Анализ норм об ответственности за преступления в сфере незаконного оборота наркотических средств и психотропных веществ показал, что, несмотря на предпринимаемые законодательные меры по совершенствованию антинаркотического законодательства, необходимость его дальнейшего совершенствования является актуальным и одним из приоритетных направлений уголовно-правовой политики.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Оперативно-розыскная деятельность органов внутренних дел. Общая часть: электронное учебное издание. – Омск: Омская академия МВД России, 2020. – 206 с.
2. Краткая характеристика состояния преступности в Российской Федерации за январь – октябрь 2022 года [Электронный ресурс]. – Режим доступа: https://мвд.рф/reports/item/33913311/ (дата обращения: 22.11.2022).
3. Отдел МВД России по Городищенскому району [Электронный ресурс]. – Режим доступа: https://городищенский.34.мвд.рф/.
4. Управление на транспорте МВД России по СЗФО [Электронный ресурс]. – Режим доступа: https://сзфоут.мвд.рф/D/.
5. Дубоносов Е.С. Оперативно-розыскная деятельность: учебник и практикум для вузов. – 6-е изд., перераб. и доп. – Москва: Юрайт, 2022. – 379 с.

УДК 343

НЕКОТОРЫЕ ПОДХОДЫ К УСТАНОВЛЕНИЮ ВЛАДЕЛЬЦЕВ ПУБЛИЧНЫХ КРИПТОАДРЕСОВ, СОВЕРШАЮЩИХ ПРОТИВОПРАВНЫЕ ДЕЯНИЯ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ (НА ПРИМЕРЕ БИТКОЙН-ПРОТОКОЛА)

Боровик П.Л.,
кандидат юридических наук, доцент;
Самойло В.И.
(Академия МВД Республики Беларусь)

Аннотация: в статье рассматривается деятельность сотрудников оперативных подразделений органов внутренних дел по выявлению, пресечению, предупреждению и раскрытию преступлений в сфере оборота криптовалют, электронных платежных систем, небанковских бирж в целях противодействия совершения преступлений различных категорий, и в том числе легализации денежных средств, полученных преступным путем. Анализируются пассивные и активные методы идентификации пользователей публичных биткойн-адресов

из открытых источников глобальной сети, варианты их использования в целях дальнейшей деаномизации пользователей с целью получения сведений о личности лиц, совершающих преступления с использованием криптовалют, и противодействия наркопреступности в целом.

Ключевые слова: компьютерная безопасность, криптовалюта, биткойн-протокол, деаномизация, транзакция, майнинговый пул, небанковская биржа, виртуальный след, биткойн-кошелек.

SOME APPROACHES TO IDENTIFYING OWNERS OF PUBLIC CRYPTO ADDRESSES WHO COMMIT ILLEGAL ACTS USING CRYPTOCURRENCIES (USING THE EXAMPLE OF THE BITCOIN PROTOCOL)

Borovik P.L.,
Candidate of Law, Associate Professor;
Samoilo V.I.
(Academy of the Interior of the Republic of Belarus)

Abstract: the article examines the activities of employees of operational units of internal affairs bodies to identify, suppress, prevent and solve crimes in the sphere of crypto currency turnover, electronic payment systems, non-bank exchanges in order to counteract the commission of crimes of various categories, including the legalization of funds obtained by criminal means. Passive and active methods of identifying users of public bitcoin addresses from open sources of the global network are analyzed, as well as options for their use in order to further deanomize users in order to obtain information about the identity of persons committing crimes using crypto currencies and countering drug crime in general.

Keywords: computer security, crypto currency, bitcoin protocol, deanomization, transaction, mining pool, non-bank exchange, virtual footprint, bitcoin wallet.

Вопросы противодействия преступности, сопряженной с использованием криптовалют (отмывание денежных средств, преступления против компьютерной безопасности, бесконтактный сбыт наркотиков, мошенничество и др.), исследовались в работах многих ученых. Исследователями в основном рассматривались такие аспекты проблемы, как предмет преступного посягательства, способы и средства совершения преступления, уголовно-правовая квалификация и др. Вместе с тем особенности выявления лиц, совершающих рассматриваемые деяния, остались в полной мере не изученными. Практика свидетельствует, что использование злоумышленниками криптовалют для оплаты противоправной деятельности и получения вознаграждения бесконтактным способом не только значительно снижает для них риск быть задержанными в момент совершения преступления, но и существенно усложняет применение сотрудника-

ми оперативных подразделений традиционных средств его выявления и документирования.

Не ставя в данной работе перед собой задачу углубиться в математико-криптографические аспекты обозначенной проблематики, ограничимся рассмотрением общих методологических вопросов, касающихся деанонимизации владельцев публичных биткойн-адресов.

Анализ оперативно-следственной и судебной практики по делам о преступлениях, связанных с использованием криптовалют, свидетельствует, что одной из насущных проблем выявления и расследования соответствующих криминальных деяний является установление личности (идентификация) владельца публичного биткойн-адреса, с которого либо на который осуществлялась транзакция. Так, используя возможности открытого обозревателя «Блокчейн», можно установить достоверную информацию обо всех проведенных транзакциях данного лица (дата и время, сумма, сведения о получателе перевода и др.). Но, поскольку процесс создания криптокошелька в основном анонимен, а переводы с одного биткойн-адреса на другой не верифицируются, установить персональные сведения о лицах (IP-адрес, географическое местоположение, ФИО и пр.), участвующих в транзакции, традиционными средствами не представляется возможным.

Вместе с тем результаты изучения и обобщения специальной литературы (как отечественной, так и зарубежной), посвященной рассматриваемой проблематике [1; 2; 3; 4 и др.], позволяют сделать вывод о наличии некоторых достаточно эффективных подходов к решению данной задачи.

Так, выделяют две группы методов деанонимизации лиц, совершающих преступления с использованием криптовалют: пассивные и активные.

Пассивные методы основываются на использовании данных, полученных из блокчейна (например, https://www.blockchain.com/) либо иного общедоступного источника информации. Применяемые при этом подходы, с одной стороны, подразумевают отсутствие прямого взаимодействия с одноранговой сетью биткойн; с другой – полагаются на комплексные и широко представленные в открытых источниках методы анализа графов и иные эвристические технологии, связанные с биткойн-протоколом.

В основе активных методов деанонимизации владельца публичного биткойн-адреса могут лежать как методы социальные инженерии, позволяющие установить непосредственный контакт с владельцем (например, узнать его адрес в ходе беседы либо просьбы об оплате), так и методы, основанные на внедрении специально разработанных обфусцированных биткойн-узлов, содержащих модифицированное программное обеспечение, позволяющее перехватывать трафик либо устанавливать прямую связь с другими узлами в сети.

При этом, если методы социальной инженерии подходят в основном для деанонимизации частично неизвестных владельцев биткойн-адресов в условной цепочке биткойн-транзакций, то использование обфусцированных биткойн-узлов позволяет перехватить IP-адреса владельцев и связать с ними определенные транзакции.

Мы прогнозируем, что наибольшей популярностью, обусловленной главным образом экономической целесообразностью, а, следовательно, и практической значимостью, могут обладать пассивные способы, основанные на использовании эвристики – совокупности логических и аналитических приемов, методов и правил, облегчающих и упрощающих решение конкретных познавательных и практических задач. Рассмотрим в этой связи их более подробно.

При пассивном сборе исследователь осуществляет поиск цифровых имен пользователей публичных биткойн-адресов из открытых источников глобальной сети: веб-сайты, форумы, социальные сети, майнинговые пулы, кошельки, банковские биржи, небанковские биржи, продавцы, азартные игры, прачечные. Существуют различные агрегаторы информации, связанные с биткойн-кошельками, доступными в Интернете [5; 6].

Пассивные методы идентификации подразделяются на следующие разновидности:

а) метод прямого совпадения, в его основе лежит традиционный поиск цифрового идентификатора владельца биткойн-адреса в общедоступных источниках с использованием поисковых систем;

б) эвристический метод нескольких входов, основанный на сопоставлении входных биткойн-адресов. Например, если сумма транзакции превышает стоимость каждого из доступных биткойнов в кошельке пользователя, то существующие биткойн-клиенты выбирают набор биткойнов из разных имеющихся адресов в кошельке владельца и выполняют платеж с помощью транзакций с несколькими входными адресами, принадлежащими одному пользователю;

в) анализ смены биткойн-адреса. Суть данного метода основывается на генерации в ходе транзакции сетью биткойн так называемых «теневых» адресов [7], на который владельцу кошелька поступает «сдача». Используя методы сопоставления и анализа, можно легко установить начальный адрес владельца кошелька, который осуществлял оплату;

г) метод кластеризации, основан на двух предыдущих подходах. Используя эвристический метод нескольких входов, исследователи смогли разделить сеть на 5.579.176 кластеров пользователей, начав с 12.056.684 открытых ключей. В последующем, анализируя смену биткойн-адресов, авторы предложили новую эвристику кластеризации, основанную на изменении адреса, позволяющую выделить и объединить адреса, принадлежащие одному и тому же владельцу кошелька [8]. С помощью данного метода можно идентифицировать основные финансовые субъекты (биржи, обменники, игровые сайты и т. п.) и способы взаимодействия между ними, используя лишь незначительное количество идентифицированных транзакций;

д) метод анализа виртуальных следов (цифровых отпечатков), в основе которого лежит механизм формирования виртуальных следов сторонними веб-трекерами в открытом сегменте сети Интернет. В литературе, посвященной рассматриваемому вопросу, отмечается, что сторонний веб-трекер в состоянии деанонимизировать пользователей криптокошельков [9]. Так, при совершении покупок в интернет-магазине и проведении соответствующих транзакций в криптовалюте в интернет-пространстве будет оставлено множество релевант-

ных виртуальных следов. Данные следы могут быть проанализированы двумя способами:

путем сопоставления транзакции (например, если у стороннего веб-трекера имеется доступ к адресу пользователя, то привязка последнего к адресу осуществляется тривиально; в другом случае, если веб-трекер владеет информаций о стоимости (даже приблизительной) покупки и времени совершения транзакции, то исследователю достаточно получить доступ к журналу транзакций);

путем формирования кластерного перекрестка (идентификация кластера адресов, позволяющая связать две либо более покупок одних и тех же пользователей с блокчейном);

е) метод деанонимизации с графовым анализом, основанный на реализации алгоритмов обнаружения сообществ и метрик центральности. Для этого могут использоваться социальные сети и (или) методы социальной инженерии. Так, исследователь может выявить сообщество друзей или соседей искомого лица, найти людей в середине цепочки, замешанных в незаконной деятельности и т.д.

ж) метод построения и анализа графика транзакций, его суть состоит в следующем. Всю цепочку блоков в блокчейне можно рассматривать как ациклический граф транзакций G = {T, E}, где T – множество транзакций, хранящихся в цепочке блоков, E – множество однонаправленных ребер между этими транзакциями. Указанный граф представляет собой поток биткойнов между транзакциями в блокчейне с течением времени. При этом, набор входных и выходных биткойнов в транзакции следует рассматривать как веса на ребрах графа. Соответственно, каждое входящее ребро в транзакции несет метку времени и количество биткойнов, формирующих вход для указанных транзакций;

з) метод построения и анализа графа адресов, сущность которого схожа с приведенным выше. Анализируя граф транзакций G, исследователь может выявить корреляцию между различными входными и выходными адресами. Открытые ключи и соответствующие взаимосвязи можно использовать для построения графа адресов G = {P, E}, где P – это набор биткойн-адресов, а E – ребра, соединяющие эти адреса;

и) метод построения и анализа графа пользователя предполагает создание на основе вышеприведенных эвристических подходов графа пользователя путем группировки адресов, которые предположительно принадлежат одному и тому же владельцу.

Каждый из вышеприведенных методов деанонимизации состоит из двух этапов: этапа сбора данных и этапа анализа данных. Сбор данных может осуществляться как в режиме онлайн (например, с применением специально разработанных обфусцированных биткойн-узлов, содержащих модифицированное программное обеспечение, позволяющее перехватывать трафик, исследовать механизм распространения адресов, устанавливать прямую связь с другими узлами в сети), так и в автономном режиме с использованием обычного биткойн-кошелька.

На основании изложенного представляется возможных сформулировать следующие выводы.

1. Деанонимизация (установление) владельца публичного биткойн-адреса представляет собой процесс привязки публичного биткойн-адреса к цифровому идентификатору пользователя или его IP-адресу. Может осуществляться с применением активных и пассивных методов.

2. В основе активных методов деанонимизации владельца публичного биткойн-адреса могут лежать как методы социальной инженерии, позволяющие установить непосредственный контакт с владельцем (например, узнать его адрес в ходе беседы либо просьбы об оплате), так и методы, основанные на внедрении специально разработанных обфусцированных биткойн-узлов, содержащих модифицированное программное обеспечение, позволяющее перехватывать трафик либо устанавливать прямую связь с другими узлами в сети.

3. Пассивные методы основываются на использовании данных, полученных из блокчейна либо иного общедоступного источника информации. Применяемые при этом подходы, с одной стороны, подразумевают отсутствие прямого взаимодействия с одноранговой сетью биткойн; с другой – полагаются на комплексные и широко представленные в открытых источниках методы анализа графов и иные эвристические технологии, связанные с биткойн-протоколом.

Все эвристические методы в значительной степени основаны на методе прямого сопоставления.

В сочетании с соответствующими оперативно-розыскными подходами активные и пассивные методы деанонимизации публичных биткойн-адресов могут помочь сотруднику органов внутренних дел установить сведения о личности лица, совершающего преступления с использованием криптовалют.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: учебно-методическое пособие. – Москва: Юрлитинформ, 2017. – 200 с.

2. Сидоренко Э.Л. Криминологические риски оборота криптовалюты и проблемы ее правовой идентификации // Библиотека криминалиста. Научный журнал. 2016. № 3(32). С. 148–154.

3. Батоев В.Б., Семенчук В.В. Использование криптовалюты в преступной деятельности: проблемы противодействия // Труды Академии управления МВД России. 2017. № 2. С. 9–15.

4. Авдошин С.М., Лазаренко А.В. Методы деанонимизации пользователей Bitcoon. – Труды ИСП РАН. Вып. 30. 2018. С. 89–102.

5. Биткойн-адресные метки / Blockchaininfo [Электронный ресурс]. – Режим доступа: https://blockchain.info/ru/tags (дата обращения: 22.10.2022).

6. Bitcoin Address Checker / BitcoinWhosWho [Электронный ресурс]. – Режим доступа: http://bitcoinwhoswho.com (дата обращения: 22.10.2022).

7. Накамото С. Биткойн: одноранговая электронная кассовая система / Биткойн [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf (дата обращения: 22.10.2022).

8. Андрукли Э., Караме Г.О. Оценка конфиденциальности пользователей в биткойнах / Cryptology ePrint Archive [Электронный ресурс]. – Режим доступа: https://eprint.iacr.org/2012/596.pdf (дата обращения: 22.10.2022).

9. Голдфедер С. Когда cookie встречается с блокчейном: риски конфиденциальности веб-платежей через криптовалюты / Библиотека Корнельского университета [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/1708.04748.pdf (дата обращения: 22.10.2022).

УДК 343.141

ОСНОВНЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ОПЕРАТИВНО-РАЗЫСКНОЙ ИНФОРМАЦИИ ПРИ ПРОТИВОДЕЙСТВИИ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ И ПУТИ ИХ РЕШЕНИЯ

Дранчук С.М.;
Челядинов Д.В.,
кандидат технических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматривается деятельность сотрудников оперативных подразделений органов внутренних дел по выявлению, пресечению, предупреждению и раскрытию преступлений в сфере противодействия незаконному обороту наркотических средств, психотропных веществ и их прекурсоров, а также преступлений иных категорий. Анализируются варианты использования оперативно-разыскной информации, формирования интегрированных банков данных, учетов правоохранительных органов с целью повышения эффективности аналитической работы при противодействии наркопреступности.

Ключевые слова: информация, банки данных, оперативно-разыскная информация, выявление, расследование и предотвращение преступлений.