spillovers, highlighting the importance of linkages between foreign investors and local SMEs. International experience demonstrates that Smart Customs and Single Window systems can reduce administrative and time costs in cross-border trade. Integrating these systems with artificial intelligence, distributed ledger technologies, and the Internet of Things expands opportunities for digital verification, customs control, cargo monitoring, and supply-chain transparency. These mechanisms can facilitate SME integration into GVCs by reducing barriers to international production networks. The study's scientific novelty lies in developing an integrated approach that combines digital, trade, and investment mechanisms for GVC integration. The study's practical significance is reflected in the proposed strategic directions for trade and digital policy. Further research should quantitatively assess the complementary effects of digital readiness and trade facilitation on countries' participation in GVCs.

Keywords: *digital transformation, global value chains, digital trade, international trade, Single Window systems, digitalization.*

Стаття надійшла до редакції / Received 04.08.2026 Прийнята до друку / Accepted 22.08.2026 Опубліковано/ Published 04.10.2026

Бібліографічний опис статті:

Осадчук В.Є. Цифрова трансформація як драйвер участі у глобальних ланцюгах вартості. Актуальні проблеми інноваційної економіки та права. 2026. № 4. С. 247-253.

Osadchuk V. Digital Transformation as a driver of participation in global value chains. Actual problems of innovative economy and law. 2026. No. 4, pp. 247-253.

УДК: 336.71.078.3; JEL Classification: G21, G28, K42 **DOI: https://doi.org/10.36887/2524-0455-2026-4-48**

PANASENKO Ganna, Doctor of Economics, Associate Professor, Professor of the Department of Financial Investigations and Economic Security at the Research and Educational Institute of Economic Security and Customs Affairs, State Tax University, Irpin; Professor of the Department of Economics and Entrepreneurship at the Kyiv Institute of Business and Technology, Ukraine, https://orcid.org/0000-0002-6743-6728

THE USE OF SUSPICIOUS ACTIVITY INDICATORS BY BANKING INSTITUTIONS TO DETECT ILLICIT CRYPTOCURRENCY TRANSACTIONS

Panasenko G. The use of suspicious activity indicators by banking institutions to detect illicit cryptocurrency transactions.

Many recent publications focus on the overall economic damage caused by the shadow economy, while researchers overlook the specific challenges of combating cross-border bribery at the corporate level. Furthermore, few in-depth studies explain how to proceed when public figures and senior management of multinational companies are involved in illegal schemes, rendering standard compliance and audit procedures incapable of delivering effective results. This study aims to systematize contemporary tools for detecting hidden corruption in international commercial transactions, assess their effectiveness within the corporate control system, and develop a conceptual multi-level model for identifying transnational bribery. The study uses a range of general scientific and specialized methods, including analysis and synthesis to examine the theoretical foundations of detecting covert corruption; comparative analysis to assess the effectiveness of various detection channels; a systemic-structural approach to develop a multi-level model; and statistical methods to process empirical data. The research has revealed that isolated anti-bribery tools (such as internal audit alone or monitoring by tax authorities alone) cannot provide reliable protection for the global market. In response, the author proposes a monitoring model comprising four sequential stages. It envisages the gradual flow of information. are unable to provide reliable protection for the global market. In response to these challenges, the author proposes a monitoring model comprising four sequential stages. It envisages the gradual flow of information from.

Keywords: *transnational bribery; public officials; international commercial transactions; corporate control; compliance.*

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© *PANASENKO Ganna*, **2026**

Statement of the problem. Virtual assets and related services stimulate financial innovation; however, their unique characteristics open up new opportunities for criminals seeking to launder illicit proceeds or finance illegal activities. The global nature, distributed structure, high transaction speed, and limited transparency make convertible virtual currencies (CVCs) an attractive alternative to traditional payment systems. Malicious actors actively use cryptocurrencies to service shadow markets (the darknet), evade sanctions, execute fraudulent schemes, engage in drug trafficking, and extract ransomware payments, as clearly illustrated in Fig. 1.

An additional layer of complexity for supervisory authorities comes from anonymity-enhancing technologies such as cryptocurrency mixers, anonymity-enhanced cryptocurrencies (AECs), and decentralized finance (DeFi) protocols, which often operate outside the legal framework and may circumvent anti-money laundering (AML) requirements.

Despite criminals' attempts to conceal the origin of funds within blockchain networks, they often must interact with the traditional financial system to convert virtual assets into fiat money. At this stage, banks must assess illicit financing risks and identify suspicious transactions.

Specialized suspicious activity indicators are crucial for detecting these threats effectively. However, because the cryptocurrency market continues to evolve, these markers cannot remain static and require regular updates. This objective shaped the choice of this article's topic.

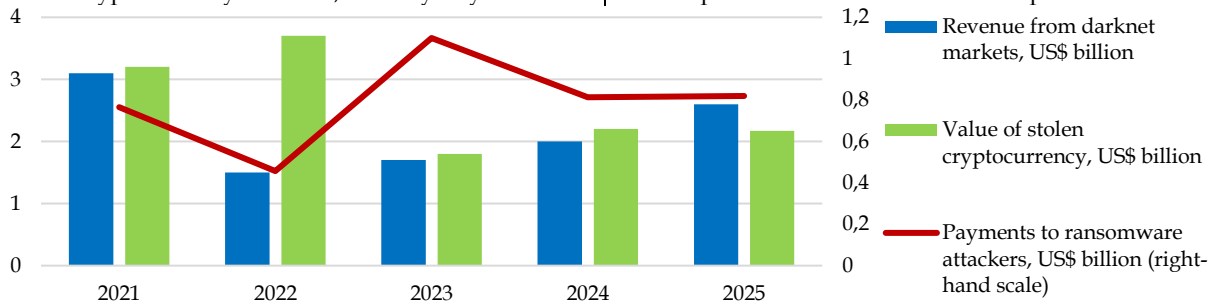


Fig. 1. Dynamics of specific types of illicit activity involving cryptocurrencies* [1].

**For 2025, the figure of $2.17 billion relates only to the period January–June 2025*

Analysis of recent research and publications. Contemporary research on AML in the crypto industry encompasses regulatory, behavioral, and algorithmic aspects. An assessment of FATF standards implementation revealed significant gaps in supervising cross-border transactions and identifying beneficial owners in the DeFi sector [2]. As studies by K. Boguslavska demonstrate, attempts to integrate virtual asset risks into national AML systems are complicated by a lack of harmonized quantitative cross-border data [3]. In parallel, the systematization of Web3 RegTech solutions conducted by Q. Mao et al. [4], and Panasenko G., Hurochkina V., Shtovba S. [5] has exposed the challenges of scaling academic compliance models, cross-chain tracing, and the monitoring of private protocols.

M. A. Naheem's analysis of regulatory and legal contradictions highlights the fundamental difficulties of applying

traditional fiat currency laws to decentralized services, which require the banking sector to radically revise its risk assessment models [6]. As studies by D. Dupuis and K. Gleason show, evolving money-laundering methods create a continuous "regulatory dialectic," in which retaliatory restrictions by supervisory authorities often burden legitimate businesses, while criminals keep finding new "open doors" to bypass monitoring systems [7]. Additionally, C. Leuprecht and co-authors' assessment of transnational criminal schemes exposed the global financial system's critical vulnerability to third-party cryptocurrency exchanges that neglect KYC procedures [8]. These authors argue that malicious actors use virtual assets predominantly at the "placement" and "layering" stages; however, their dependence on fiat conversion at the "integration" stage and the mass transition to private altcoins render existing supervisory mechanisms insufficient to deter cybercrime.

The purpose of the research. The article aims to systematize international approaches to financial monitoring of virtual assets and to develop a new conceptual profile of behavioral indicators for banking institutions, aimed at proactively detecting shadow corporate crypto-intermediaries within the global AML system.

Presentation of the main research material. Banking institutions are the key link in the transition of virtual assets into traditional financial circulation. Despite the pseudonymity of blockchain transactions, laundering illicit proceeds generally requires converting them into fiat money or integrating them into banking products; as a result, banks act as a key "chokepoint" for most money-laundering schemes involving virtual assets. Banks implement their role in the AML system through customer identification, monitoring cryptocurrency-to-traditional-money exchange transactions, reassessing risk, and filing suspicious activity reports (SARs) on time. At the same time, the cross-border nature of transactions, the elimination of traditional intermediaries, and regulatory contradictions significantly complicate the practical execution of these functions.

To understand the architecture of crypto asset laundering and accurately position banking control within this chain, it is necessary to trace the full lifecycle of illicit funds. Fig. 2 presents a conceptual scheme of how illicit proceeds transform, showing the stages of obfuscation within the blockchain environment and their subsequent integration into the traditional financial system.

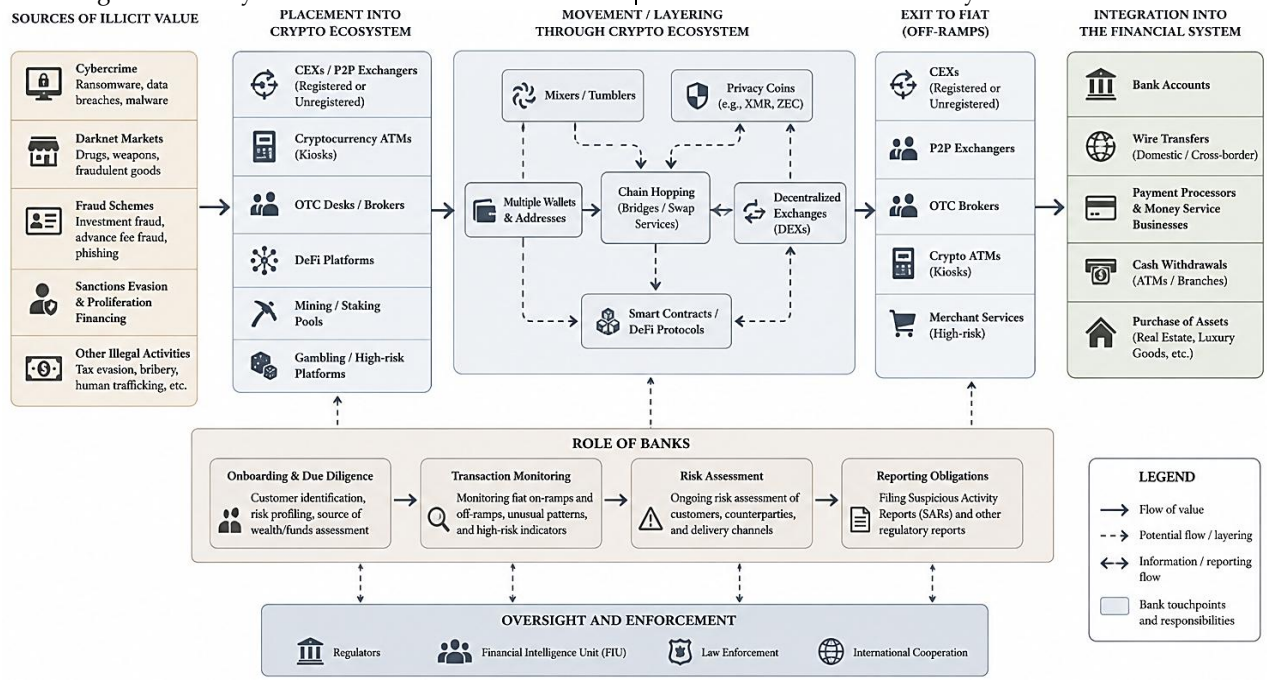


Fig. 2. Scheme of illicit value transformation in the crypto ecosystem and the role of banking control in the financial monitoring system (completed by author)

As shown in Fig. 2, illicit value passes through the stages of formation and placement in the virtual environment (exchanges, P2P exchangers, crypto ATMs, OTC platforms, DeFi), layering (mixers, privacy coins, multiple wallets, chain-hopping, decentralized exchanges, smart contracts), and exit to fiat currency with subsequent integration into the financial system. The last two stages concentrate bank functions—due diligence, transaction monitoring, risk assessment, and reporting to regulators and law enforcement agencies —making banks the final line of defense in AML/CFT.

The layering stage presents a particular challenge for bank compliance, as malicious actors use cross-network transfers, smart contracts, and decentralized protocols that impede tracking of money movement on the blockchain from its original source to the ultimate recipient. Consequently, by the time assets enter the fiat environment, traditional financial monitoring algorithms often prove insufficient: incoming transactions are frequently disguised as legitimate activity through P2P platforms or over-the-counter (OTC) brokers. Therefore, banks' final barrier role requires a shift from linear transaction analysis to proactive behavioral risk assessment. This underscores the critical dependence of corporate control systems on a two-way exchange of intelligence with Financial Intelligence Units (FIUs) and law enforcement agencies, and also necessitates implementing enhanced, dynamically updated suspicious activity indicators sensitive to atypical patterns at the intersection of fiat and cryptocurrency ecosystems [9].

The effectiveness of these functions depends directly on compliance departments having up-to-date suspicious activity indicators.

Banks should begin building a proactive model for monitoring suspicious cryptocurrency transactions by systematizing advanced international experience and adapting global best practices (in particular, FATF guidance, FinCEN analytical reports, and Egmont Group typologies) to the realities of modern bank compliance. In the author's view, traditional markers of suspicion applied to fiat transactions require significant calibration in the crypto context. As the analysis of international standards shows, the primary line of banking control relies on aggregated groups of risk indicators, which can be conditionally divided into four key domains: behavioral anomalies of the client, transactional atypicality, technological obfuscation markers, and jurisdictional risks.

For the banking sector, the main challenge is limited visibility into on-chain data. A financial institution typically records only the fiat "footprint" of a transaction—the moment funds enter a cryptocurrency platform or exit back into

the traditional banking system. Consequently, baseline indicators should be focused on identifying discrepancies between the client's declared profile and their actual economic activity at the intersection of the two financial worlds.

For clarity and to support a global perspective, Table 1 systematizes baseline indicators of suspicious activity in the crypto sphere, adapted for banking institutions.

Taken together, the markers in the table suggest that modern AML methodology already provides banking institutions with tools to detect baseline anomalies in crypto transactions. A single indicator does not necessarily prove money laundering; however, combining indicators (the simultaneous "triggering" of several markers) provides sufficient grounds to conduct an Enhanced Due Diligence investigation and suspend transactions.

Nevertheless, a critical analysis of this generally accepted paradigm reveals its significant conceptual flaw. Most indicators regulated by the FATF and national regulators are historically oriented toward the individual user—a retail client (natural person) attempting to launder relatively small volumes of funds through primitive structuring or direct interaction with suspicious crypto exchanges. This approach has proven effective in combating low-level cybercrime, but it is practically useless against professional transnational money-laundering networks.

The shadow economy is now shifting from individual laundering schemes to complex institutional infrastructure. Under these conditions, malicious actors camouflage flows of illicit liquidity not through individual accounts, but by creating seemingly legitimate corporate structures.

Table 1

Typology of baseline indicators for the laundering of illicit proceeds through virtual assets

Risk category	Nature of suspicious activity	Fiat manifestation in banking monitoring systems
Profile and KYC anomalies	Discrepancy between crypto-transaction volumes and the client's actual income level; concealment of the origin of assets.	A sharp increase in turnover on the accounts of individuals with low official income (students, the unemployed). The client's refusal or inability to provide documentary evidence of the source of funds invested in virtual assets, or evidence of their accumulation history.
Structuring and dynamics	Structuring of transactions to bypass financial monitoring thresholds; abnormal velocity of capital turnover.	Multiple regular transfers of small amounts (just below the mandatory control threshold) to cryptocurrency exchanges or P2P platforms. Immediate withdrawal of incoming fiat funds from the account right after their conversion from cryptocurrency (the "transit nature" of the account).
Infrastructural and technological markers	Use of high-risk intermediaries or anonymization tools (mixers, privacy coins) prior to exiting into fiat.	Incoming payments from unlicensed virtual exchanges, P2P services with weak KYC policies, or from crypto ATM operators. Regular fund transfers to the accounts of companies providing cloud mining services without apparent economic logic.
Geographical determinants	Interaction with jurisdictions having a weak AML regime, or discrepancy between IP addresses and the declared place of business.	Initiation of payments to VASPs registered in offshore zones or countries from the FATF "grey/black lists". Systematic fund transfers to foreign counterparties whose activities are related to crypto asset turnover, in the absence of foreign trade contracts.

Compiled by the author based on: [2, 10, 11].

To bridge this conceptual gap, this study proposes shifting financial monitoring toward detecting "Shadow OTCs" and so-called "Nested Services." Shadow intermediaries are understood as formally legitimate corporate structures (legal entities) that covertly function as unlicensed virtual asset exchange points, over-the-counter brokers, or P2P liquidity aggregators, serving the interests of transnational cybercrime.

Outwardly, such companies may masquerade as entities within the real sector of the economy—IT consulting, marketing agencies, logistics, or wholesale trading firms. However, their actual economic substance is reduced to bridging shadow crypto assets and the traditional banking system. The primary threat is that such structures accumulate fiat flows, mix illicit liquidity with legitimate funds (commingling), and then integrate them into the global financial network via classic cross-border wire transfers. Traditional bank compliance, focused on single-transaction analysis, often overlooks such schemes and algorithmically treats them as ordinary high-intensity business activity.

To detect this activity, we propose a specialized profile of behavioral indicators developed by the author to identify hidden corporate crypto-intermediaries. The proposed marker system is based not on a static assessment of limits, but on a comprehensive analysis of the legal entity's operational pattern. Thus, the determinants of a corporate client's high-risk activity include the following.

1. Abnormal cash flow typology (transit multiplier). The formation of the corporate account's incoming balance predominantly through mass, unstructured (fan-type) transfers from unrelated individuals (C2B), followed by the immediate (within 1-2 banking days) aggregation and withdrawal of funds in large tranches in favor of foreign financial, payment, or investment institutions (B2B).

2. Absence of basic operational load (phantom business). A complete or critical absence of operating expenses typical for the declared type of activity. A legal entity generating multi-million turnovers does not make commensurate payments for commercial real estate leasing, utilities, or logistics, nor does it have an adequate payroll fund and corresponding tax contributions.

3. Discrepancy between economic purpose and payment behavior. A critical divergence of the declared economic activity codes (e.g., software development) from the actual purposes of the payments. The systematic use of extremely vague formulations ("for consulting services," "account replenishment," "under contract No...." without specification) coupled with an ultra-high transaction frequency.

4. Infrastructural integration with high-risk gateways. The systematic use of fiat accounts to interact with cross-border payment aggregators (Payment Service Providers — PSPs) and neobanks known for lenient policies toward the crypto industry, without an objective business necessity (foreign trade contracts) for the company's core business.

Implementing the proposed corporate indicators in banking institutions' scoring models will enable a qualitative shift from reactive compliance to proactive threat hunting. Recognizing shadow OTC brokers at the early stages of their integration into the banking system will provide the opportunity not only to block isolated attempts to withdraw illicit crypto proceeds into fiat but also to dismantle transnational nodes of money laundering infrastructure. Ultimately, this will neutralize the banking sector's vulnerability to "nested services" and significantly increase the overall effectiveness of corporate control within the global economic security system.

Conclusions and prospects for further research. The research shows that evolving virtual asset laundering methods require a fundamental revision of banking anti-money laundering procedures. The study establishes that the critical vulnerability in the traditional financial sector today stems not from retail clients, but from the institutionalization of illegal exchange through fictitious corporate entities.

The author's approach to detecting hidden activity transforms corporate compliance from a tool for retrospective anomaly recording into a preventive barrier. Evaluating a business through the prism of transit multipliers and phantom operational load enables financial institutions to algorithmically identify professional illicit proceeds-laundering nodes at early stages.

The practical value of the proposed set of risk indicators lies in its readiness for direct integration into scoring

AML systems and modern RegTech platforms. Prospects for further scientific research include developing mathematical models for weighted assessment of each described trigger, as well as designing an architecture for secure cross-institutional data exchange among banks, licensed crypto exchanges, and financial intelligence units using machine learning algorithms.

Література.

1. ***Chainalysis.*** *The 2026 Crypto Crime Report*. 2026. URL: https://www.chainalysis.com/reports/crypto-crime-2026/
2. ***Financial Action Task Force.*** *Seventh targeted update on implementation of the FATF standards on virtual assets/VASPs*. 2026. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html
3. ***Boguslavska, K.*** *Basel AML Index 2025: 14th public edition – Global money laundering and financial crime risk ranking*. Basel Institute on Governance, 2025. URL: https://index.baselgovernance.org
4. ***Mao, Q., Wang, J., Liu, Y., Zhu, L., Chen, J., Yan, J.*** *SoK: Web3 RegTech for cryptocurrency VASP AML/CFT compliance*. arXiv, 2025. DOI: https://doi.org/10.48550/arXiv.2512.24888
5. ***Panasenko, G., Hurochkina, V., Shtovba, S.*** Two-level model information system for RegTech-monitoring the reporting entities in risk-based supervision. *CEUR Workshop Proceedings*. 2026. Vol. 4225. P. 25–39. URL: https://ceur-ws.org/Vol-4225/
6. ***Naheem, M. A.*** Regulating virtual currencies – The challenges of applying fiat currency laws to digital technology services. *Journal of Financial Crime*. 2018. Vol. 25, No. 2. P. 562–575. DOI: https://doi.org/10.1108/JFC-08-2016-0055
7. ***Dupuis, D., Gleason, K.*** Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime*. 2021. Vol. 28, No. 1. P. 60–74. DOI: https://doi.org/10.1108/JFC-06-2020-0113
8. ***Leuprecht, C., Jenkins, C., Hamilton, R.*** Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*. 2022. Vol. 30, No. 4. P. 1036–1054. DOI: https://doi.org/10.1108/JFC-07-2022-0161
9. ***Panasenko, G., Hurochkina, V.*** Intelligent compliance as a fundamental tool for Ukraine's economic security. In A. Semenov, I. Yepifanova, J. Kajanová (Eds.), *Data-Centric Business and Applications: Modern Trends in Financial and Innovation Data Processes 2025*. 2026. Vol. 272. P. 1–19. Springer. DOI: https://doi.org/10.1007/978-3-032-06608-4_1
10. ***Financial Action Task Force.*** *Virtual assets red flag indicators of money laundering and terrorist financing*. FATF, 2020. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Virtual-assets-red-flag-indicators.html
11. ***Financial Crimes Enforcement Network.*** *Advisory on illicit activity involving convertible virtual currency* (FIN-2019-A003). U.S. Department of the Treasury, 2019. URL: https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

References.

1. ***Chainalysis.*** (2026). *The 2026 Crypto Crime Report*. URL: https://www.chainalysis.com/reports/crypto-crime-2026/
2. ***Financial Action Task Force.*** (2026). *Seventh targeted update on implementation of the FATF standards on virtual assets/VASPs*. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html
3. ***Boguslavska, K.*** (2025). *Basel AML Index 2025: 14th public edition – Global money laundering and financial crime risk ranking*. Basel Institute on Governance. URL: https://index.baselgovernance.org
4. ***Mao, Q., Wang, J., Liu, Y., Zhu, L., Chen, J., Yan, J.*** (2025). *SoK: Web3 RegTech for cryptocurrency VASP AML/CFT compliance*. arXiv. DOI: https://doi.org/10.48550/arXiv.2512.24888
5. ***Panasenko, G., Hurochkina, V., Shtovba, S.*** (2026). Two-level model information system for RegTech-monitoring the reporting entities in risk-based supervision. *CEUR Workshop Proceedings*, 4225, 25–39. URL: https://ceur-ws.org/Vol-4225/
6. ***Naheem, M. A.*** (2018). Regulating virtual currencies – The challenges of applying fiat currency laws to digital technology services. *Journal of Financial Crime*, 25(2), 562–575. DOI: https://doi.org/10.1108/JFC-08-2016-0055
7. ***Dupuis, D., Gleason, K.*** (2021). Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime*, 28(1), 60–74. DOI: https://doi.org/10.1108/JFC-06-2020-0113
8. ***Leuprecht, C., Jenkins, C., Hamilton, R.*** (2022). Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 30(4), 1036–1054. DOI: https://doi.org/10.1108/JFC-07-2022-0161
9. ***Panasenko, G., Hurochkina, V.*** (2026). Intelligent compliance as a fundamental tool for Ukraine's economic security. In A. Semenov, I. Yepifanova, J. Kajanová (Eds.), *Data-Centric Business and Applications: Modern Trends in Financial and Innovation Data Processes 2025*. Vol. 272, 1–19. Springer. DOI: https://doi.org/10.1007/978-3-032-06608-4_1
10. ***Financial Action Task Force.*** (2020). *Virtual assets red flag indicators of money laundering and terrorist financing*. FATF. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Virtual-assets-red-flag-indicators.html
11. ***Financial Crimes Enforcement Network.*** (2019). *Advisory on illicit activity involving convertible virtual currency* (FIN-2019-A003). U.S. Department of the Treasury. URL: https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

Abstract.

Панасенко Г. Використання банківськими установами індикаторів підозрілої діяльності для виявлення незаконних операцій із криптовалютою.

У статті розглядається актуальна проблема необхідності модернізації механізмів банківського фінансового моніторингу на тлі активного використання віртуальних активів тіньовим сектором. У ситуації, коли кредитні організації виступають ключовим шлюзом інтеграції кримінальних капіталів у фіатне середовище, традиційні методи AML-комплаєнсу, орієнтовані на роздрібних користувачів, втрачають актуальність. Метою роботи є формування оновленої парадигми ризик-орієнтованого нагляду для виявлення прихованих транснаціональних мереж обміну криптовалют. У статті наведено концептуальну схему життєвого циклу легалізації незаконних коштів у криптоекосистемі, яка дозволяє чітко визначити критичні точки банківського контролю на етапі виведення активів у фіатну валюту. У процесі дослідження зазначено, що сучасний ландшафт відмивання грошей змістився у бік інституціоналізації: нелегальні доходи легалізуються через складні корпоративні структури, що маскуються під законну господарську діяльність. На основі синтезу міжнародних стандартів контролю та аналізу вразливостей міжмережевих транзакцій запропоновано концептуально новий підхід до оцінки ризиків відмивання незаконних доходів, пов'язаних із криптовалютами. Цей підхід грунтується на спеціалізованому профілі поведінкових детермінант, спрямованому на виявлення «тіньових брокерів» та прихованих платіжних шлюзів у корпоративному сегменті банку. Сформований інструментарій передбачає глибокий аудит операційної адекватності юридичних осіб та фіксацію розбіжностей між декларованими бізнес-процесами та фактичною динамікою платежів. Очікується, що застосування запропонованих маркерів забезпечить перехід інституційного контролю ризиків відмивання грошей до стратегії попереджувального виявлення загроз у банківських установах. Результати дослідження мають високу прикладну значимість для калібрування автоматизованих скорингових систем та розширення можливостей архітектури RegTech у сфері AML.

Ключові слова: *криптовалюта, банк, фінансовий моніторинг, ризик, відмивання грошей, корпоративний сегмент, платежі, фіатні гроші.*

Стаття надійшла до редакції / Received 05.09.2026 Прийнята до друку / Accepted 08.09.2026 Опубліковано/ Published 04.10.2026

Бібліографічний опис статті:

Панасенко Г. Використання банківськими установами індикаторів підозрілої діяльності для виявлення незаконних операцій з криптовалютою. Актуальні проблеми інноваційної економіки та права. 2026. № 4. С. 253-256.

Panasenko G. The use of suspicious activity indicators by banking institutions to detect illicit cryptocurrency transactions. Actual problems of innovative economy and law. 2026. No. 4, pp. 253-256.