А. В. Пучнин,
кандидат юридических наук

ИСПОЛЬЗОВАНИЕ ОСОБЕННОСТЕЙ КРИПТОВАЛЮТ ПРИ РЕШЕНИИ ЗАДАЧ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ ИНТЕРНЕТ

USING THE FEATURES OF CRYPTO CURRENCIES WHEN SOLVING TASKS ON THE NETWORK ON THE INTERNET TO COUNTER CRIMINAL ACTIVITIES

В статье анализируется современное состояние использования криптовалют при осуществлении преступной деятельности различных видов и возможности органов внутренних дел по выявлению фактов использования виртуальных денег в качестве способа сокрытия преступлений и установления личности участников незаконных операций.

The article analyzes the current state of the use of cryptocurrencies in carrying out criminal activities of various types and the ability of the internal affairs bodies to identify the facts of using virtual money as a way to conceal crimes and establish the identity of participants in illegal operations.

В конце прошлого столетия цифровые технологии развитых стран мира стали серьезно преобразовываться, это было связано с быстрой информатизацией всех сторон хозяйственной деятельности, вследствие чего затронуло и ее логистическую составляющую. На современном этапе мы видим, как широко стали применяться цифровые технологии в повседневной деятельности человека. Использование электронных платежных систем для осуществления операций в различных сферах деятельности повлекло за собой появление новых видов преступлений. Не обошел цифровой процесс стороной и Россию.

Можно полагать, что в настоящее время наблюдается стремительное освоение преступности IT-технологий, ее уход на теневые анонимные площадки сети Интернет, углубление специализации сайтов и расширение перечня криминальных профессий, использующих криптовалюту как основное средство платежа и отмывания преступных доходов.

Целесообразно в первую очередь выделить классификацию преступлений, совершаемых с помощью использования электронных платежных систем и средств. За последний период с помощью электронных средств и платежных систем были совершены следующие виды преступлений:

- интернет-кражи;
- вымогательство;
- интернет-казино;
- интернет-мошенничество;
- легализация доходов, полученных незаконным путем (продажа различных видов наркотиков и оружия);
- взяточничество с помощью криптовалюты (монеты Bitcoin);
- компьютерные преступления в банковской сфере и др.

Дело в том, что большое количество граждан России не пользуется услугами, связанными с электронным оборотом денег, лишь по одной причине — боязнь стать жертвой мошенничества либо использования данных пользователя для совершения преступления. Такой психологический фактор становится серьезной проблемой на пути развития рынка интернет-платежей. Многие люди до сих пор не признают интернет как безопасную среду осуществления платежной деятельности в своих личных целях.

Согласно исследованиям, на текущий период наиболее частым объектом для атаки со стороны преступников либо электронных мошенников являются юридические лица. Физические лица не представляют для преступников такого интереса, однако угрозу их безопасности также нельзя отрицать. Каждый месяц органы внутренних дел регистрируют десятки таких происшествий. Размер ущерба, как правило, достигает 250 тысяч рублей, хотя зарегистрированы случаи, где размер ущерба достигает более 10 миллионов рублей [3].

Такие атаки преступников осуществляются даже при помощи установленных в компьютере юридического лица USB-токенов, которые представляют собой миниатюрные устройства с клавиатурой и ЖК индикатором [5]. В теории токен должен предохранить ключ от несанкциониро-

ванного доступа не только на программном, но и на физическом уровне, поскольку без секретного кода невозможно получить доступ к хранящейся в нем информации.

Не менее распространенным способом хищения является несанкционированный перехват команд на запрос электронной цифровой подписи, который может даже не дойти до сервера получателя, например банка. Выходит, что клиент использует свое устройство одновременно со злоумышленником.

Целесообразно выделить некоторые основания классификации преступлений, совершенных с помощью системы электронных платежей и средств:

- преступления в сфере компьютерной информации;
- преступления в сфере экономической деятельности (в том числе легализация доходов путем отмывания денег в электронных системах);
- преступления против государственной власти (дача взятки посредством систем электронных платежей, а также получение взятки с помощью электронных средств).

На современном этапе в России, как отмечает Е. Л. Логинов, происходит значительная легализация доходов, полученных незаконным путем, с помощью электронных платежных систем. Проведенный автором подробный анализ в отношении данного вида преступлений показывает, что осуществление расчетов и переводов денежных средств в системах электронных платежей достаточно просто. Примером может служить регистрация нескольких электронных кошельков и затем зачисление на них денежных средств, полученных незаконным путем, с целью дальнейшего их обналичивания. Что касается кредитных организаций, то там проводится тщательный контроль за потоком денежных средств (при приеме денежных средств от физических лиц на квитанции указываются паспортные данные пользователя и ставится подпись), а в электронных платежных системах поступление денежных средств, полученных незаконным путем, отследить крайне сложно. Также важной функцией электронных систем платежей является обмен ресурсами между собой, т.е. возможен перевод денежных средств с одного электронного кошелька на другой, что повышает трудность контроля таких операций [4].

В последнее время отмечаются случаи использования виртуальных платежных систем денежных переводов с использованием электронных денежных средств при осуществлении расчетов за предметы, изъятые из свободного оборота, например наркотические средства. Значительная угроза исходит от вовлечённых в наркотрафик представителей незаконной миграции и этнических ОПГ (в основном из Центральной и Восточной Азии, Украины). Существует риск использования электронных платежных систем в целях расчетов за наркотики и финансирования нарколабораторий, так как операторы таких систем имеют статус кредитных организаций и, как правило, входят в банковские группы, но не все они могут быть выявлены [6].

По статистическим данным Росфинмониторинга, на конец июля 2018 года были представлены зафиксированные расчеты наркопотребителей за наркотики, сведения по легализации полученного дохода и распределению денежных средств между организаторами преступной группы, а также выплате вознаграждений закладчикам, наркокурьерам, работникам нарколабораторий.

Что касается использования криптовалют в преступной деятельности, то стоит заострить внимание на событии 2017 года, когда был установлен факт использования криптовалюты, в том числе с помощью монет Bitcoin, в системе незаконного оборота наркотиков на территории более 20 субъектов Российской Федерации. Анонимность расчетов с использованием криптовалют обеспечивает популярность данного способа при совершении преступлений и, кроме того, усложняет процесс расследования сотрудникам оперативных подразделений. МВД России и Росфинмониторингом в пределах Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма проводится типологическое исследование по установлению трансграничных схем наркорасчетов и легализации доходов, полученных от незаконного оборота наркотических средств, с использованием криптовалют, в частности монет Bitcoin. В рамках таких исследований зачастую предоставляются и обобщаются данные правоохранительных органов и подразделений финансовых разведок зарубежных стран о способах криминальных расчетов и моделях правового регулирования криптовалют в различных государствах.

Монеты Bitcoin обладают большим преимуществом, но в то же время из-за своей нормативной незащищенности являются уязвимыми, тем самым позволяя использовать их для совершения преступлений. Существует ряд характеристик по поводу монет Bitcoin, которые обязательно должны быть рассмотрены:

- простота регистрации (необходимо понимать, что, имея доступ к сети Интернет, пользователь может зарегистрировать Bitcoin-адрес, который функционирует аналогично счетам на сайтах провайдеров услуг по обмену монет Bitcoin или на сайтах организаций онлайн-кошельков) [8];
- отсутствие контроля (основным существенным отличием системы является ее децентрализованность или, как принято говорить, пол-

ное отсутствие частного или государственного контролирующего органа) [8];

- колебание курса (благодаря статистике невысокого колебания обменного курса Bitcoin значительно снижает риски обменных операций в сети Интернет);

- доступность (любой может скачать бесплатное приложение с веб-сайта для отправки, получения и хранения монет Bitcoin, а также для контроля операций в децентрализованной системе);

- распространённость (по данным от оперативных подразделений правоохранительных органов, монеты Bitcoin довольно часто применяются в уголовном мире. Также необходимо отметить случаи использования веб-сайтов, связанных с террористическими организациями, для сбора пожертвований в системе Bitcoin. В последнее время были выявлены случаи, когда экстремисты обсуждали возможность использования монет Bitcoin для приобретения оружия);

- быстрота перевода (система Bitcoin позволяет мгновенно и без комиссий перевести любые денежные средства, в том числе полученные незаконным путем, из одной страны в другую);

- анонимность (необходимо отметить, что в основе системы Bitcoin лежит технология Blockchain, состоящая из сформированной цепочки блоков. Каждый из этих блоков представляет собой средство записи своего рода транзакций и включает в себя информацию о предыдущей транзакции. Однако эта информация содержит только криптоадреса, без какой-либо привязки к физическому лицу, при этом участник оборота криптовалют может иметь их множество и оставаться анонимным).

Все перечисленные характеристики монет Bitcoin, с одной стороны, являются преимуществами для участников оборота криптовалют, но, с другой стороны, могут стать инструментом для покупки и продажи наркотиков, оружия, отмывания денег и других противоправных действий. За счет анонимности системы Bitcoin можно оставлять преступную деятельность злоумышленников в тайне. Тут следует отметить, что в настоящий момент в целом с задачей деанонимизации участников криптовалютных операций отечественные оперативные подразделения справляются успешно, нерешенной проблемой остается отсутствие возможности прервать или не допустить биткоинперевод.

Интернет-ресурс Western Express International, созданный с целью кибермошенничества и используемый для обмена криптовалюты, используется злоумышленниками для продажи краденных кредитных карт, данных пользователя, идентификационных кодов с целью подделки и использования банковских карт кредитных организаций. Основной слабостью данной системы и одним из способов ухода от преследования правоохранительных органов стала анонимность чатов участников, а также счетов виртуальных кошельков с монетами Bitcoin. Передача полученных от продаж средств осуществлялась сразу в нескольких зарубежных странах. Более 35 миллионов долларов США было выведено благодаря данной схеме, в том числе с помощью монет Bitcoin. Основным звеном преступной цепочки была компания Western Express International, зарегистрированная в Нью-Йорке. По своей сущности организация являлась провайдером услуг денежных переводов и обмена виртуальной валюты. В феврале 2016 года 16 членов преступной группировки были задержаны и вскоре признали себя виновными в мошенничестве и отмывании денег.

Одной из крупнейших в мире схем мошенничества с использованием криптовалют, в частности монет Bitcoin, является Liberty Reserve. Она представляет собой онлайн-систему денежных переводов, благодаря которой отправитель конвертирует национальную валюту США (доллары) в виртуальную валюту Liberty Dollars. С помощью виртуальной валюты осуществлялся перевод денежных средств с последующей конвертацией в фиатные валюты. Система была основана в Коста-Рике и достигала огромных масштабов (более миллиона пользователей во всем мире, в том числе более 200 000 пользователей в США). Организаторы схемы были замечены правоохранительными органами США в отмывании денег путём перемещения незаконных доходов на сумму более 6 миллиардов долларов США, после чего Liberty Reserve полностью лишилась доступа к финансовой системе Соединённых Штатов Америки [8].

Новым теневым трендом в Российской Федерации является растущее количество предложений так называемых химических конструкторов, позволяющих пользователю или участнику преступной деятельности самостоятельно изготовлять наркотики. Оплата этих конструкторов в 100% случаев осуществляется с использованием криптовалюты. Как правило, за криптовалюту в России на теневых сервисах интернета приобретаются легкие наркотики и порнография, в большинстве случаев именно за монеты Bitcoin распространяется детская порнография. Согласно мониторингу за 2018 год, можно увидеть повышенную активность такого рода анонимных интернет-площадок, в 70% случаев клиенты-педофилы для покупки контента используют монеты Bitcoin и в 30% — другую криптовалюту.

Сотрудникам оперативных подразделений, в том числе и ОВД, необходимо осваивать возможности IT-технологий для выявления преступлений, связанных с криптовалютой, в особенности с монетами Bitcoin.

Ввиду открытости информации об операциях, связанных с криптовалютой, сотрудникам ОВД были предложены алгоритмы действий,

одним из которых является привязывание к конкретным кошелькам операций с входными и выходными узлами. Данный алгоритм был опубликован в сети Интернет, его основное действие связано с процессом кластеризации, который анализирует данные базы технологии Blockchain и объединяет несколько адресов кошельков с монетами Bitcoin, связанных с одним участником, в единый кластер [2]. Задача кластерного анализа транзакционных сетей заключается в нахождении нескольких входов, объединенных в одну транзакцию, что позволяет получить данные о едином источнике контроля.

На этой основе в интересах правоохранительных органов и оперативных подразделений, осуществляющих оперативно-розыскную деятельность, компания Bitfury Group представила новый универсальный инструмент Crystal для исследований технологии Blockchain и, в частности, монет Bitcoin.

Данный инструмент способен работать с информацией о различных потоках операций и транзакций в сети технологии Blockchain, выявляя подозрительные операции и связывая их с объектами правонарушений. Тем самым он способен деанонимизировать отдельные объекты и финансовые взаимоотношения между злоумышленниками [1, 7]. Следует отметить, что адрес монет Bitcoin можно попытаться связать с конкретными лицами, если их персональные данные были каким-либо образом отождествлены с ними. Например, если использовался один из адресов монет Bitcoin для депозитного счета, снятия денег с регулируемого онлайн-кошелька или с помощью Bitcoin осуществлялся расчёт в интернет-магазине и т.п., то в открытом доступе находится адрес для перечисления монет. В этом случае происходит глобальный поиск по всем информационным ресурсам (социальные сети, блоги, сайты (в том числе даркнета) и т.д.) с ключевым признаком номера онлайн-кошелька, что может позволить сотрудникам оперативных подразделений выявить определенное лицо, совершившее незаконные действия. Кроме того, у операций с криптовалютами существуют особенности, которые могут быть выявлены на стадии конвертации.

В качестве таких стадий могут выступить отдельные данные об этапах перемещения криптовалюты, связанных с приобретением, продажей запрещенных категорий товаров. Основной процесс приобретения или обмена монет Bitcoin осуществляется на виртуальных торговых площадках — криптобиржах. Сотрудничество оперативных подразделений с организаторами криптобирж в рамках выявления и раскрытия преступлений позволит получать значимую для раскрытия и расследования информацию о банковских счетах обмена криптовалют, IP-адресах пользователей в сети Интернет и иные персональные данные о злоумышленниках.

Также предпринимаются попытки, направленные на обеспечение получения требуемой информации, в том числе деанонимизации расчетов криптовалютой. Примером служит Европейский парламент, утвердивший пакет новых мер по борьбе с отмыванием средств в странах Евросоюза, в числе которых усиление контроля над монетами Bitcoin и другими виртуальными валютами. Площадки обмена, виртуальные кошельки и банковские учреждения теперь обязаны осуществлять контроль за своими клиентами, включая требования к проверке информации об их операциях, что, в свою очередь, способствует предотвращению анонимности криптовалют [6].

Важную для расследования информацию сотрудники ОВД могут получить на компьютерных устройствах, используемых при осуществлении операций с криптовалютами. Своевременное выявление сведений о предполагаемом месте нахождения такой компьютерной техники позволит принять решение о проведении соответствующих мероприятий оперативного и процессуального характера, по результату которых можно обнаружить и изъять соответствующие технические устройства и носители информации.

Необходимо обратить внимание на то, что для покупки, обмена, продажи монет Bitcoin требуется наличие электронного кошелька, например Wallet, управление которым происходит с помощью программы клиента сети Bitcoin. Факт использования этого кошелька, а также иного программного обеспечения, связанного с криптовалютой, может быть обнаружен путем производства осмотра компьютера, ноутбука, смартфона, планшета, а также в последующем при исследовании компьютерной информации. В связи с этим правоохранительным органам рекомендуется фиксировать посещенные пользователем веб-сайты и установленное программное обеспечение, имеющее отношение к операциям с монетами Bitcoin.

Характерным свойством технологии Blockchain считается наличие на информационном носителе файла wallet.dat. Исследование такого файла может способствовать получению информации о злоумышленнике, баланса найденного кошелька. Кроме того, оперативными подразделениями, осуществляющими оперативно-розыскную деятельность путем использования гласного или негласного содействия граждан, могут быть обнаружены дополнительные данные, а также сделаны выводы, подтверждающие операции с криптовалютой.

Таким образом, для предупреждения и пресечения криптопреступности необходимо принятие нормативного правового акта, раскрывающего понятие и правила оборота критовалют, который должен отражать следующие основные аспекты:

- введение обязательной регистрации и учета цифровых кошельков и их владельцев, участвующих в обороте криптовалют;

- определение процедуры конвертации криптовалют в национальные;

- особенности ответственности за нарушение правил оборота криптовалют, в том числе уголовной и административной;

- порядок взаимодействия с органами иностранных государств, занимающимися оборотом и применением цифровых финансовых активов, а также осуществляющими противодействие преступлениям, совершаемым с использованием криптовалют;

- процедуру лицензирования деятельности финансово-кредитных организаций, которые будут осуществлять разнообразные виды операций с деньгами, ценными бумагами и криптовалютами и оказывать финансовые услуги правительству, юридическим и физическим лицам в сфере цифровых активов.

ЛИТЕРАТУРА

1. Bitfury выпустила Crystal — блокчейн-инстумент для финансовых расследований. — URL: http://cryptowiki.ru/news/

2. Абдеева З. Р. Проблемы безопасности электронной коммерции в сети Интернет // Проблемы современной экономики. — 2012. — № 1.

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. Букин М. Активная безопасность ДБО // Банковские технологии. — 2010. — № 10.

5. Евросоюз вводит верификацию владельцев криптовалют для деанонимизации транзакций // URL: https://forklog.com

6. Национальная оценка рисков легализации (отмывания) преступных доходов. 2017—2018 // URL: https://www.nalog.ru/html/sites/www.new.nalog.ru/docs/kont/ot_orleg.pdf

7. Сорокина Я. С., Торжевский К.А. Биткоин: инновационная валюта или инструмент финансовых преступлений? // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. — 2017. — №131. — С. 1301—1310.

8. URL: http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics.