УДК 34

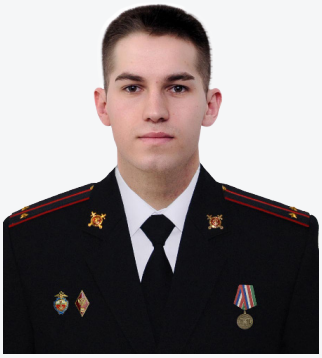
МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТНЫХ АКТИВОВ

FRAUD USING CRYPTOCURRENCY ASSETS

Динар Минзеферович Фарахиев,

оперуполномоченный Управления экономической безопасности и противодействия коррупции МВД по Республике Татарстан (г. Казань)

dfarakhiev@mail.ru



Роман Юрьевич Гольченко,

курсант Казанского юридического института МВД России (г. Казань)

romangolchenko@mail.ru

Ключевые слова:
преступность, мошенничество, криптовалютные активы, криптокошельки, способы борьбы, безопасность.

В настоящее время мошенничество является наиболее актуальным и распространенным преступлением на территории России. Количество регистрируемых преступлений год за годом возрастает. Подвергаясь цифровизации, общество прибегает к использованию криптовалютных активов. Целью настоящее исследования является анализ способов совершения хищений криптовалютных активов путем обмана или злоупотребления доверием. Рассматриваются основные виды мошенничеств, совершаемые с использованием криптовалютных активов. В заключении приводятся рекомендации по минимизации возможности стать жертвой исследуемого вида преступления.

Keywords:
crime, fraud, cryptocurrency assets, crypto wallets, ways to fight, security.

Currently, fraud is the most relevant and widespread crime in Russia. The number of registered crimes is increasing year after year. Being digitalized, society resorts to the use of cryptocurrency assets. Thus, the purpose of this study is to analyze ways to commit theft of cryptocurrency assets by deception or abuse of trust. The main types of fraud committed using cryptocurrency assets are considered.

In conclusion, recommendations are given to minimize the possibility of becoming a victim of the type of crime under study.

На сегодняшний день в обществе проходит активный процесс цифровизации. Рассматривая сферу оборота денежных отношений с точки зрения «координации» субъектов правоотношений, следует отметить, что ранее преобладал непосредственный контакт, однако сегодня исследуемые отношения осуществляются в виртуальной среде, с использованием информационно-телекоммуникационных технологий, в частности с использованием криптовалютных активов.

Одним из наиболее распространенных преступлений на территории Российской Федерации является мошенничество (ст. 159-159.6 УК РФ). Уголовным законодательством мошенничество определяется как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Согласно статистическим данным Главного информационно-аналитического центра МВД России, за 2021 год зарегистрированы 238560 случаев мошенничества (ст. 159 УК РФ), 10258 фактов мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ). В 2022 году по сравнению с 2021 годом показатели киберпреступности в целом остались стабильными. С использованием высоких технологий совершаются каждое четвертое преступление. Прирост зарегистрированных фактов мошенничества составил 4,8% (249984 случаев), на 29% сократилось количество фактов мошенничества с использованием электронных средств платежа (7288 случаев). За первое полугодие 2023 года (январь-июнь) зарегистрированы 163666 фактов мошенничества, что на 43,3% больше, чем за аналогичный период 2022 года (114215), и на 31,5% больше, чем за аналогичный период 2021 года (112032) За январь-июнь 2023 года зарегистрированы 2870 фактов мошенничества с использованием электронных средств платежа, что на 31,7% меньше, чем за аналогичный период 2022 года (4200) и на 47% меньше, чем за аналогичный период 2021 года (5421).

Цифровые финансовые активы и криптовалюта – это новые явления в экономике и праве. В настоящее время большое внимание государства уделяется правовому регулированию цифровых финансовых активов, в частности криптовалютных активов, что подтверждается принятием Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ № 259). Положения данного закона легализуют криптовалюту, но запрещают ее использование в России для оплаты товаров и услуг.

Под цифровыми финансовыми активами законодатель понимает цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных цен-

ных бумаг, которые предусмотрены решением о выпуске цифровых финансовых, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы.

В современном цифровом обществе криптовалюты имеют динамичный характер обновления. Активно создается новая криптовалюта, так как со старой появляются существенные сложности. Связано это с тем, что затруднительнее становится майнинг (процесс производства) ранее появившейся криптовалюты, например Bitcoin, Litecoin, Namecoin и многих других, в результате чего создание новой криптовалюты является менее затратным процессом, чем добыча старой.

В производстве криптовалютных активов используется технология блокчейн, которая дает возможность создавать неограниченное количество видов цифровых денежных средств. Разработчики пытаются добиться высокой популярности цифровых денежных средств и вовлечь в майнинг большое количество пользователей. Одной из задач является создание максимального количества цифровых денежных средств с целью повышения активности со стороны потенциальных инвесторов.

Многократное увеличение объемов криптопреступности обусловливается рядом следующих факторов.

1. Существует потребность в поиске качественно новых механизмов отмывания доходов, полученных преступных путем, в силу увеличения их объема. Данный вывод подтверждают следующие данные: около 80% клиентов организаций, занимающихся отмыванием преступных доходов, – это крупные нелегальные сервисы по продаже порнографии и психоактивных веществ.

2. Правовой вакуум вокруг статуса криптовалют и системы их финансового контроля является мощным стимулом для развития квазифинансовых структур, обеспечивающих сохранность денежных потоков с использованием технологии блокчейн либо занимающихся конвертацией криптовалютных активов в фиатную валюту. В 2018 году на счета сервисов по конвертации около четверти средств пришло от организаций, занимающихся незаконной деятельностью.

3. До настоящего времени не выработан единый подход к определению предупредительной политики в этой сфере. Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) в числе основных препятствий для сотрудничества государств в сфере выявления и пресечения отмывания преступных доходов с использованием цифровой валюты указала неконтролируемые масштабы легализуемых средств, анонимные отношения между пользователями, отсутствие идентификации клиентов, отсутствие единого координационного органа для выработки единой уголовной политики в отношении незаконных криптотранзакций[1].

1 Ключевые определения и потенциальные риски в сфере ПОД/ФТ. URL: ttps://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf (дата обращения: 14.06.2023).

На сегодняшний день мошенничества с использованием криптовалютных активов набирают оборот. Следует отметить, что злоумышленники не останавливаются на стандартных схемах реализации своих преступных умыслов, а шагают «в ногу со временем», разрабатывая новые способы и методы совершения исследуемых преступлений.

К основным видам мошенничества с использованием криптовалютных активов следует относить:

1) использование фишинговых веб-сайтов [3, с. 89] и криптокошельков. В процессе развития информационных технологий киберпреступники научились создавать точную копию сайта, на котором пользователь, сам не подозревая о его неоригинальности, будет майнить или приобретать криптовалюту. Создавая сайт, злоумышленники меняют одну букву сайта, причем из-за идентичности оформления сайта и способа работы с ним пользователю трудно заметить такой обман. Регистрируясь на фишинговых веб-сайтах, пользователь передает свои данные в руки киберпреступников, которые впоследствии распоряжаются ими.

Для хранения криптовалютных активов требуются электронные кошельки, на которых хранятся сами криптовалютные активы, а также все проведенные транзакции в системе блокчейн. Злоумышленники создают фейковые приложения, к примеру GreenAddress; Simple Bitcoin Wallet; GreenbBits Bitcoin Wallet и др., которые используются для хищения средств. После установки приложения пользователь начинает активно пользоваться им, не подозревая о том, что данное приложение не является официальным. После того, как сумма средств на криптокошельке достигает определенного значения, заранее определенного разработчиком, они списываются в пользу злоумышленника;

2) схема Понци. Данная модель хищения средства схожа с финансовой пирамидой, где средства перераспределяются от нижестоящих участников пирамиды к вышестоящим. Схема Понци выстроена на рекомбинации прибыли в пользу инвесторов, которые вложили свои средства в тот или иной проект ранее, за счет инвесторов, вложившихся позже. Одной из самых известных является платформа Bitconnect. В результате своей незаконной деятельности основатель Bitconnect Сатиш Кумбхани был обвинен в мошенничестве с криптовалютами[1].

В 2021 году Центральный Банк обнародовал список компаний, которые занимаются незаконной деятельностью, а именно имеют признаки финансовых пирамид. Таковыми являются: Crypto-Max, Crypto Inc, Crypto Invest, Exchange Coindesk и Secretcryptodeals[2];

3) облачный майнинг. Данное мошенничество заключается в том, что инвесторам предлагают вкладывать средства в развитие центра для майнинга биткоинов, в результате которого инвесторы получают процент. Наиболее

1 Bits Media. Биткоин форум. URL: https://bits.media/organizatoru-piramidy-bitconnect-predyavleny-ofitsialnye-obvineniya/ (дата обращения: 15.06.2023).

2 В черный список ЦБ попали представители криптоиндустрии. URL: https://www.rbc.ru/crypto/news/60b609409a7947268c59456a (дата обращения: 15.06.2023).

прибыльным и менее затратным способом извлечения прибыли является облачный майнинг. Особенность состоит в том, что очень сложно понять, в какой именно момент мошенник присвоил денежные средства инвестора, ведь некоторое время работающий сайт создает видимость прозрачной операции. Один из самых крупных ресурсов облачного майнинга является HashOcean, который гарантировал прибыль в размере 320%. Внезапно данный проект прекратил свою деятельность. Один из инвесторов подал жалобу на HashOcean, в петиции полностью разъяснил ситуацию, согласно которой сайт исчез из онлайн-пространства, а ее владельцами были присвоены средства более шестисот тысяч инвесторов со всего мира в размере, составляющем миллионы долларов[1];

4) фальшивые обменники и криптобиржи. Заработанная с помощью майнинга криптовалюта не может выступать средством платежа, ведь согласно российскому законодательству законным платежным средством на территории Российской Федерации является рубль. Фактически криптовалютные активы обезличены: «невозможно определить, кто является владельцем криптовалюты, так как данная система предполагает полную анонимность»[2]. Владельцу криптовалюты остается лишь обменять ее на фиатные деньги. Злоумышленники предлагают обменять криптовалюту по более выгодному курсу, нежели предлагают популярные биржи (Binance, OKEx, Bit2Me, CoinEx, Indacoin). В результате противоправных действий злоумышленники проектов (например, Project Impulse, bestswapcoins.shop, convert-monet.com, cryptoswapper.ru и др.) присваивают криптовалютные активы инвесторов.

Криптовалютные биржи предлагают внести депозит и приобрести криптовалюту (BTC) на выгодных условиях: от возможностей использования многообразия платежных систем до низких комиссий по операциям. В итоге складывается ситуация, при которой обратно вывести BTC уже не получится;

5) пампинг криптовалюты. Особенностью данного мошенничества является искусственное завышение стоимости криптовалютных активов. Злоумышленники, приобретая криптовалютные активы, начинают распространять информацию среди инвесторов с призывами вложить свои средства в ту или иную валюту под предлогом увеличения ее стоимости в дальнейшем. Для правдоподобности часто используется инсайдерская информация. В результате противоправной деятельности пользователи начинают приобретать «прибыльные» криптовалютные активы, искусственно провоцируя повышение ее стоимости.

Рассмотрев наиболее распространенные способы совершения мошенничеств с использованием криптовалютных активов, предлагаем рассмотреть методику раскрытия и расследования данных преступлений.

Так, И.И. Кучеров пишет, что «методика расследования преступлений в сфере финансов во многом основывается на получении необходимых сведений от

1 HashOcean оказался мошенническим проектом. Livejournal. URL: https://100monet.livejournal.com/64374.html (дата обращения: 15.06.2023).

2 Сделки с криптовалютой: разъяснения ФНП. URL: https://www.garant.ru/news/1545036/ (дата обращения: 15.06.2023).

кредитных организаций, которые представляют их органам расследования в документированном виде на основании официальных запросов» [2, с. 19]. При использовании криптовалюты осуществить такие действия не получится, ведь в рамках криптовалютных транзакций отсутствует посредническая функция банков и небанковских кредитных организаций. Все переводы осуществляются исключительно напрямую от отправителя к получателю. При расследовании преступлений в сфере криптовалютных активов главной целью является выяснение места, с которого были списаны средства. Для этого необходимо установить идентификатор криптокошелька (открытый и закрытый ключи). После этого составляется запрос о предоставлении каких-либо документов или информации об операциях с криптовалютой. Альтернативные платежные средства, использующиеся в Интернете, не имеют администратора или иного лица, отвечающего за единый центр управления переводами. Поэтому правоохранительным органам не представляется возможности адресной подачи такого запроса.

В ходе производства следственных действий необходимо установить целевое предназначение перевода (транзакции). В целях достижения данной цели необходимо осуществлять допрос и очные ставки с участием отправителя и получателя перевода. Любая транзакция оставляет электронный след в системе блокчейн, что помогает с помощью проведения оперативно-розыскных мероприятий установить факты незаконного приобретения криптовалюты.

В процессе раскрытия и расследования исследуемых преступлений оперативникам и следователям целесообразно назначать исследования и экспертизы на предмет получения значимой информации по уголовным делам; оперативным сотрудникам также целесообразно осуществлять осмотр всех электронных устройств, использованных злоумышленниками, по поручениям следователя, а также исследовать предметы и документы, которые были получены в рамках оперативно-розыскного мероприятия «наведение справок».

В процессе раскрытия и расследования важно установить наименование биржи и аккаунта, с которых незаконно были похищение средства – финансовые активы; выявить, каким образом осуществлялась транзакция; зафиксировать суммы транзакций; реквизиты и прочую информацию.

Следует отметить, что цифровые технологии, в том числе система блокчейн, являются принципиально новыми и отличаются от известных классических банковских технологий. Технология блокчейн играет определяющую роль для процесса документирования и доказывания. В.П. Галушин пишет, что цифровые следы предоставляют дополнительные возможности для доказывания фактов преступного использования криптовалютных активов [1, с. 91].

Цифровые следы, оставляемые в сети Интернет, классифицируются на видимые (активные) и невидимые (пассивные). Видимые цифровые следы являются общедоступными, с различимым содержанием сведений; невидимые следы – это метаданные, которые являются сопровождающей информацией к

видимому содержанию. Так, к активным следам относятся электронные письма, сообщения в социальных сетях, в том числе фотографии, видеозаписи, документы, а также оставленные под публикациями комментарии, «лайки», «репосты» и прочее. Пассивными следами являются статистика посещений определенных сайтов, история поисковых запросов, местонахождение и передвижение используемого устройства, его IP-адрес и т.д.

Идентификация цифровых следов в сети Интернет возможна как посредством анализа данных, которые находятся в открытом доступе, так и с помощью получения необходимой информации путем запроса от владельцев серверов, обслуживающих посещенные пользователем сайты, на которых и происходят транзакции [4, с. 44].

На сегодняшний день, обеспечение безопасности криптовалютных активов пользователя является первостепенной задачей онлайн-кошельков и локальных или мобильных программ (Google Authenticator, Coinmarketcap, TradingView[1] DApps, SushiSwap, PancakeSwap и др.). Так, в данных электронных системах широко используются двухфакторная аутентификация и защитная seed-фраза. Смысл двухфакторной аутентификации состоит в том, что пользователь при входе в криптокошелек вводит не только собственный пароль для входа в систему, но и дополнительный одноразовый код, указанный в SMS-сообщении. Однако в связи с развитием информационных технологий преступники научились противостоять и такому способу защиты. Злоумышленники способны перехватить данные SMS-сообщения с целью получения доступа к личному кабинету пользователя и реализации своих корыстных целей. Если пользователь забыл пароль к кошельку, то, согласно принципам политики онлайн-хранилищ, восстановить его будет невозможно. Для этого существует seed-фраза, которая является инструментом получения доступа к кошельку в случае утери основного пароля. Она представляет собой уникальную фразу, состоящую из двенадцати английских букв, не связных между собой по смыслу, которая генерируется системой. Следует принимать во внимание, что утрата кодовых слов повлияет на возможность работы с криптокошельком и хранящимися в нем валютами [4, с. 44].

В настоящее время нами прогнозируется повышение уровня мошеннических действий с использованием цифровых активов, в частности, цифрового рубля, который с 1 августа 2023 года официально стал третьим видом национальной валюты, наряду с наличной и безналичной. Принципиальным отличием цифрового рубля от криптовалюты будет то, что эмитентом первого является Банк России, тогда как у второй нет единого эмитента ввиду децентрализации[2]. Один из его признаков – отсутствие возможности капитализации вкладов с цифровыми рублями, что, на наш взгляд, сыграет «на руку» мошенникам. Кроме того, существует риск создания новых мошеннических схем, по-

1 Полезная загрузка. Что скачать на смартфон для работы с криптовалютой. URL: https://www.rbc.ru/crypto/news/5d2705999a794763c5b1 35af (дата обращения: 26.07.2023).

2 Цифровой рубль. URL: https://cbr.ru/fintech/dr/ (дата обращения: 26.07.2023).

этому государству необходимо обеспечивать тотальный контроль за развитием цифровых сервисов.

Для того чтобы не стать жертвой исследуемого мошенничества, в том числе с использованием методов социальной инженерии, рекомендуется:

– не вкладывать личные денежные средства и не осуществлять переводы криптовалютных активов, опираясь на советы лиц, с которыми пользователь осуществлял взаимодействие в онлайн-пространстве;

– быть бдительным при пользовании социальными сетями, не верить сообщениям, предлагающим получение криптовалютных активов на выгодных условиях;

– хранить ключи, позволяющие получить доступ к цифровым финансовым активам, в безопасных местах, не доступных другим лицам (желательно в автономном режиме, где их нельзя взломать).

В целях предупреждения дальнейшего развития преступности в сфере криптовалютных активов органы государственной власти должны осуществлять задачи по предупреждению мошенничеств, совершаемых с использованием криптовалютных активов, а также по поддержке инвестиционного потенциала населения. Граждане стремятся увеличить уровень своего благосостояния путем размещения личных денежных средств на банковских вкладах. Однако с каждым годом банковские организации предлагают все менее выгодные условия, процентные ставки становятся ниже, уровень инфляции в обществе увеличивается, в результате чего население вынуждено искать более выгодные способы для заработка, не подозревая, что многие из них являются мошенническими.

Библиографический список

1. Галушин, П.В. Сведения об операциях с криптовалютами (на примере Биткойна) как доказательство по уголовному делу / П.В. Галушин, А.Л. Карлов // Ученые записки Казанского юридического института МВД России. – 2017. – Т. 2. – № 4. – С. 91.

2. Кучеров И.И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. – 2018. – № 12. – С. 17-21

3. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С.В. Иванцов, Э.Л. Сидоренко, Б.А. Спасенников [и др.] // Всероссийский криминологический журнал. – 2019. – Т. 13. –№ 1. – С. 85-93. – DOI 10.17150/2500-4255.2019.13(1).85-93.

4. Шнейдерова, Д.И. Криминалистический анализ способов хищений в сфере оборота криптовалют / Д.И. Шнейдерова // Вестник Сибирского юридического института МВД России. – 2020. – № 2(39). – С. 41-48. – DOI 10.51980/2542-1735_2020_2_41.