Секция «LegalTech. Цифровая криминалистика»

Применение методов цифровой криминалистики при расследовании преступлений, связанных с криптовалютой

Научный руководитель – Сидоренко Элина Леонидовна

Савенкова Полина Германовна
Студент (бакалавр)
Московский государственный институт международных отношений, Международный институт энергетической политики и дипломатии, Москва, Россия
E-mail: Sanverst@yandex.ru

Аннотация*: В данной работе исследуется вычислительный артефакт как прогрессивный метод доказывания в уголовном судопроизводстве. Анализируется его роль в расследовании преступлений связанных с криптовалютой, на примере биткойна, изучаются конкретные методы, применяемые для поиска доказательств незаконных действий, связанных с технологией блокчейн.*
Ключевые слова*: криптовалюта, цифровая криминалистика, расследование преступлений*

Цифровая криминалистика является неотъемлемой частью почти каждого уголовного расследования, учитывая объем доступной информации и возможности, предоставляемые электронными данными для расследования и доказательства преступления. Однако в уголовном судопроизводстве цифровые доказательства часто рассматриваются с крайней подозрительностью и неопределенностью [1].

Важным понятием в цифровой криминалистике является понятие вычислительного артефакта. Под вычислительным артефактом понимается все, что создается человеком с помощью компьютера. Артефакт может быть, но не ограничивается, программой, изображением, аудио, видео, презентацией или файлом веб-страницы, биткойн также является вычислительным артефактом. [2]. При расследовании незаконных операций с криптовалютой в первую очередь исследуется, какие артефакты остаются в системе пользователя в результате операций с биткойном, что означают эти артефакты и как их восстановить. На сегодняшний день эти вопросы остаются слабо изученными, тем не менее, играют важную роль.

При первичной регистрации пользователя для работы с биткойнами, ему необходима загрузка программного обеспечения для создания биткойн-кошелька. В биткойн-кошельке перечисляются все транзакции пользователя в системе [3]. Впоследствии, в случае подозрительных действий, при изучении данных пользователя, все данные будут помещены в специальные папки, каждая из которых имеет свою специфическую функцию и в каждой содержаться определенные криминалистические артефакты и информация, которые могут быть использованы в ходе расследования.

В дополнение к доказательственным артефактам, которые могут быть обнаружены на компьютере пользователя, следователи могут также обнаружить артефакты, проведя углубленное исследование блокчейна. Так как блокчейн - это публичная запись транзакций биткойнов, то при необходимости, возможно отследить покупки и действия с биткойнами до других потенциальных подозреваемых [4].

Вещественные доказательства, используемые при расследовании, обеспечивают цифровому делу прочную основу, необходимую для того, чтобы оно могло быть принято судом. Таким образом, важно, чтобы судебные эксперты имели четкое представление о различных криминалистических инструментах и методах, используемых для анализа биткойна, а также о том, какое значение может оказать найденный артефакт на дело [3].

Источники и литература

1) Arshad H., Jantan A., Abiodun O.Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence / Journal of Information Processing Systems. 2018 №14(2). – 30 С.
2) Turner R. Computational Artifacts: Towards a Philosophy of Computer Science. – Электронный ресурс. URL: https :// www . researchgate . net / publication /312626867_ The _ Philosophy _ of _ C omputer _ Science (дата обращения: 20.02.2020).
3) Doran M. A Forensic Look at Bitcoin Cryptocurrency. – Электронный ресурс. URL: https :// digital - forensics . sans . org / community / papers / gcfa / forensic - bitcoin - cryptocurrency _11168 (дата обращения: 20.02.2020).
4) Сидоренко Э. Криминологические риски оборота криптовалюты. – Электронный ресурс. URL:https://cyberleninka.ru/article/n/kriminologicheskie-riski-oborota-kriptovalyuty (дата обращения: 20.02.2020).