ОТЗЫВ

зарубежного научного консультанта на диссертационную работу
Шайзата Медета Жанболатулы
на тему «Разработка методов и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций», представленную на соискание степени доктора философии (PhD)
по образовательной программе «8D06301 – Системы информационной безопасности»

Диссертационная работа Шайзата Медета Жанболатулы посвящена актуальной научно-прикладной задаче разработки методов и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций. Актуальность темы определяется тем, что цифровые активы, включая Bitcoin, все чаще становятся объектом финансового мониторинга и расследования противоправной деятельности. Особенность Bitcoin заключается в сочетании публичности блокчейн-реестра и псевдонимности участников. Данные блокчейна позволяют анализировать движение средств, транзакционные связи и графово-временные закономерности, однако сами по себе не дают однозначной криминалистической интерпретации. Поэтому для киберкриминалистических расследований важны интерпретируемые признаки и воспроизводимые процедуры анализа, требующего экспертной проверки.

Цель исследования заключается в разработке методов и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций. Объектом исследования являются процессы определение нелегальных Bitcoin-транзакции. Предметом исследования выступают модели и методы машинного обучения процессов определение нелегальных Bitcoin-транзакции.

К основным научным результатам диссертации следует отнести разработку графово-временного представления Bitcoin-транзакции и системы криминалистически интерпретируемых признаков. В работе предложены транзакционные, структурно-топологические, локально-контекстные, темпоральные признаки и признаки происхождения средств, позволяющие учитывать положение транзакции в графе, ее окружение, временное поведение и цепочку движения активов. Показано, что расширение признакового пространства такими признаками улучшает качество выявления подозрительных транзакций по сравнению с базовым реконструированным представлением. Автор также анализирует вклад отдельных групп признаков, логику решений модели и ошибки классификации, что делает предложенный подход полезным инструментом аналитической поддержки киберкриминалистического исследования.

Научная новизна диссертации состоит в развитии подхода к анализу Bitcoin-транзакций, при котором модельная классификация дополняется реконструкцией графово-временного контекста и системой криминалистически интерпретируемых признаков. Автором предложено многоуровневое представление транзакции, обоснована применимость разработанных признаков для повышения качества выявления операций с признаками нелегальной активности, а также формализованы вопросы отбора признаков в анонимизированных блокчейн-наборах данных.

Теоретическая значимость исследования заключается в развитии научно-методических основ киберкриминалистического анализа публичных блокчейн-реестров. Практическая значимость диссертации определяется разработкой программно-аналитического инструментария для выявления нелегальных Bitcoin-транзакций.

Достоверность и обоснованность полученных результатов обеспечиваются использованием известных наборов данных, сравнением различных классов моделей, применением релевантных метрик качества, анализом вклада признаков, интерпретацией решений модели и рассмотрением ошибок классификации.

Личный вклад Шайзата Медета Жанболатулы состоит в постановке исследовательской задачи, анализе научной литературы, подготовке и реконструкции данных, разработке криминалистически интерпретируемых признаков , сравнительной оценке моделей машинного обучения, реализации программно-аналитического прототипа и интерпретации полученных результатов.

Считаю, что диссертационная работа Шайзата Медета Жанболатулы выполнена на высоком научном уровне, имеет значительную практическую ценность и соответствует требованиям, предъявляемым к диссертациям на соискание степени доктора философии (PhD) по образовательной программе «8D06301 - Системы информационной безопасности», а ее автор заслуживает присуждения степени доктора философии (PhD).

Доктор технических наук, профессор, профессор
кафедры системного программирования
и специализированных компьютерных систем
Национального технического университета
Украины "Киевский политехнический институт
имени Игоря Сикорского" Терейковский И.А.

Підпис гр.

ЗАСВІДЧУЮ
Відділ кадрів та діловодства
(підпис) (пр-ще)

Відділ кадрів і архівної справи № 6