

долговечности конструкций и оптимизации использования ресурсов. Перспективы широкого внедрения 3D-графена в строительную практику связаны с дальнейшим совершенствованием технологий его производства и интеграции в строительные процессы.

Трехмерные графеновые структуры закладывают основу для следующего поколения строительных материалов – более прочных, долговечных, многофункциональных и интеллектуальных, способных отвечать вызовам современной архитектуры и строительства.

СПИСОК ЛИТЕРАТУРЫ

1 Что такое 3D-графен. – URL: <https://avadaingraphene.com/what-is-3d-graphene/> (дата обращения: 19.02.2026).

2 3D-структуры, содержащие графен, для тканевой инженерии. – URL: <https://www.sciencedirect.com/science/article/abs/pii/S2468519419302113> (дата обращения: 19.02.2026).

3 Трехмерные графеновые материалы: получение, структуры и применение. – URL: <https://pubs.rsc.org/en/content/articlehtml/2014/ee/c4ee00050a> (дата обращения: 19.02.2026).

Получено 19.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

UDC 343.72

P. S. KURAPY (ГС-21)

Research Supervisor – Master of Philology, lecturer A. S. *DROBYSHEVSKAYA*

TRANSFORMATION OF CRYPTOCRIME UNDER THE INFLUENCE OF AI = ТРАНСФОРМАЦИЯ КРИПТОПРЕСТУПЛЕНИЙ ПОД ВЛИЯНИЕМ ИИ

Artificial intelligence lowers the entry threshold for crypto fraudsters by automating attacks and scaling schemes. The efficiency of AI operations exceeds traditional indicators, but the revenue laundering infrastructure does not keep up with their volumes. AI remains an auxiliary tool – it speeds up analysis, but does not replace an expert in decision-making.

The cryptocurrency market has been gradually integrating into the traditional economic system over the past few years, but this process has been accompanied by an increase in the volume of related crimes. Artificial intelligence (AI) has rapidly moved from the experimental technology phase to a publicly available service. Mostly in the public field, AI is often discussed as a tool for analyzing the blockchain or detecting suspicious transactions, but to a lesser extent, its use as a means of attack.

AI, by virtue of its functioning mechanism, does not create any completely new types of cryptocrimes. But it, in turn, significantly lowers the entry bar for intruders by automating routine attack preparation and allowing fraudulent schemes to be launched on a much larger scale. As a result, methods that previously required serious programming or social engineering skills are becoming available for implementation by "less qualified" scammers.

The availability of fraudulent tools does not guarantee that the income of the attackers will grow proportionally. The number of attacks can go up, while revenue can stand still or even fall. The main thing here is not the number of attempts, but efficiency, that is, the amount of money that the attacker will actually receive for each unit of effort expended.

In order to assess the actual effectiveness, it is necessary to compare schemes that used generative models and content synthesis with those that dispensed with them. So fraudulent transactions can be divided according to whether they are related to suppliers of AI services – those that trade deepfakes and language models. The key indicators of the impact of AI on the effectiveness of crypto fraud are shown in Table 1.

Table 1 – Key indicators of the impact of AI on the effectiveness of crypto fraud [1]

Indicator	AI	non - AI	AI vs non - AI
Average revenue per fraudulent transaction	3,2 million dollars	719 dollars	AI is 4.5 times higher
Median daily revenue	4,838 dollars	518 dollars	AI is 9.3 times higher
Average number of transactions per day	35.1	3.89	AI is 9 times more intense
The share of AI scams in the highly efficient quadrant (time-weighted efficiency)	76 %	–	–

The data in Table 1 indicate a structural, not just quantitative, discrepancy between the two categories of fraudulent transactions. The use of artificial intelligence takes the economics of crime to a different level: the average revenue per scheme turns out to be many times higher not due to single anomalies, but due to a systemic increase in intensity and scale.

Operators using AI tools generate nine times as many transactions per day with a comparable number of active operations. Automation allows you to process more victims at the same time, and the capabilities of deepfakes and language models increase the conversion of contacts into payments with a higher average receipt.

The median daily revenue shows a nine-fold gap. This excludes the interpretation that high AI scams are caused by rare outliers. A steady daily excess is recorded. Artificial intelligence translates fraud from the category of piece trades into a conveyor process with predictably high returns.

Access to AI alone does not guarantee success. The decisive factor is the integration of technology into already functioning criminal infrastructures: phishing plat-

forms, mass SMS mailing services, and sales channels for compromised accounts. In the presence of such integration, efficiency increases by orders of magnitude; in its absence, the indicators remain within the boundaries of traditional schemes.

Micro-level shifts – a multiple increase in the effectiveness of a single fraudulent scheme, automation of attacks, and an increase in transaction intensity – accumulate into macro trends. How exactly did these changes manifest themselves in the overall dynamics of crypto crimes in 2020–2025? And what parallel processes have affected the infrastructure of money laundering? Without an answer to the last question, the picture is incomplete. The legalization of the funds received is an independent stage. Without it, the increase in fraudsters' fees loses its practical meaning.

The 2020–2025 data makes it possible to compare two disparate but interrelated lines. The first is the dynamics of cumulative losses from crypto fraud. This indicator reflects the effectiveness of the attackers. The second, the change in the share of Chinese-language networks (CMLN) in the total amount of laundering through the blockchain, shows a structural restructuring of the logistics of criminal finance. The two rows are not identical in nature. Their joint review gives an idea of how well the professional laundering infrastructure has turned out to be ready to receive the growing volumes of AI-accelerated scams.

The systematization of annual values for both indicators is presented in Table 2.

Table 2 – Dynamics of the main indicators of cryptocrimes, 2020–2025 [1]

Indicator	2020	2021	2022	2023	2024	2025
Fraud losses, billions dollars	~3,5	~5,5	~7,5	~9,5	12,0	14,0
CMLN's share in laundering, %	~5	~10	~15	~18	~20	~20

The dynamics of losses from crypto fraud and CMLN's share in laundering, according to Table 2, did not change synchronously. Losses grew faster than the expansion of Chinese-language networks. The gap between the volume of funds withdrawn and the laundering capacity peaked in the middle of the analyzed period. By 2025, the gap had narrowed but not disappeared. CMLN's infrastructure has adapted to the increased flows, but its bandwidth has remained a constraint. Further growth of fraudulent fees will hit this ceiling without developing other channels or improving the efficiency of current ones.

Artificial intelligence has significantly changed the investigation of crypto-crimes. It accelerates the analysis of blockchain data, helps to identify hidden connections between addresses, transactions and wallets, and also makes it more accurate to search for suspicious patterns in large arrays of transactions [2].

This becomes particularly important when investigating money laundering, embezzlement, and trace concealment schemes through intermediary wallets and anonymization services. Algorithms allow you to quickly separate atypical operations from the usual transaction flow and build probable asset movement chains, which reduces the burden on the analyst and saves time on initial verification.

At the same time, AI does not replace expert assessment. He works well with formal features in the blockchain, but understands the context outside the chain worse: blockchain connections, motives of participants, and procedurally significant details. Therefore, in the investigation of cryptocrimes, the hybrid model remains the most effective, where AI performs an analytical function, and the final conclusions are drawn by a specialist.

Artificial intelligence has not just accelerated certain elements of cryptocrime, but has changed the very logic of fraudulent transactions. It lowered the entry threshold for intruders, expanded the scale of attacks, and made criminal schemes more technologically accessible. At the same time, an increase in the number of episodes does not mean a linear increase in profitability: the key indicator is not the number of attempts, but the effectiveness of each scheme.

A comparison of AI and non-AI operations shows a steady gap in economic efficiency. The use of generative models, deepfakes, and automated content synthesis transforms fraud from a mode of disparate actions into a more stable and productive format. This is especially noticeable where AI is embedded in an existing infrastructure: phishing platforms, mass mailings, networks of compromised accounts, and cashing channels. Without such a bundle, the technological effect remains limited.

At the same time, the environment of money laundering is also changing. The growth of losses from crypto fraud and the expansion of money laundering structures are not proceeding synchronously, but with a noticeable lag. This means that the criminal infrastructure does not always have time to adapt to the amount of funds generated by AI-accelerated schemes. The limiter is the bandwidth of laundering channels, not just the intensity of attacks.

As a result, AI occupies an ambivalent position. On the one hand, it enhances counteraction tools by speeding up the analysis of blockchain data and identifying suspicious connections. On the other hand, it increases the technological complexity of the criminal environment itself. Therefore, the most stable research and practical conclusion is not related to the opposition of a person and an algorithm, but to their joint work, where AI provides scalable analysis, and an expert provides interpretation and procedural assessment.

LIST OF LITERATURE

1 The 2026 Crypto Crime Report. – URL: <https://www.chainalysis.com/wp-content/uploads/2026/03/the-2026-crypto-crime-report-3-17-release.pdf> (date of access: 20.05.2026).

2 Применение технологий искусственного интеллекта и блокчейн-аналитики в системах ПОД/ФТ // CyberLeninka. – URL: <https://cyberleninka.ru/article/n/primenenie-tehnologiy-iskusstvennogo-intellekta-i-blokcheyn-analitiki-v-sistemah-pod-ft-dlya-m> (дата обращения: 20.05.2026).

Получено 29.05.2026