - Незаконный перехват;
    - Вмешательство в данные;
    - Вмешательство в систему; и
    - Неправомерное использование устройств.
- В отличие от преступлений против конфиденциальности, целостности и доступности компьютерных систем и данных, преступления, связанные с данными контента, могут означать любое уголовное преступление, совершенное с использованием информационных технологий и/или в значительной степени

отягощенное использованием такой технологии. Одним из таких примеров является компьютерное мошенничество, обозначающее традиционные элементы мошенничества в сочетании с использованием компьютерных систем и данных.

Вопрос 14: Назовите, по крайней мере, две страны, которые запретили или ограничили использование bitcoin, и дайте подробные объяснения причинам таких решений.

- На данный момент Китай и Канада приняли решение, соответственно запретить или ограничить использование bitcoin в своих финансовых/ банковских системах. Дополнительные поиски по данному вопросу могут пополнить этот список Россией и Данией.
- Оба из вышеуказанных государств сослались на более или менее общие причины для ограничения/ запрещения использования bitcoin в своих финансовых/ банковских системах. По большей части эти причины связаны с предполагаемыми рисками отмывания денег, а также, в некоторой степени, с волатильностью и спекулятивным характером криптовалют.
- Правильный вывод из этих двух примеров состоит в том, что bitcoin не запрещены в строгом смысле этого слова, а скорее им временно отказано в признании в силу некоторых особенностей виртуальных валют, которые повышают риски отмывания денег и финансовой стабильности.

2 Модуль 2: Проблемы, связанные с виртуальными валютами

Вопрос 1: Опишите угрозы, связанные с виртуальными валютами, которые делают их привлекательными для целей отмывания преступных доходов.

- Быстрые и невозвратные транзакции
  - Скорость операций, в частности, скорость, с которой средства могут быть сняты или конвертированы увеличивает сложность осуществления мониторинга, а также добавляет трудностей при попытке заморозить средства.
  - Возможность отмены операций зависит от конкретной виртуальной валют. К примеру, операции с bitcoin не могут быть отменены.
- Анонимность
  - Характерна, в первую очередь, для децентрализованных виртуальных валют. Впрочем, не все децентрализованные виртуальные валюты создаются для обеспечения анонимности.
  - Информация о совершении транзакции – доступна, а информация о связях транзакций с реальными людьми – нет.
  - В случае с централизованными виртуальными валютами возможно получить информацию об участниках транзакции либо от бирж виртуальных валют, либо от центральных администраторов.
- Недостаточные данные об операциях
  - Центральные администраторы и биржи виртуальных валют могут хранить данные о транзакциях и их участниках.
  - Однако, обычно не существует юридически закрепленного обязательства администраторам и биржам виртуальных валют собирать и хранить такие данные, поэтому их качество и точность может варьироваться.
  - Возможен как преднамеренный, так и непреднамеренный недостаточный сбор, и учет данных.
- Установление фактов использования виртуальных валют
  - Относительно слабая изученность виртуальных валют (в сравнении с наличными деньгами, платежными картами и пр.)
  - Поэтому осознание того, что использовались виртуальные валюты, может создать проблему.
  - Для выявления отмывания денег, совершенного посредством виртуальных валют, необходима соответствующая правовая база.

- Сложные / запутанные модели транзакций

  - Отсутствие связи между счетами в виртуальных валютах и реальными людьми.
  - Возможность создания неограниченного количества счетов.
  - Вышеуказанные факторы могут быть использованы для создания новых сложных схем операций.
- Отсутствие ограничений по сумме
  - В случае с централизованными виртуальными валютами администратор имеет возможность ввести ограничение по максимальной сумме. Однако, это, как правило, связано с профилактикой мошенничества.
  - Транзакции с децентрализованными виртуальными валютами, как правило, не имеют ограничений по сумме.

Вопрос 2: Расскажите, как преступники используют заочную природу виртуальных валют для отмывания преступных доходов.

- Большинство операций с виртуальными валютами предполагают минимальный или не предполагают вообще контакт «лицом к лицу». Такое положение вещей способствует тому, что виртуальные валюты используются преступниками для отмывания денег.
- Одна категория случаев использования виртуальных валют в криминальных целях включает в себя сценарий, при котором преступники получают контроль над счетами законных пользователей и возможность осуществлять по ним операции.
- Известно о двух возможных ситуациях, ранее имевших место:
  «В ряде случаев продукты, связанные с новыми способами платежей, использовались для отмывания незаконных доходов после хищения персональных данных или кражи денег с банковских счетов или кредитных / дебетовых карт посредством взлома компьютерных сетей или «фишигна». Поскольку банковские счета или кредитные и дебетовые карты были изначально открыты на имя законных клиентов, преступники могли использовать их в качестве счетов, с которых будут поступать деньги для размещения средств на предоплаченные карты или счета, или использовался для осуществления Интернет-платежей. В этих случаях провайдеры НСП не могли установить, что операции проводились не их законными клиентами, а также не могли выявить никакой другой подозрительной деятельности.»
  «В других случаях украденные или поддельные персональные данные использовались для открытия счетов НСП, которые также использовались в качестве транзитных счетов для отмывания незаконных доходов, либо для одновременного совершения преступлений (например, мошенничества) и отмывания денег.»

- Вторая категория случаев использования заочной природы счетов НПМ связана с использованием анонимного характера некоторых из таких услуг.
  «В некоторых юрисдикциях электронные платежи осуществляются анонимно. Также необходимо отметить, что оборот электронных денег осуществляется вне банков и, как результат, вне банковской системы надзора. Банки выступают в качестве агентов, которые вводят деньги в электронную платежную систему или выводят их из нее, а в некоторых случаях как эмитенты электронных денег.»

Вопрос 3: Объясните, почему регуляторные и надзорные угрозы, связанные с администраторами централизованных виртуальных валют, представляют собой риски отмывания денег.

- Требования к финансовым учреждениям о регулировании и соответствии лучшим практикам в сфере противодействия отмыванию денег хорошо известны.
- Исходя из используемой ФАТФ терминологии, провайдеры централизованных виртуальных валют подпадают под определение «финансовые учреждения».
- В случае децентрализованных виртуальных валют не существует финансовых учреждений, которые предоставляли бы услуги перевода денег или стоимости. Тем не менее, услуги перевода стоимости существуют.
- Требуется соответствующая законодательная база для регулирования виртуальных валют.
- Внедрение надзора, в особенности в отношении систем децентрализованных виртуальных валют, представляет собой значительные практические сложности.

Вопрос 4: Перечислите следственные трудности, которые скрывают в себе виртуальные валюты, и предложите возможные пути их решения.

- Недостаток знаний
  - Знания следователей и прокуроров о существовании и возможностях виртуальных валют, а также об инструментах и методах эффективного проведения расследований преступлений, совершенных посредством виртуальных валют, ограничены.
- Ставка на электронные доказательства
  - Большинство доказательств, касающиеся виртуальных валют, вероятно, будут электронными.
  - Электронные доказательства требуют должного обращения. Они должны быть аутентичными, допустимыми и иметь отношение к делу.

  - Может оказаться непростым делом найти электронные доказательства, и потребуются специальные инструменты и знания для их сбора и анализа.
  - Электронные доказательства могут быть крайне волатильными.
  - Электронные доказательства очень восприимчивы к изменениям и поэтому требуют специальной техники и условий хранения.
  - Электронные доказательства можно копировать, что может вызвать вопросы в суде с точки зрения их аутентичности.
- Пробелы в законодательстве
  - Основной проблемой в случае виртуальных валют является отсутствие должного регулирования и прямо применимых законодательных норм.
  - Необходима соответствующая законодательная база для обеспечения допустимости электронных доказательств.
- Сложности, связанные с регуляторным / надзорным режимом
  - Требования к финансовым учреждениям о регулировании и соответствии лучшим практикам в сфере противодействия отмыванию денег хорошо известны.
  - Исходя из используемой ФАТФ терминологии, провайдеры услуг централизованных виртуальных валют подпадают под определение «финансовые учреждения».
  - В случае децентрализованных виртуальных валют не существует финансовых учреждений, которые предоставляли бы услуги перевода денег или стоимости. Тем не менее, услуги перевода стоимости существуют.
  - Необходимость в соответствующей законодательной базе для регулирования виртуальных валют.
  - Внедрение надзора, в особенности в отношении систем децентрализованных виртуальных валют, представляет собой значительные практические трудности.
- Уголовное преследование и осуждение
  - Должный сбор и обращение с электронными доказательствами.
  - Правильное понимание судьями соответствующих вопросов.
- Сотрудничество на национальном уровне
  - Учитывая неурегулированный статус виртуальных валют, преступления, связанные с виртуальными валютами или являющиеся предикатными к их незаконному использованию, на практике часто могут относиться либо ни к чьей, либо к следственной компетенции сразу нескольких ведомств.
  - Сотрудничество на национальном уровне имеет важное значение для проведения криминалистической экспертизы, а также для уголовного преследования за преступления,

совершенных посредством или в отношении информационных технологий.
    - Основными партнерами являются правоохранительные органы, ПФР, подразделения по вопросам киберпреступлений и финансовые следователи.
    - Главной проблемой такого сотрудничества может оказаться то, что часто уголовные и финансовые следователи относятся к различным ведомствам, которые практикуют различные подходы для раскрытия и расследования преступлений, совершенных с использованием информационных технологий. Финансовые следователи полагаются на методы уголовного расследования, применимые к традиционным осязаемым доказательствам, в то время как подразделения по вопросам киберпреступлений полагаются на электронные доказательства.
    - Все чаще встречаются случаи сотрудничества между подразделениями по вопросам киберпреступлений и центрами по реагированию на инциденты в области компьютерной безопасности (CSIRT). CSIRT – это группа специалистов, которая играет важную роль в защите ключевой национальной информационной инфраструктуры.
    - Государственно-частное сотрудничество также важно в контексте сотрудничества на национальном уровне. Сотрудничество с провайдерами Интернет-услуг является основным источником информации о пользователях, данных трафика и других важных электронных доказательствах. Финансовые учреждения также являются важными источниками доказательств.
    - Государственно-частному сотрудничеству, среди прочего, могут препятствовать правовые (конфиденциальность данных пользователей, отсутствие правовых оснований для сбора и хранения данных) или практические (нежелание сотрудничать с государственными органами в связи с отсутствием соглашений/ меморандумов, затраты на специализированное оборудование для сбора и/ или хранения данных и т.д.) соображения.
- Сотрудничество на международном уровне
    - Одной из самых характерных особенностей, присущих преступлениям, совершенными посредством виртуальных валют, и киберпреступлениям, является их транснациональный характер.
    - Международное сотрудничество при расследовании отмывания денег, совершенного с использованием виртуальных валют, зачастую зависит от наличия и грамотного использования механизмов международного

сотрудничества между следственными органами и другими ведомствами системы уголовного правосудия соответствующих стран.

- Сотрудничество на международном уровне гораздо более формализовано, чем сотрудничество на национальном уровне.
- Отсутствие регулирования виртуальных валют во многих юрисдикциях представляет собой проблему для международного сотрудничества.
- Трудоемкость процедур ВПП или схожих процедур являются проблемой, учитывая высокую волатильность электронных доказательств.
- Подобные сложности характерны также и для непосредственного (прямого) международного сотрудничества между органами полиции.
- Существует ряд механизмов международного сотрудничества, созданных в рамках различных договоров в сфере борьбы с киберпреступностью (контактные пункты 24/7 в соответствии с Конвенцией Совета Европы о компьютерных преступлениях, национальные бюро Интерпол, G8 Сеть подразделений в сфере высокотехнологичных преступлений). Эффективность использования таких механизмов часто недостаточна из-за отсутствия необходимых знаний у правоохранительных или надзорных/ регулирующих органов.
- В контексте государственно-частного сотрудничества существует возможность сотрудничества следственных органов с иностранными компаниями, которые могут иметь актуальные для расследований данные. Примерами могут служить социальные сети, провайдеры электронной почты и прочие. Проблемой в этой связи может оказаться юридически обязательное сотрудничество с иностранными материнскими компаниями. Некоторые из наиболее важных данных могут обрабатываться и/ или находится у материнской компании или другого лица, находящегося в другой стране.

Вопрос 5: Перечислите некоторые из особенностей электронных доказательств, которые отличают их от физических (традиционных) доказательств.

- Сложность выявления, требующая специальных знаний о том, где искать в конкретной компьютерной системе и какие другие данные могут быть с ними связаны;
- Необходимость привлечения узких специалистов, означающая, что без необходимых экспертных знаний и опыта найденную в компьютерных системах информацию может оказаться невозможным извлечь и сохранить. Также потребуются специалисты в области финансов, налогообложения и/или в сфере борьбы с отмыванием денег для целей расследования преступлений, совершенных посредством виртуальных валют.
- Высокая волатильность, означающая, что данные могут быть уничтожены или стать недоступными обычным способом использования компьютерных систем.
- Склонность к изменениям означает, что компьютерные системы и устройства постоянно изменяют и обновляют данные либо автоматически, либо посредством вмешательства извне. Это важно хорошо понимать, чтобы избежать недооценки временных ограничений и состояний электронных доказательств в разные периоды времени.
- Неограниченные возможности по копированию. В сущности, не существует никаких копий цифровой информации. Каждая из копий является точной и безупречной копией оригинала, что делает сложным доказывание аутентичности электронных доказательств.

Вопрос 6: Каковы юридические основания допустимости электронных доказательств в уголовных делах в вашей стране?

- Ответ будет зависеть от конкретной страны, но, по крайней мере, одно из перечисленного ниже будет справедливым:
    - Электронные доказательства являются отдельной категорией или типом доказательств, которые могут быть признаны допустимыми в судебном процессе на ровне с традиционными доказательствами;
    - Электронные доказательства в виде электронного документа могут признаваться допустимыми при условии, что каждая страна признает допустимость таких документов в судебном процессе;
    - Электронные доказательства относятся к понятию «информация», что обычно является допустимым доказательством в судебном процессе.

Вопрос 7: Дайте объяснение понятию дискреционного уголовного преследования и его применимости в расследованиях, связанных с виртуальными валютами.

- Дискреционное уголовное преследование позволяет прокурору снять обвинения в конкретном уголовном деле в связи с отсутствием государственного интереса продвигать его далее. Такие соображения могут быть самыми различными, в том числе финансовые, возраст подсудимого, положение потерпевшего, тяжесть преступления или любой другой фактор, который может позволить освободить преступника от уголовного наказания.
- Во многих случаях существуют альтернативы уголовному преследованию, которые, в случае их принятия, будут обязательными для правонарушителя. Например, примирение с жертвой, компенсация ущерба преступления, обязательное лечение от наркомании и т.д.
- В преступлениях, связанных с виртуальными валютами, часто присутствует элемент киберпреступления, что может негативно повлиять на проведение уголовного преследования, так как компьютерные преступления, как правило, менее тяжкие и есть законные основания для прокурора освободить преступника от уголовного наказания.
- Чтобы нивелировать эти риски, обвинение должно концентрироваться не на компьютерном преступлении, а на отмывании денег, являющимся более тяжким преступлением, таким образом, не оставляя места для дискреционных полномочий прокурора.

Вопрос 8: Расскажите о преимуществах, которые правоохранительные органы могут извлечь из сотрудничества с подразделением финансовой разведки.

- Доступ к современным знаниям и опыту в отношении методов и практик по легализации преступных доходов (общая экспертиза)
- Использование сотрудников ПФР в качестве экспертов в делах, связанных с отмыванием денег, совершенного посредством виртуальных валют (специализированная экспертиза);
- Доступ к информации разведывательного характера, такой как сообщения о подозрительных операциях (СПО);
- Обмен знаниями о киберпреступлениях с финансовым сектором, тем самым усиливая общее понимание вопросов в контексте сотрудничества.

Вопрос 9: Перечислите возможные механизмы прямого международного сотрудничества следственных органов (полиции), которые могут быть использованы в расследованиях, связанных с виртуальными валютами.

- Контактные центры 24/7 в соответствии с Конвенцией Совета Европы о компьютерных преступлениях являются главными контактами по вопросам киберпреступности, непосредственно уполномоченные предоставлять помощь в связи с запросами об информации и других следственных действиях аналогичных контактных центров из других стран;
- G8 Сеть подразделений в сфере высокотехнологичных преступлений открыта также и для других стран, не входящих в G7+. Эти подразделения имеют схожие функции с контактными центрами 24/7.
- Национальные бюро Интерпол могут быть использованы в контексте международного сотрудничества органов полиции для расследования любых уголовных преступлений, для которых нет специализированных контактных центров или двусторонних соглашений, предлагающих более эффективные механизмы сотрудничества.

Вопрос 10: Какие тенденции вероятнее всего окажут влияние на использование виртуальных валют для целей отмывания доходов от преступлений?

- Увеличение числа виртуальных валют
    - С момента своего появления число виртуальных валют резко возрастает.
    - Первая криптовалюта (bitcoin) появилась в 2009 г. В 2014 г. в общей сложности насчитывается 12 популярных криптовалют.
    - Нет оснований исключать, что в ролевых играх/ виртуальных мирах не появится свои внутренние (неконвертируемые) виртуальные валюты.
    - Крупные торговые сайты (например, amazon.com) начали внедрение виртуальных валют для оплаты приложений и покупки других товаров на своих сайтах.
- Растущая доступность виртуальных валют
    - С ростом доступности виртуальных валют увеличивается количество бизнес-моделей и источников финансирования.
    - Если требования администратора или биржи виртуальных валют, направленные на борьбу с мошенничеством, удовлетворяются, то не будет и никаких географических

ограничений, препятствующих приобретению любой конвертируемой виртуальной валюты.

- Увеличивающаяся сложность схем отмывания денег
  - Отсутствие связей между счетами в виртуальных валютах и реальными людьми в сочетании с возможностью иметь любое количество счетов позволяет создавать новые сложные схемы операций, целью которых является сокрытие незаконного происхождения средств.
  - Виртуальные валюты, таким образом, могут предоставлять дополнительные возможности для создания новых методов отмывания денег.
- Ужесточение регулирования виртуальных валют
  - Администраторы централизованных виртуальных валют и биржи виртуальных валют могут регулироваться как финансовые учреждения, которые предлагают услуги передачи стоимости.
  - Ожидается, что тенденция по ужесточению регулирования этих видов провайдеров виртуальных валют будет усиливаться.

3 Модуль 3: Выявление и расследование отмывания преступных доходов, совершенного посредством виртуальных валют

Вопрос 1: Опишите с точки зрения материального уголовного права взаимосвязи между отмыванием денег и киберпреступлениями в случаях, когда используются виртуальные валюты.

- Предикатные преступления: киберпреступления по несанкционированному доступу, вмешательству в данные, компьютерному мошенничеству или другие подобные преступления могут генерировать незаконные доходы, требующие сокрытия и отмывания.
- Вспомогательные преступления: киберпреступления против компьютерных систем и данных способствуют отмыванию денег путем создания благоприятных условий для сокрытия доходов или их преобразования в законные активы, особенно в случаях, когда безопасность кошельков виртуальных валют ставиться под угрозу.
- Автономные преступления: киберпреступления против надлежащей работы систем или данных, участвующих в операции с использованием виртуальных валют, может свидетельствовать о подготовке к отмыванию денег, так как взломанные или зараженные системы подвержены повышенному риску использования в качестве инструментов отмывания денег.

Вопрос 2: Приведите пример преступления по неправомерному доступу в контексте виртуальных валют?

- Неправомерный доступ к компьютерным системам и данным означает несанкционированный доступ к компьютерной системе или любой ее части (оборудованию, комплектующим, данным установленной системы, каталогам, данным трафика и контента), независимо от типа подсоединения и способа связи. В контексте виртуальных валют такие хакерские преступления могут быть нацелены на:
    - Базу данных центрального администратора, управляющего эккаунтами пользователей игры и их операциями;
    - Bitcoin-кошельки и другие возможные места хранения виртуальной валюты;
    - Серверную инфраструктуру обменника виртуальных валют с целью получения контроля над данными по обмену этих валют.

Вопрос 3: Опишите, как использование позволяющих скрывать личность онлайновых (прокси) программ может быть представлено в качестве элемента преступления по вмешательству в данные на примере, когда речь идет о вмешательстве в персональные данные пользователей виртуальных валют.

- Преступление по вмешательству в данные подразумевает несанкционированные акты манипулирования данными, такие как повреждение, удаление, порча, изменение или подавление компьютерных данных.
- Использование скрывающих личность программ или прокси, или любого другого решения, которое повышает уровень анонимности, можно считать неправомерным деянием, направленным на сокрытие личности потенциального преступника.
- Использование дополнительных онлайновых инструментов помимо виртуальных валют самих по себе в целях повышения уровня анонимности пользователей децентрализованных виртуальных валют может быть представлено в качестве элемента преступления по вмешательству в данные, в частности, как доказательство умысла.

Вопрос 4: Объясните, как использование децентрализованных виртуальных валют может быть использовано, чтобы доказать элемент «расслоения» преступления по отмыванию денег?

- С точки зрения отмывания денег под «расслоением» понимается совершение ряда операций, целью которых является скрытие источника средств, полученных от преступной деятельности.
- Рассматривая использование виртуальных валют для «расслоения», свойственные им черты, такие как анонимность и сложность отслеживания транзакций, могут быть представлены в качестве элемента преступления по отмыванию денег, доказав сознательный выбор такой альтернативы традиционным финансовым операциям именно в силу наличия у виртуальных валют таких характеристик.
- В уголовном судопроизводстве по отмыванию денег, сосредоточение внимания на использовании виртуальных валют для «расслоения» может стать центральным аргументом для доказательства умысла.

Вопрос 5: Объясните возможные взаимосвязи между компьютерным мошенничеством и отмыванием денег посредством виртуальных валют.

- Преступление по компьютерному мошенничеству является ассимилирующим преступлением, совмещающим элементы традиционного мошенничества с информационно-коммуникационными технологиями. С этой точки зрения компьютерное мошенничество представляется актуальным для отмывания денег посредством виртуальных валют:
    - компьютерное мошенничество может быть предикатным преступлением, когда доходы, полученные от мошеннической деятельности в сети Интернет, конвертируются в виртуальные валюты с целью их отмывания;
    - компьютерное мошенничество может быть вспомогательным преступлением, способствующим совершению отмывания денег посредством манипулирования данными пользователей виртуальных валют;
    - пользователи эккаунтов или кошельков виртуальных валют могут быть обманным путем вовлечены в деятельность, имеющую признаки отмывания денег.

Вопрос 6: Какие данные, которыми располагает CSIRT, могут быть использованы для финансовых расследований по отмыванию денег, совершенных посредством виртуальных валют?

- Сообщения об инцидентах в сфере компьютерной безопасности, получаемые CSIRT либо из местных сенсорных сетей, либо из международных баз, данных, содержат важные данные трафика финансовый учреждений;
- Информация об использовании вредоносных программ, которые непосредственно нацелены на кражу личных данных или нарушение неприкосновенности частной финансовой информации, в том числе о случаях, когда следы трафика таких вредоносных программ содержат данные программного обеспечения, используемого для управления централизованной или децентрализованной виртуальными валютами;
- Общие сведения о хакерском сообществе и угрозах национальному киберпространству, а также важные оперативные данные о различных форумах и платформах по обмену информацией, имеющей отношение к киберпреступлениям и киберпреступникам.

Вопрос 7: Какова правовая основа и требования, предъявляемые к перехвату данных контента в делах, связанных с использованием виртуальных валют?

- Перехват данных контента представляет собой применение традиционных методов снятия данных контента с телекоммуникационных устройств (например, телефонные разговоры) к среде информационных технологий. Поэтому к нему предъявляются, в сущности, те же требования, что и к традиционным процедурам перехвата данных / прослушивания:
    - открытое уголовное расследование серьезных преступлений, которые могут включать использование виртуальных валют;
    - перехват данных только с санкции суда;
    - прокурорский надзор.

Вопрос 8: Объясните процедурные различия (с точки зрения законодательства и практики) между оперативным обеспечением сохранности компьютерных данных и обыском, и изъятием компьютерных данных.

- Обеспечение сохранности компьютерных данных позволяет оперативно обеспечить сохранность указанных компьютерных данных, в частности, когда есть основания полагать, что такие

данные подвержены рискам уничтожения или изменения. Характерные черты данной процедуры:
    - эта мера предполагает меньшую степень вмешательства в частную жизнь человека;
    - данные остаются в собственности и под контролем владельца при условии, что они не подвергнуться изменениям;
    - от держателей, данных требуется неразглашение информации о применении процедуры по обеспечению сохранности компьютерных данных;
    - не требуется наличие специальных знаний для осуществления процедуры по обеспечению сохранности компьютерных данных.
- Обыск и изъятие компьютерных данных (т.е. электронных доказательств) являются, по сути, ассимилирующими положениями, направленные на гармонизацию уже существующих уголовно-процессуальных полномочий по обыску и изъятию материальных объектов с точки зрения их применения к компьютерным системам и данным. Однако, существуют некоторые особенности, отличающие эти процедуры от обеспечения сохранности компьютерных данных:
    - большая степень вторжения в частную жизнь человека/ хозяйствующего субъекта, чьи помещения обыскиваются;
    - обыск и выемка выполняются не конфиденциально и, как правило, требуют присутствия человека/ представителя юридического лица, чьи помещения обыскиваются;
    - данные, объекты и любые другие доказательства изымаются из-под контроля владельца и передаются в распоряжение государства;
    - обыск и выемка электронных доказательств потребует специальных знаний для обеспечения целостности изъятых доказательств.

Вопрос 9: Назовите, как минимум, три элемента обеспечения последовательности электронных доказательств.

- Целостность данных, означающая, что компьютерные данные должны всегда оберегаться от возможных изменений с помощью различных приемов и методов (например, доступ в режиме «только для чтения», анализ цифровой копии, а не оригинала доказательства, формирование изображений или фиксация обработки доказательств и т.д.), что гарантирует аутентичность данных.
- Контрольный след, который означает сохранение всех официальных документов, подтверждающих процесс расследования: контрольные списки, отчеты, фотографии, записи, заметки с места преступления

и другие формы документирования с целью подтверждения аутентичности электронных доказательств.

- Привлечение специалистов по компьютерной криминалистической экспертизе является важным, хотя и не всегда обязательным требованием, которое обусловлено сугубо техническим характером компьютерной среды, а также очень узкой специализацией, необходимой для правильной обработки определенных типов электронных доказательств.
- Законность доказательств, что означает, что только данные, имеющие отношение к расследованию должны изыматься и сохранятся. Другие персональные данные конфиденциального характера должны исключаться и не могут обрабатываться без соответствующей санкции. В случае если в таких данных возникнет необходимость, для дальнейшего продолжения анализа информации понадобятся судебные решения, обеспечивающие охрану конфиденциальных данных личного характера.

Вопрос 10: Назовите национальные ведомства, чей экспертный потенциал может быть полезен в расследованиях, связанных с виртуальными валютами.

- Специалисты центров по реагированию на инциденты в области компьютерной безопасности (CSIRTs) могут быть использованы в качестве экспертов по вредоносным программам и анализу сети в случаях, когда применяются виртуальные валюты.
- Подразделения финансовой разведки (ПФР) имею ценный опыт и знания в вопросах финансовых преступлений и методов отмывания денег. Кроме того, ПФР имеет ценных экспертов по анализу сообщений о подозрительных операциях.
- Подразделения по вопросам киберпреступлений/ высокотехнологичных преступлений располагают экспертным потенциалом в вопросах применения процессуальных действий, направленных на сбор оперативных данных в ходе расследований киберпреступлений (мониторинг, обеспечение сохранности, перехват данных), и возможностями по обработке и анализу электронных доказательств.
- Центральные экспертные учреждения стран, исходя из их квалификации и технических возможностей, могут быть привлечены для проведения экспертизы и предоставления отчетов в отношении электронных доказательств.
- В случаях, когда для обработки специфических видов доказательств (например, систем энергоменеджмента или мобильной связи) возникает необходимость в узкоспециализированных знаниях и

опыте, можно обращаться за помощью и использовать возможности частного сектора.

Вопрос 11: Опишите следственные индикаторы, которые могут указывать на использование виртуальных валют для отмывания преступных доходов.

- Использование красных флажков/индикаторов
  - Не являются уникальными для использования виртуальных валют, однако, те, которые применяются в более общих случаях отмывания преступных денег в сети Интернет могут также применяться к случаям использования виртуальных валют.
  - Обратитесь к типологическому исследованию ФАТФ «Новые способы платежей, используемые для отмывания денег» и расскажите об перечисленных там красных флажках.
  - Обратитесь к типологическому исследованию Совета Европы «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками» и расскажите об перечисленных там красных флажках.
- Наличие программного обеспечения, связанного с использованием виртуальных валют
  - Bitcoin-кошельки
  - ПО для использования других виртуальных валют
  - ПО для доступа в виртуальные миры
- История просмотров вэб-сайтов, имеющих отношение к виртуальным валютам
- Услуги удаленного хранения данных (например, dropbox)
  - могут использоваться для хранения виртуальной валюты и/или учетных данных
- Защищенное паролем ПО для хранения данных
  - может использоваться для хранения виртуальной валюты и/или учетных данных
- Виртуальные машины
  - могут использоваться для скрытия фактов использования виртуальных валют в виртуальной среде
  - часто поддерживается функция шифрования жестких дисков виртуальных машин
- Мобильные устройства
  - ПО виртуальных валют часто может устанавливаться как на компьютер, так и на мобильные устройства
  - признаки просмотров вэб-сайтов, имеющих отношение к виртуальным валютам, можно найти и на мобильных устройствах.

Вопрос 12: Расскажите о видах доказательств, которые могут быть собраны с помощью криминалистической экспертизы компьютера подозреваемого и которые могут свидетельствовать об отмывании преступных доходов посредством виртуальных валют. В качестве примера используйте Bitcoin-кошелек.

- Доказательства в виде учетных данных, посещения вэб-сайтов, электронной почты и т.д., свидетельствуют о наличии связи подозреваемого с администратором виртуальной валюты или биржей (обменником) виртуальных валют.
- Доказательства, свидетельствующие о владении подозреваемым некоторым количеством виртуальной валюты.
- В случае с bitcoin вероятно получится установить конкретные адреса, контролируемые подозреваемым. Впоследствии bitcoin-адреса могут быть исследованы с целью определить, с каких адресов bitcoin переводились на адрес подозреваемого и на какие адреса bitcoin переводились с адреса подозреваемого.
- IP-адрес компьютера в определенное время может быть связан с известными операциями подозреваемого или другой финансовой деятельностью.
- Доказательство использования услуг удаленного хранения данных, посредством которых может обеспечиваться хранение виртуальной валюты.
- Пароли или другие учетные данные, которые могут быть использованы для доступа к счетам в виртуальных валютах или к виртуальной валюте.

Вопрос 13: Расскажите, какую информацию можно получить от центрального администратора виртуальной валюты и/ или биржи виртуальных валют, а также о возможных способах получения такой информации.

- Данные о клиенте, его операциях и коммуникации с подозреваемым.
- Каналы сбора информации
    - Прямой контакт с администратором, исходя из условий предоставления услуг или политики конфиденциальности.
    - Через местные правоохранительные органы, используя механизм международного взаимодействия органов полиции.
    - Взаимная правовая помощь

Вопрос 14: Расскажите, как государственно-частное партнерство может стать эффективной контрмерой в отношении отмывания преступных доходов посредством виртуальных валют. Аргументируя свой ответ, используйте примеры.

- Является, вероятно, наиболее эффективной мерой по профилактике и борьбе с криминальными потоками денег в сети Интернет.
- Большинство инициатив касаются сотрудничества и обмена информацией на национальном уровне.
- Является сложным вопросом, зависящим от сторон в государственном и частном секторах соответственно, а также от характера предполагаемого сотрудничества.
- Организации частного сектора могут предоставить важную для следствия информацию. Примерами таких организаций являются финансовые учреждения, провайдеры Интернет и телекоммуникационных услуг.
- В международном контексте важную информацию могут предоставить крупных международные провайдеры услуг, как например, социальные сети, провайдеры онлайновой электронной почты и пр.

Вопрос 15: Расскажите, как межведомственное сотрудничество государственных органов может стать эффективной контрмерой в отношении отмывания преступных доходов посредством виртуальных валют. Аргументируя свой ответ, используйте примеры.

- Межведомственное взаимодействие может быть формальным или неформальным.
- Формальное взаимодействие предполагает наличие постоянной основы или механизмов такого взаимодействия (например, наличие меморандума о взаимопонимании).
- Часто на практике существуют также неформальные механизмы сотрудничества между различными учреждениями. Вот некоторые примеры организации такого межведомственного сотрудничества, реализованного в некоторых странах:
  - Создание на базе нескольких ведомств единого «мозгового центра» для выявления и анализа следственных вызовов.
  - Привлечение представителей полиции к проведению проверок и анализу полученных результатов.
  - Пересмотр используемых в работе подходов с учетом подходов, используемых полицией и надзорными органами.
  - Создание единой информационной системы, позволяющей разным компетентным ведомствам иметь доступ к информации о прошлых или текущих расследованиях в отношении

конкретного физического и/ или юридического лица. Это помогает избежать дублирования и содействует взаимопомощи.
- Установление политик и процедур, способствующих обмену информацией / разведданными.
- Установление процедур, позволяющих решать спорные вопросы в интересах следствия.
- Заключение письменных соглашений, как, например, меморандума о взаимопонимании или подобного ему с целью формализации процессов сотрудничества.

4 Модуль 4: Арест виртуальных валют

Вопрос 1: Каковы различия между преступными доходами и орудиями преступлений?

- Доходы (преступлений) означают любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения какого-либо преступления. Могут состоять из любого имущества, будь то материального или нематериального, движимого или недвижимого, выраженного в вещах или в правах, а также юридических документах или актах, подтверждающих право на такие активы или интерес в них.
- Орудия (преступлений) означают любое имущество, использованное или предназначенное для использования, любым способом, целиком или частично, для совершения преступления или преступлений.
- Виртуальные валюты могут являться как доходами, так и орудием преступлений, особенно в случае отмывания денег.

Вопрос 2: Каковы различия между замораживанием и арестом преступных доходов и орудий преступлений?

- «Замораживание» доходов и орудий преступлений означает временное запрещение передачи, преобразования, отчуждения или передвижения имущества, которое остается под законным и эффективным контролем владельца такого имущества.
- Арест доходов или орудий преступлений тоже означает запрещение передачи, преобразования, отчуждения или передвижения имущества по решению компетентного органа или суда, которое позволяет этим органам осуществлять контроль в отношении такого имущества.
- Несмотря на то, что арестованное имущество остается собственностью физического или юридического лица, или лиц, имеющих право на такие активы или интерес в них, компетентный

орган или суд часто берут на себя владение, администрирование или управление арестованным имуществом.

Вопрос 3: Объясните необходимость экспертной помощи для выявления и ареста преступных доходов и орудий преступлений.

- Обеспечение сохранности доходов и орудий преступлений требует специальных знаний, а применительно к виртуальным валютам может потребовать еще более узкой специализации, которая может отсутствовать у правоохранительных органов.
- Официальные экспертиза и отчеты финансовых экспертов могут быть необходимыми для осуществления ареста преступных доходов и орудий преступлений.
- Привлечение экспертов особенно актуально в случаях, когда следственные действия требуют одобрения судом с целью обеспечения процедур ареста доходов/ орудий преступлений.

Вопрос 4: Объясните, как нужно определять соответствующую юрисдикцию для процессуальных действий в отношении децентрализованных виртуальных валют как доходов преступления?

- Децентрализованные виртуальные валюты предполагают операции между кошельками отдельных пользователей.
- В случае децентрализованных виртуальных валют территориальная юрисдикция над доходами или орудиями преступления будет определяться местом нахождения кошелька. Иными словами, это – физическое место расположения оборудования, на котором хранится кошелек, содержащий виртуальную валюту. Это и будет юрисдикцией для целей замораживания, ареста и конфискации преступных доходов и орудий преступлений.
- Определение местоположения кошелька с виртуальной валютой является предметом следственных и разведывательных действий, которые, по крайней мере, должны дать ответ на вопрос, в какой юрисдикции находится соответствующее оборудование.

Вопрос 5: Назовите, по крайней мере, два «красных флажка», применимых для выявления преступных доходов, связанных с обменниками виртуальных валют.

- Большое количество банковских счетов, принадлежащих одному администратору виртуальной валюты или компании, занимающейся обменом виртуальных валют (иногда находятся в разных странах), которые, по всей видимости, используются как транзитные счета (что может свидетельствовать о деятельности,

характерной для второго этапа процесса отмывания денег – «расслоения»).

- Компания, занимающейся обменом виртуальных валют, находится в одной стране, но имеет счета в других странах (нелогичное обоснование такой бизнес деятельности, что может быть подозрительным)
- Круговое движение денежных средств между банковскими счетами, находящихся в разных странах и принадлежащие разным компаниям, которые занимаются обменом виртуальных валют (может свидетельствовать о деятельности, характерной для второго этапа процесса отмывания денег – «расслоения», если такая деятельность не является обычной бизнес-активностью компании);
- Объем и частота операций с наличностью (иногда разбиты на суммы, меньшие порога предоставления отчетности), которые проводятся собственником компании, занимающейся обменом виртуальных валют, и не имеют экономического смысла.

Вопрос 6: Объясните значение сообщений о подозрительных операциях (СПО) для целей выявления преступных доходов и орудий преступлений, совершенных с использованием виртуальных валют.

- Сообщения о подозрительных операциях (СПО) являются основными инструментами получения финансовых разведданных и используются подразделениями финансовой разведки.
- Наличие и значение СПО от центральных администраторов будет, как правило, определяться степенью государственного регулирования виртуальных валют и наличием законодательных требований к таким учреждениям о предоставлении СПО национальному ПФР.
- В случаях с криптовалютами СПО от бирж виртуальных валют будут особенно полезным источником разведданных для целей финансовых расследований в отношении доходов и орудий преступлений.
- Особенно важными являются СПО, в основе которых лежат операции с «красными флажками» или операции по обмену виртуальной валюты.

Вопрос 7: Опишите процесс ареста (взятия под контроль) децентрализованной виртуальной валюты.

- Самым жизнеспособным вариантом взятия под контроль виртуальных валют является передача их на счет (кошелек) правоохранительного органа, который предпримет следующие шаги:

  - Определит количество виртуальной валюты или кошельков, или и того и другого, подлежащих аресту;
  - Обеспечит сотрудничество со стороны подозреваемого или установит контроль над кошельком с помощью других разрешенных законом средств, чтобы необходимая сумма была переведена на контролируемый правительством кошелек с целью последующей конфискации и ликвидации;
  - Задокументирует должным образом получение активов; или
  - Если сотрудничество или контроль над кошельком невозможны:
    - определит на основе обменного курса стоимость виртуальной валюты, подлежащей аресту, в местной валюте;
    - применит процедуру стоимостной конфискации.
- Стоимостная конфискация может применяться и изначально в случаях, когда традиционный арест и контроль над виртуальными валютами невозможны в силу либо соображений безопасности, либо с точки зрения обременительности управления такими активами.

Вопрос 8: Назовите, по крайней мере, два механизма международного сотрудничества в финансовых расследованиях.

- Сотрудничество через сети международного сотрудничества, специально созданных для выявления доходов от преступлений: Камденская межучрежденческая сеть возвращения активов (CARIN), Инициатива по возвращению похищенных активов (StAR) или более специализированные сети по возвращению активов, такие как Глобальная сеть координаторов по возвращению активов.
- Использование механизмов сотрудничества между органами полиции, в особенности такие: контактные центры 24/7 в соответствии с Конвенцией Совета Европы о компьютерных преступлениях, G8 Сеть подразделений в сфере высокотехнологичных преступлений или национальные бюро Интерпол, которые могут предоставить данные разведывательного характера, выполнить запросы по обеспечению сохранности данных, а также другие следственные запросы напрямую в обход трудоемкой процедуры взаимной правовой помощи.
- Установление посредством национального ПФР контактов с ПФР иностранных государств, запрашивая по защищенному каналу Egmont Secure Web данные о СПО или другую разведывательную информацию, или результаты проведенного анализа, а также использование других, в том числе двусторонних, механизмов сотрудничества.
- Использование формальных процедур обмена информацией через центральный орган (прокуратуру) – механизм обмена запросами о предоставлении взаимной правовой помощи.

UNODC
Управление Организации Объединенных Наций
по наркотикам и преступности