

2. Шевченко, Р. Б., Іващенко, Т. О. (2024). Стагнація транспортної галузі України як результат системних соціальних потрясінь . *Проблеми сучасних трансформацій. Серія: економіка та управління*, (11). <https://doi.org/10.54929/2786-5738-2024-11-03-07>.

3. Мойсеєнко В.В. Характеристика особи злочинця, який вчиняє кримінальні правопорушення у сфері господарської діяльності. *Юридична наука*. 2020. № 1(103). С. 40 – 49.

4. Кузьменко О.В., Січко Н.П. Особливості криміналістичної характеристики привласнення та розтрата, вчиненої співробітниками агропромислового підприємства. *Науковий вісник Ужгородського Національного Університету*. 2023. Серія ПРАВО. Випуск 76: частина 2. С. 167 – 171.

5. Левченко Ю.О., Миронюк Т.В. Кримінологічна характеристика привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем. *Науковий вісник Ужгородського Національного Університету*. 2023. Серія ПРАВО. Випуск 76: частина 2. С. 126 – 132. DOI <https://doi.org/10.24144/2307-3322.2022.76.2.21>

6. Бучинський О. Кримінологічна характеристика особи, яка вчиняє корупційні кримінальні правопорушення. *Věda a perspektivy*. 2024. № 6(37) [https://doi.org/10.52058/2695-1592-2024-6\(37\)-110-119](https://doi.org/10.52058/2695-1592-2024-6(37)-110-119).

Секція 5. ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ У ПРОТИДІЇ ОРГАНІЗОВАНИЙ ЗЛОЧИННОСТІ ТА КОРУПЦІЇ

HABORETS Olha – Associate Professor of the Department of Operational-Search Activities and Information Security, Donetsk State University of Internal Affairs, PhD, Associate Professor

CRYPTOGRAPHIC METHODS IN ENSURING TRANSPARENCY OF FINANCIAL INVESTIGATIONS: CHALLENGES AND PROSPECTS

In today's era of globalization and digital innovation, financial crimes are becoming more sophisticated and pervasive. Criminal organizations and corrupt networks increasingly utilize cutting-edge technologies to obscure illicit activities and launder money, making it difficult for law enforcement to track. Simultaneously, advancements in cryptography, one of the most promising fields of modern science, offer new tools to enhance transparency and security in financial investigations, providing essential support in the fight against these complex crimes.

Cryptographic methods not only safeguard confidential data but also serve as powerful tools for identifying, tracking, and analyzing illegal financial activities. By incorporating cryptography, law enforcement agencies can increase the transparency of financial investigations, reduce the risk of data manipulation, and ensure that financial evidence remains authentic and admissible in legal proceedings. This technology plays a crucial role in modern financial crime investigations, offering a secure framework for uncovering and combating complex illegal transactions.

The implementation of cryptographic solutions in financial investigations presents several challenges. These include the demand for highly skilled specialists, the complexity of integrating cryptographic methods with existing systems, and the potential threat of cybercriminals attempting to bypass security mechanisms. Despite these obstacles, the future of cryptographic technology in law enforcement is promising, offering opportunities to enhance financial investigation processes and improve the security and transparency of financial crime investigations.

This article explores modern cryptographic methods, their role in enhancing the transparency of financial investigations, and the key challenges law enforcement faces, such as specialist requirements, integration complexities, and cybersecurity threats. It will also discuss the vast opportunities that cryptographic advancements offer in improving the effectiveness of financial crime investigations.

Cryptography, as a critical tool for securing information systems, plays a pivotal role in combating financial crimes. Its primary functions include ensuring the confidentiality, integrity, and authenticity of data. This is especially vital in financial investigations, where financial data often becomes the target of manipulation or efforts to obscure illegal activity. Cryptographic technologies facilitate the secure transmission and storage of sensitive data, safeguarding it from unauthorized access or forgery, thereby enhancing the reliability of financial crime investigations.

Modern cryptographic methods are divided into key areas, with symmetric and asymmetric cryptography being two of the most prominent. Symmetric algorithms like AES offer strong data security through a shared key for both encryption and decryption. However, asymmetric methods such as RSA and ECC are more advantageous for financial investigations, as they use a pair of keys (public and private), improving reliability and reducing the risk of data breaches. Asymmetric cryptography also supports the use of digital signatures, ensuring the authenticity of financial documents and transactions.

Another promising area in cryptography is the use of cryptographic hash functions, such as SHA-256 and SHA-3, which are essential for ensuring data integrity. Hashing generates unique digital fingerprints for information, making it impossible to tamper with or alter data without detection. In financial investigations, this plays a crucial role in ensuring the reliability of evidence, which can be critical when presented in legal proceedings, as it confirms the authenticity and consistency of the data throughout the investigation process.

Cryptographic hash functions, such as SHA-256 and SHA-3, are essential tools for ensuring data integrity. By generating unique digital fingerprints, these functions make it impossible to tamper with or alter data without detection. In financial

investigations, this is crucial for maintaining the integrity and reliability of evidence that may be presented in legal proceedings.

Blockchain technology, grounded in cryptography, also enhances financial transparency by creating decentralized, immutable ledgers. This makes it difficult to falsify or obscure transactions and allows investigators to effectively track funds and build comprehensive transaction histories, vital for investigating crimes like money laundering.

However, implementing cryptographic methods in financial investigations poses certain challenges, with cybersecurity being a primary concern. While cryptography serves as a strong defense, it also becomes a target for cybercriminals. The hacking of encryption algorithms or the forgery of digital signatures can compromise investigations, leading to data breaches. To counter these risks, cryptographic algorithms must be continuously improved, and cutting-edge technologies like quantum cryptography, which promises nearly unbreakable encryption, should be adopted to ensure absolute protection against cyberattacks.

Another significant challenge is the legal regulation surrounding cryptographic technologies. Cryptography must align with national and international legal standards, necessitating the development of clear legal frameworks for its use in financial investigations. Additionally, law enforcement agencies may encounter difficulties in accessing encrypted data if they lack the legal authority or technical capacity to decrypt it. Balancing the need for privacy with the ability of law enforcement to access crucial data for investigations remains a critical issue in the legal regulation of cryptographic methods.

Despite these challenges, the potential for cryptographic methods in financial investigations is vast. The advancement of artificial intelligence and machine learning technologies may automate the analysis of large volumes of cryptographically protected data, enhancing law enforcement efficiency in tackling financial crimes. Moreover, integrating cryptography with other technologies like blockchain and smart contracts offers new possibilities for transparent monitoring and auditing of financial transactions, creating more robust systems to detect and prevent illicit activities.

In conclusion, modern cryptographic methods hold great potential for enhancing financial investigations. They offer improved data security, transparency, and accuracy, which are crucial for detecting and preventing financial crimes. However, their successful application hinges on overcoming technical challenges, such as cybersecurity threats, and legal barriers, including the need for clear regulations and lawful access to encrypted data. With continued advancements and careful regulation, cryptographic technologies can become essential tools in law enforcement's fight against financial crime.

REFERENCES:

Haborets O. Ensuring cybersecurity of Ukraine against cyberterrorism threats: a systematic approach. *Scientific innovations and advanced technologies*. Issue № 11(25) 2023. Pp. 197–205.