ОТЗЫВ

отечественного научного консультанта
на диссертационную работу
Шайзата Медета Жанболатұлы
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 Жанболатұлы посвящена актуальной научно-прикладной задаче разработки интерпретируемых моделей машинного обучения и программно-аналитического инструментария киберкриминалистики для анализа транзакций в сети Bitcoin. Актуальность исследования определяется ростом значимости цифровых активов для финансового мониторинга, цифровой криминалистики и расследования киберпреступлений. Публичность блокчейна Bitcoin создает возможности для анализа транзакёционных следов, однако псевдонимность и сложность интерпретации модельных выводов требуют разработки специальных воспроизводимых и объяснимых методов анализа.

Научная проблема работы связана с ограниченной криминалистической интерпретируемостью существующих подходов. Многие модели показывают высокие значения метрик качества классификации, но не всегда позволяют объяснить, почему конкретная транзакция была отнесена к группе риска. Диссертант обоснованно показывает, что для задач киберкриминалистики важна не только точность модели, но и возможность связать результат с наблюдаемыми транзакционными, структурными, временными признаками и признаками предшествующей транзакционной истории.

Цель исследования состоит в разработке методов формирования интерпретируемых признаков и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций.

К основным результатам диссертации следует отнести создание специализированного набора данных Bitcoin-транзакций на основе сведений публичного блокчейна, формирование системы транзакционных, структурно-графовых, локально-контекстных, темпоральных и GAR-признаков предшествующей истории, разработку экспериментального протокола с учетом временной структуры данных и риска утечки данных, программную реализацию предложенного подхода в виде системы киберкриминалистического анализа Bitcoin-транзакций.

Научная новизна исследования заключается в разработке комплексного подхода к выявлению нелегальных Bitcoin-транзакций. Предложена система из 61 криминалистически интерпретируемого признака, формализующих паттерны движения средств и характеризующих локальные графовые отклонения, интенсивность последующего перераспределения и несогласованность транзакции с предшествующей историей. На их основе сформировано набора данных из 87 вычисляемых характеристик и разработана модель, обеспечившая PR-AUC 90,27%, F1-score 83,90% и recall 81,11%. Кроме того, предложен метод отбора анонимизированных признаков на основе генетического алгоритма, его применение позволило сократить набор Elliptic со 166 до 53 признаков и получить F1-score 84,26%, превысив опубликованный результат RF+GCN на 4,7 п.п.. Предложенные решения уменьшают избыточность признакового пространства,

повышают качество классификации и обеспечивают содержательную интерпретируемость результатов анализа.

Достоверность результатов подтверждается использованием известных benchmark-наборов данных, учетом временного разбиения, сравнением моделей, применением релевантных метрик, абляционным анализом, SHAP-интерпретацией, анализом ошибок и фиксацией ограничений. Личный вклад докторанта состоит в подготовке и реконструкции данных, разработке признаков, построении моделей, проведении экспериментов, интерпретации результатов и формировании выводов.

Задачи, сформулированные на основе научных положений и выводов диссертации, выполнены в полном объеме. В ходе выполнения диссертационной работы Шайзат Медет показал способность самостоятельно осуществлять научно-исследовательскую работу, продемонстрировал умение глубоко и всесторонне обобщать научно-техническую литературу, а также обосновывать научную новизну и итоговые результаты исследования. Представленная работа является самостоятельным исследованием, имеющим научно-практическую значимость. Диссертация выполнена на высоком теоретическом уровне и имеет выраженный прикладной характер.

Считаю, что диссертация Шайзата Медета Жанболатұлы является самостоятельным завершенным научным исследованием, соответствует требованиям, предъявляемым к PhD-диссертациям, а ее автор заслуживает присуждения степени доктора философии PhD по образовательной программе 8D06301 – Системы информационной безопасности.

к.ф.-м.н., профессор,
профессор-исследователь кафедры Мусиралиева Ш.Ж.
Кибербезопасность и криптология