- расширять международное сотрудничество для оперативного обмена данными и эффективного преследования преступников.

Борьба с преступлениями, связанными с оборотом наркотиков и использованием криптовалют, требует интеграции инновационных технологий и разработки эффективных политико-правовых механизмов, обеспечивающих контроль за финансовыми потоками и предотвращение незаконной деятельности.

Теофило Арнольдо Урбина Павон,
Хосе Сантьяго Эрнандес Араус,
Ледер Рафаэль Руис Арролига,
Серхио Джованни Мендоса Эрнандес,
Ядер Осман Санчес Лопес
Научное руководство при подготовке тезисов:
В.Ю. Жандров, кандидат юридических наук, доцент,
А.В. Токолов, кандидат юридических наук
(Московскийуниверситет МВД России имени В.Я. Кикотя)

Алгоритм выявления и документирования мошенничества, совершаемого с использованием криптовалют.

С ростом популярности криптовалют увеличилось количество преступлений, совершаемых с их использованием. В соответствии со статьями 229 и 230 Закона 641 Уголовного кодекса Республики Никарагуа, мошенничество определяется как преднамеренное введение в заблуждение с целью незаконного обогащения, что влечет за собой уголовную ответственность. Однако правоприменительная практика сталкивается с рядом сложностей, таких как анонимность транзакций, отсутствие строгого регулирования и международный характер преступлений.

Первая зафиксированная криптовалютная транзакция в Никарагуа была совершена в 2014 году, когда гражданин США приобрел участок земли в Сан-Хуан-дель-Сур за 80 биткойнов. С тех пор цифровые активы стали популярны не только среди добросовестных пользователей, но и среди мошенников, применяющих их для проведения нелегальных операций. В данной статье представлен детальный алгоритм расследования преступлений, связанных с криптовалютами, а также меры их предотвращения.

Определение мошенничества с криптовалютами

Криптовалютное мошенничество включает различные схемы обмана, направленные на завладение средствами жертв. Наиболее распространенные виды:

– пирамидальные схемы – обещание высокой прибыли за счет привлечения новых участников без реальной инвестиционной деятельности;

– фальшивые инвестиционные платформы – создание мошеннических сайтов, имитирующих легитимные биржи и фонды, с целью сбора депозитов;

– фишинговые атаки – получение доступа к криптовалютным кошелькам пользователей путем обмана;

– поддельные ico – сбор инвестиций под предлогом запуска новых криптовалютных проектов, после чего организаторы исчезают с деньгами.

Особенность мошеннических схем в Никарагуа заключается в том, что злоумышленники предлагают высокую доходность за короткий срок, убеждая жертв сначала инвестировать небольшие суммы, а затем увеличивать вклады. В момент вывода средств мошенники требуют дополнительных платежей или просто исчезают.

Криптовалютные кошельки и их классификация

1. По подключению к Интернету:

- «горячие» кошельки (онлайн-сервисы, мобильные и десктопные приложения);
- «холодные» кошельки (аппаратные устройства, бумажные носители).

2. По типу устройства:

- мобильные;
- аппаратные;
- настольные.

3. По уровню контроля:

- кастодиальные (управляются третьей стороной);
- некастодиальные (управляются владельцем напрямую).

Знание этих классификаций играет ключевую роль при расследовании преступлений в сфере криптовалют.

Алгоритм расследования преступления

1. Получение заявления от потерпевшего – фиксируются детали преступления, собираются сведения о транзакциях и рекламных объявлениях.

2. Осмотр места преступления – фотографическая фиксация цифровых доказательств, сбор данных о платформе мошенников.

3. Запрос информации у криптовалютной платформы – идентификация владельца кошелька, анализ транзакций в блокчейне.

4. Экспертиза цифровых носителей – исследование устройств жертвы и подозреваемого, восстановление удаленных данных.

5. Идентификация подозреваемых – анализ IP-адресов, цифровых следов, запрос в финансовые учреждения.

6. Документирование транзакций – фиксация движения средств, взаимодействие с банками и платежными системами.

7. Проведение обысков и допросов – изъятие технического оборудования, получение свидетельских показаний.

8. Сотрудничество с экспертами – привлечение криминалистов, использование инструментов анализа блокчейна (Chainalysis, Elliptic, CipherTrace).

9. Запрос в финансовые организации – анализ банковских счетов жертв и подозреваемых.

10. Заключительный отчет – подготовка материалов дела и передача его в судебные органы.

Расследование вымогательства с использованием криптовалют

Вымогательство в сфере криптовалют часто проявляется в виде угроз, хакерских атак и требований перевода средств в цифровых активах. Особенности таких преступлений включают анонимность платежей, сложность отслеживания получателей и применение децентрализованных сервисов. Алгоритм расследования включает:

- анализ зашифрованных сообщений и угроз;
- блокчейн-аналитику для отслеживания маршрутов транзакций;
- запрос данных у интернет-провайдеров и криптовалютных бирж;
- взаимодействие с международными правоохранительными органами.

Противодействие мошенничеству

Для снижения уровня криптовалютного мошенничества необходим комплексный подход:

- просвещение граждан – обучение пользователей правилам безопасности, выявлению мошеннических схем;
- регулирование – введение требований для криптовалютных платформ по регистрации и предоставлению отчетности;
- международное сотрудничество – взаимодействие с правоохранительными органами других стран для отслеживания преступников.

Криптовалютное мошенничество представляет значительную угрозу для пользователей и экономики. Современные технологии позволяют раскрывать такие преступления, но для их эффективного расследования требуется внедрение строгого регулирования, развитие инструментов анализа блокчейна и повышение цифровой грамотности граждан. Только комплексный подход, включающий правоприменительную, техническую и образовательную составляющие, позволит минимизировать риски мошенничества и вымогательства с использованием криптовалют в Никарагуа и других странах.