UDC 336.71:343.9
JEL G21, K42, C53
DOI: https://doi.org/10.32782/2786-8273/2026-14-23

Ganna Panasenko
Doctor of Economics, Associate Professor,
Professor of the Department of Financial Investigations and Economic Security,
Research and Educational Institute of Economic Security and Customs Affairs,
State Tax University, Irpin;
Professor of the Department of Economics and Entrepreneurship,
Kyiv Institute of Business and Technology
ORCID: https://orcid.org/0009-0008-0484-7045

Панасенко Г.О.
Науково-освітній інститут економічної безпеки та митної справи
Державного податкового університету;
Київський інститут бізнесу та технологій

ADAPTIVE MANAGEMENT IN MODERN BANKS TO PREVENT CROSS-BORDER MONEY LAUNDERING

АДАПТИВНИЙ МЕНЕДЖМЕНТ У СУЧАСНИХ БАНКАХ ДЛЯ ЗАПОБІГАННЯ ТРАНСНАЦІОНАЛЬНОМУ ВІДМИВАННЮ ГРОШЕЙ

Abstract. Introduction: *traditional banking control mechanisms are highly vulnerable to complex global money laundering networks, necessitating a transition toward adaptive risk management.* ***Purpose.*** *To develop a conceptual model of an adaptive transaction risk management ecosystem capable of preemptively detecting transnational illicit financial flows.* ***Methods.*** *Network graph analysis, predictive machine learning, systematisation, grouping.* ***Results.*** *The proposed architecture merges internal banking analytics with macro-level RegTech. By utilizing topological graph analysis and explainable artificial intelligence, it uncovers hidden transactional pathways, ensures transparent risk prioritization, and continuously retrains algorithms in real time.* ***Conclusion.*** *Transitioning to a dynamic, predictive compliance framework enables banks to proactively block the integration of illicit proceeds. Future research will focus on the empirical validation of the model using large-scale interbank datasets.*

Keywords: *adaptive management, commercial banks, transnational money laundering, financial monitoring, compliance risks, predictive analytics, machine learning, RegTech.*

Анотація. Вступ. *Сучасне управління комерційними банками стикається з безпрецедентними викликами, зумовленими глобальними транснаціональними мережами відмивання грошей, які використовують децентралізовані роздрібні рахунки та складні неформальні системи переказу коштів, щоб обійти традиційні механізми дотримання вимог. Традиційні детерміновані алгоритми контролю залишаються вкрай вразливими до горизонтальних мереж та «тіньових дзеркальних» переказів, що зумовлює необхідність глибокої методологічної трансформації в напрямку адаптивного управління ризиками транзакцій.* ***Мета.*** *Розробка концептуальної моделі екосистеми адаптивного управління транзакційними ризиками для комерційних банків, призначеної для превентивного виявлення та аналізу мінливих транснаціональних незаконних фінансових потоків та кримінальних типологій у всіх операційних юрисдикціях.* ***Методи.*** *Структурно-функціональний аналіз, концептуальне моделювання та синтез передових емпіричних регуляторних практик. Основним* ***результатом*** *є багаторівнева архітектура, яка поєднує внутрішню банківську прогнозну аналітику з платформами регуляторних технологій (RegTech) макрорівня. Запропонована модель базується на топологічному аналізі графів прихованих мережевих зв'язків, передбачає багатофакторну оцінку поведінкових аномалій та обробку природної мови для виявлення прихованих шляхів здійснення транзакцій.* ***Висновок.*** *Отримані результати підтверджують, що перехід від ізольованих статичних правил дотримання нормативних вимог до динамічної, прогностичної та адаптивної системи управління ризиками дає змогу банкам проактивно запобігати інтеграції незаконних доходів у легальну фінансову систему. Запропонована модель оптимізує операційні навантаження, одночасно зміцнюючи глобальну архітектуру фінансової безпеки. Майбутні наукові дослідження передбачають емпіричну валідацію розробленої моделі з використанням масштабних наборів даних про міжбанківські транзакції та її інтеграцію в автоматизовані системи стрес-тестування банків.*

Ключові слова: *адаптивний менеджмент, комерційні банки, транснациональне відмивання грошей, фінансовий моніторинг, комплаєнс-ризики, предиктивна аналітика, машинного навчання, регтех.*

Problem Statement and Its Relevance. Amid globalization and end-to-end digitalization, banking management increasingly faces threats from transnational money laundering networks (MLNs) seeking large volumes of freely convertible currency to meet demand from citizens evading domestic currency controls. The scale is vast: the UNODC estimates annual laundered funds at 2–5% of global GDP – up to USD 2 trillion [11].

Traditional deterministic compliance algorithms often fail against decentralized structures exploiting fragmented retail accounts and cross-border schemes. Banks must therefore shift toward adaptive risk management – a global, continuous monitoring ecosystem capable of detecting latent connections and responding to evolving criminal patterns across jurisdictions [5].

China's MLNs illustrate this dynamic. Strict currency controls introduced in 2016, following a capital-outflow

© Ganna Panasenko, 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

surge, have only tightened: in 2024, China recorded a record USD 168 billion outflow of foreign direct investment [8]. Current restrictions include an annual USD 50,000 limit on RMB-to-foreign-currency conversion and a ban on transferring RMB abroad without approval from the State Administration of Foreign Exchange.

To meet demand for US dollars, shadow networks partner with transnational criminal organizations and cartels holding large volumes of cash needed for laundering through legitimate banks. FinCEN reports that US institutions flagged USD 312 billion in suspicious transactions tied to Chinese MLNs between 2020 and 2024 [2]. These networks also launder proceeds from unrelated crimes – fraud, human trafficking, marijuana operations, tax evasion – facilitating covert cash exchange; the US State Department estimates USD 154 billion in illicit funds flow through such channels in the PRC annually [10]. This concentration of opaque flows creates critical risk exposure for banks.

Accordingly, this study's relevance stems from the financial sector's urgent need for a scientifically grounded methodology to transform AML/CFT compliance systems.

Analysis of Recent Research and Publications. The effectiveness of FATF mechanisms is called into question in the work of M. Nazzari and P. Reuter [4], who find little evidence that current AML measures meaningfully raise the cost of laundering. Systemic non-compliance by large transnational banks is identified as a key driver of dysfunction – worsened by weak supervision and limited personal liability for executives – while the authors nonetheless affirm compliance's value as an intelligence tool for investigating predicate offenses. The main limitation of this study is the difficulty of quantifying latent laundered volumes.

A different angle is offered by G. V. Raymond's study of transnational "grey capital" in Thailand [7], which draws on the concept of institutional isomorphism to show how structural similarities between informal practices enable largely unimpeded cross-border capital movement, blurring the line between legitimate commerce and criminal networks – though without substantive evidence of direct state-level collusion.

The legitimization of the global AML/CFT regime, as supervisory functions are delegated to private actors such as compliance officers and associations (e.g., ACAMS), is the focus of E. Tsingou's research [9]. She proposes an "outsourcing model" in which compliance professionals generate their own "pragmatic authority" through best practices and networking, though the practical impossibility of quantitatively assessing regime effectiveness remains a key limitation.

Informal value transfer systems such as hawala are examined by J. G. Ercanbrack through British case law [1], showing that such systems are driven by interpersonal trust and Islamic legal norms as much as by profit; a framework is offered for distinguishing legitimate migrant transactions from criminal activity, although reliance on judicial precedent limits generalizability.

Social network analysis of Dutch police data underpins the study by J.-A. Kramer et al. on Money Laundering as a Service (MLaaS) [3], confirming organized structures tied to real estate and underground banking, with "broker" nodes acting as corporate-like intermediaries – though fragmented law-enforcement data prevented full reconstruction of network evolution.

Domestic scholarship links financial-monitoring effectiveness to its integration into overall bank risk management, as shown by M. P. Fedyshyn and O. G. Stuzhuk [14], who cite excessive formalization and weak automation as obstacles. Banking risk drivers and losses are systematized in a phased risk-management model proposed by Ye. Yu. Mordan et al. [13], who note the lack of a unified assessment methodology. Transactional data's role in detecting hidden threats – offshore links, risky-asset concentration – within crisis-scenario stress testing is demonstrated by T. D. Kosova et al. [12], who emphasize flexible informal rules for rapid compliance adaptation.

The emerging contradiction between the globalization of criminal challenges described by foreign researchers and the static nature of national bank internal control systems determines **the objective of this study** – the development of a conceptual model of an adaptive transactional monitoring ecosystem capable of preemptively identifying evolving patterns of cross-border capital laundering.

The methodological framework of the study relies on a comprehensive systemic approach, which enabled the systematization of the operational mechanisms of transnational money laundering networks and the identification of critical vulnerabilities in traditional banking compliance. During the research process, structural-functional analysis methods were applied to theoretically substantiate the architecture of the adaptive transactional monitoring ecosystem, alongside conceptual modeling methods in the development of the multi-layered predictive analytics framework. The theoretical and methodological rationale for integrating machine learning technologies, graph analysis, and explainable artificial intelligence is based on methods of scientific synthesis and logical design.

Results. For the conceptual design of an adaptive bank risk management system, it is necessary first of all to deconstruct the operational mechanisms of shadow money laundering networks and identify the vulnerabilities of the traditional banking infrastructure that they exploit. The key operational features of transnational MLNs, with a specific emphasis on the role of banks in facilitating their existence and the corresponding triggers for internal control (AML/CFT), are presented in Table 1.

The most representative example of the exploitation of the described vulnerabilities is the Chinese Underground Banking System (CUBS), also known as "Fei-Chien" or "Flying Money".

CUBS consists of various individuals and companies from different industries that collaborate through "mirror transfers" to move funds across borders within the framework of informal value transfer systems. Such decentralization makes these flows practically invisible to classic banking monitoring. In turn, CUBS critically depends on global MLNs to obtain large volumes of foreign currency, creating a stable symbiosis of the legal demand for capital and criminal supply.

Figure 1 clearly illustrates this symbiosis and the mechanism of cashless value exchange.

The architecture of this scheme is based on so-called "mirror transactions," in which no physical cross-border movement of funds occurs:

Table 1

Points of contact between MLNs and the traditional banking system

Operational Feature of MLNs	Mechanism of Exploiting Banking Infrastructure	Banking Compliance Vulnerabilities (KYC/AML)	Risk Indicators for Internal Banking Control
Decentralized network structure	Fragmentation of financial flows through a multitude of unconnected retail accounts (P2P transfers) instead of using classic corporate structures.	Traditional banking algorithms are configured to search for hierarchical connections and beneficial owners, causing horizontal networks based on interpersonal trust to remain "invisible".	High frequency of transactions between individuals lacking obvious familial or business ties; utilization of retail accounts for transit.
Cross-border coordination (with other MLNs/illicit networks)	Use of bank correspondent accounts to execute shadow "mirror transfers," bypassing direct cross-border control.	Limited visibility of transactions for an individual bank: the bank sees only the local part of the operation and cannot track the counter-flow in another jurisdiction.	Regular incoming payments from international shadow banking systems or shell companies; discrepancy between the geography of payments and the client's economic profile.
Dual-income model (servicing cartels and investors)	Commingling of "dirty" criminal money (from cartels) with the capital of private investors attempting to bypass currency controls through the host country's banking system.	Difficulty in distinguishing between legitimate capital outflow (e.g., for purchasing real estate) and the integration of drug proceeds, as both operations are disguised as lawful investment activity.	Large transfers to escrow accounts, purchase of elite real estate or luxury goods by individuals without a verified legal Source of Wealth in the bank's country of operation.
Recruitment of "money mules" (including students)	Mass utilization of basic retail and student accounts for the initial placement of cash funds (structuring/smurfing).	Student accounts are traditionally categorized by banks as low-risk during onboarding (account opening), allowing criminals to easily pass the initial filter.	Regular cash deposits in small amounts (below the mandatory reporting threshold); turnover atypical for a student; rapid transit of funds to third-party accounts after deposit.
Exploitation of national passports and forged IDs	Penetration into the legal economy through the mass opening of accounts for non-resident citizens using synthetic identities and falsified documents.	Insufficient effectiveness of biometric verification systems and poor knowledge among front-office bank staff regarding the specifics of foreign identity documents.	Use of serial addresses (mail drops) for registering non-resident accounts; detection of inconsistencies in document metadata during digital onboarding; sudden activity on the accounts of individuals who have left the country.

Source: compiled by the author

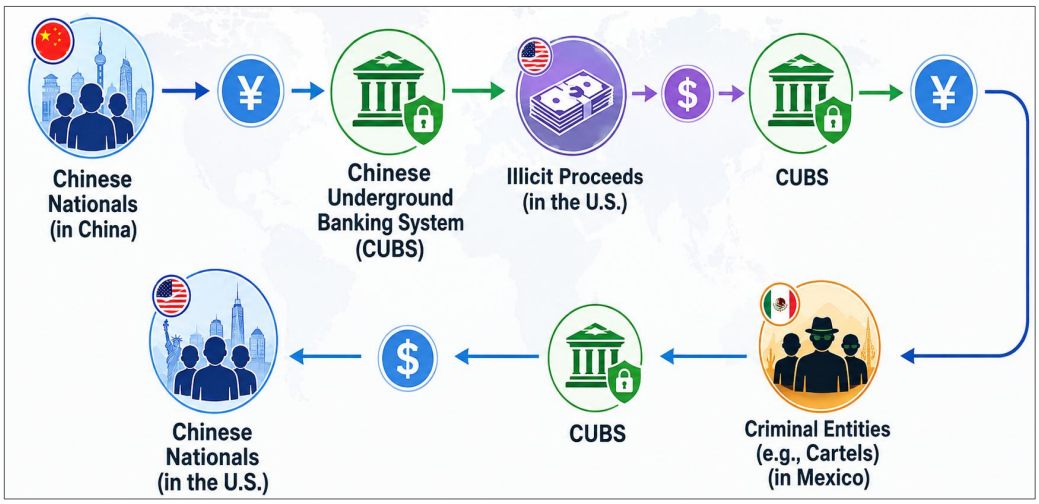

Fig. 1. Scheme of Transnational Laundering of Criminal Proceeds through Informal Banking and Mirror Transactions

Source: compiled by the author

Step 1: PRC citizens residing in China who wish to circumvent currency restrictions transfer yuan to brokers of the Chinese Underground Banking System (CUBS).

Step 2: concurrently, transnational criminal structures, such as cartels in Mexico, generate enormous volumes of illicit proceeds in US dollars from their operations in North America.

Step 3: the CUBS network acts as a connecting link. Brokers receive dollars from cartels in the US and, in exchange, pay the cartels (or their shell companies) the equivalent in yuan within China. Criminals can use these funds to purchase goods or precursors in Asian markets for further shadow operations.

Step 4: the CUBS network transfers the «dirty» dollars obtained from criminals to Chinese citizens (or their trusted proxies) already within US territory. The citizens receive the currency they need, while their yuan remains in China.

The critical vulnerability for the legal banking sector here lies in the fact that both sides of the transaction (the transfer of yuan within China and the placement of dollars

within the US) appear to local banks as independent, domestic operations. Traditional financial monitoring systems fail to see the connection between these flows, which requires risk management to transition toward global, adaptive data analysis models to identify such shadow networks.

To effectively configure adaptive bank monitoring algorithms for the prevention of transnational money laundering, national and international Financial Intelligence Units (FIUs) highlight universal "red flags" that help identify «money mules» and transit structures associated with transnational money laundering networks (MLNs). The integration of these markers into banks' AML/CFT systems requires special attention to the following behavioral anomalies:

– non-resident clients from high-risk jurisdictions who indicate a socially vulnerable status (e.g., "student," "retiree," or "housewife") yet execute transactions with disproportionately large sums;

– critical inconsistencies in identity documents (e.g., discrepancies in the date of issue or date of birth; photographs taken several years apart; signs of utilizing synthetic identities during digital onboarding);

– corporate clients trading in high-end goods and receiving regular cross-border transfers, but simultaneously failing to purchase commensurate inventory (a key marker of Trade-Based Money Laundering – TBML);

– the atypical use of bank checks and escrow accounts for the direct payment of elite real estate or luxury goods without a transparent source of capital origin;

– abnormally frequent transfers between individuals (P2P transactions) or credit card payments that do not align with the expected client profile and lack documented economic justification;

– regular cash deposits by clients in volumes that contradict their declared income or place of employment (which indicates classic initial placement schemes – structuring or smurfing).

In the paradigm of adaptive risk management, relying on isolated static rules to capture these triggers is no longer sufficient. A modern bank must employ predictive analytical models capable of identifying non-obvious combinations of these indicators in real time and continuously learning from new typologies of transnational money laundering.

According to the author, in light of the aforementioned, the concept of a "Comprehensive Coverage Strategy" acquires particular relevance, serving as a fundamental mechanism for the detection and preemptive mitigation of the activities of specific criminal structures, such as MLNs. To implement this concept in practice, a bank requires a global, inclusive continuous monitoring ecosystem that ensures absolute control over every transaction of any client across all geographical jurisdictions of its presence. Such an approach establishes a reliable, resilient, and adaptive protective infrastructure capable of rapidly responding to evolving risk patterns.

Figure 2 presents a visualization of the adaptive management framework of banking institutions for the prevention of transnational money laundering.

The practical implementation of the multi-level monitoring framework presented in Figure 2 begins with an analysis of the transnational threat architecture, where solid red vectors illustrate the critical vulnerabilities of traditional banking compliance. These directed links clearly demonstrate how decentralized criminal networks, exploiting shadow «mirror» transfers and the horizontal fragmentation of financial flows through retail accounts, seamlessly circumvent basic deterministic customer control rules and static transaction threshold limits. In response to these challenges, an intrabank predictive analytics core (highlighted in green on the diagram) is formed, serving as the primary innovative element of the protective infrastructure. Unlike isolated verifications of correspondent accounts, this algorithmic core integrates topological graph analysis to identify latent network connections and multifactor scoring of behavioral anomalies, which allows the credit institution to detect complex routing schemes and the atypical intensity of P2P transactions.

The external catalyst for this core is the macro-level state RegTech platform (represented by the blue block), which plays the role of data enrichment: it supplies the banking algorithms with aggregated macroeconomic triggers, sanction profiles, and textual risk markers, without replacing the autonomous intrabank scoring [6].

The results generated by the predictive core are transmitted to the intelligent control and response module (visualized in yellow), where the application of explainable artificial intelligence (Explainable AI) becomes a critical step in the evolution of financial monitoring. This tool mitigates the limitations of classical neural networks, providing a transparent interpretation of weight coefficients for the well-founded multidimensional clustering and stratification of compliance risks in descending order of their probability. At this stage, the process of selecting incidents for in-depth investigation by specialized analysts is based exclusively on intelligent sampling methods.

The key mechanism ensuring the fundamental adaptability of the entire presented ecosystem consists of the feedback loops, visualized by dashed lines. The red dashed vector reflects the closed-loop process of continuous retraining of machine learning models based on the empirical results of expert investigations, which allows the system to adapt in real time to evolving criminal typologies. In turn, the blue dashed line demonstrates the export of verified data regarding new shadow networks to the regulator level. The final convergence of all processes, symbolized by the thickened solid blue vectors, is aimed at achieving the main objective of the research — the formation of a robust adaptive management system that guarantees a commercial bank the preemptive mitigation of cross-border capital laundering risks while simultaneously optimizing the operational workload.

Conclusions. Based on the conducted research, it has been established that traditional deterministic bank control algorithms have lost their relevance in the face of decentralized transnational money laundering networks that exploit informal channels of mirror transfers and methods of horizontal capital fragmentation.

The primary scientific result of the work is the developed conceptual model of an adaptive transactional risk management system for banks, the architecture of which is based on the synergy of an autonomous intrabank predictive core and a macro-level regulatory technology (RegTech) platform. It is expected that the integration of topological graph analysis, natural language processing, and the multidimensional clustering of anomalies will

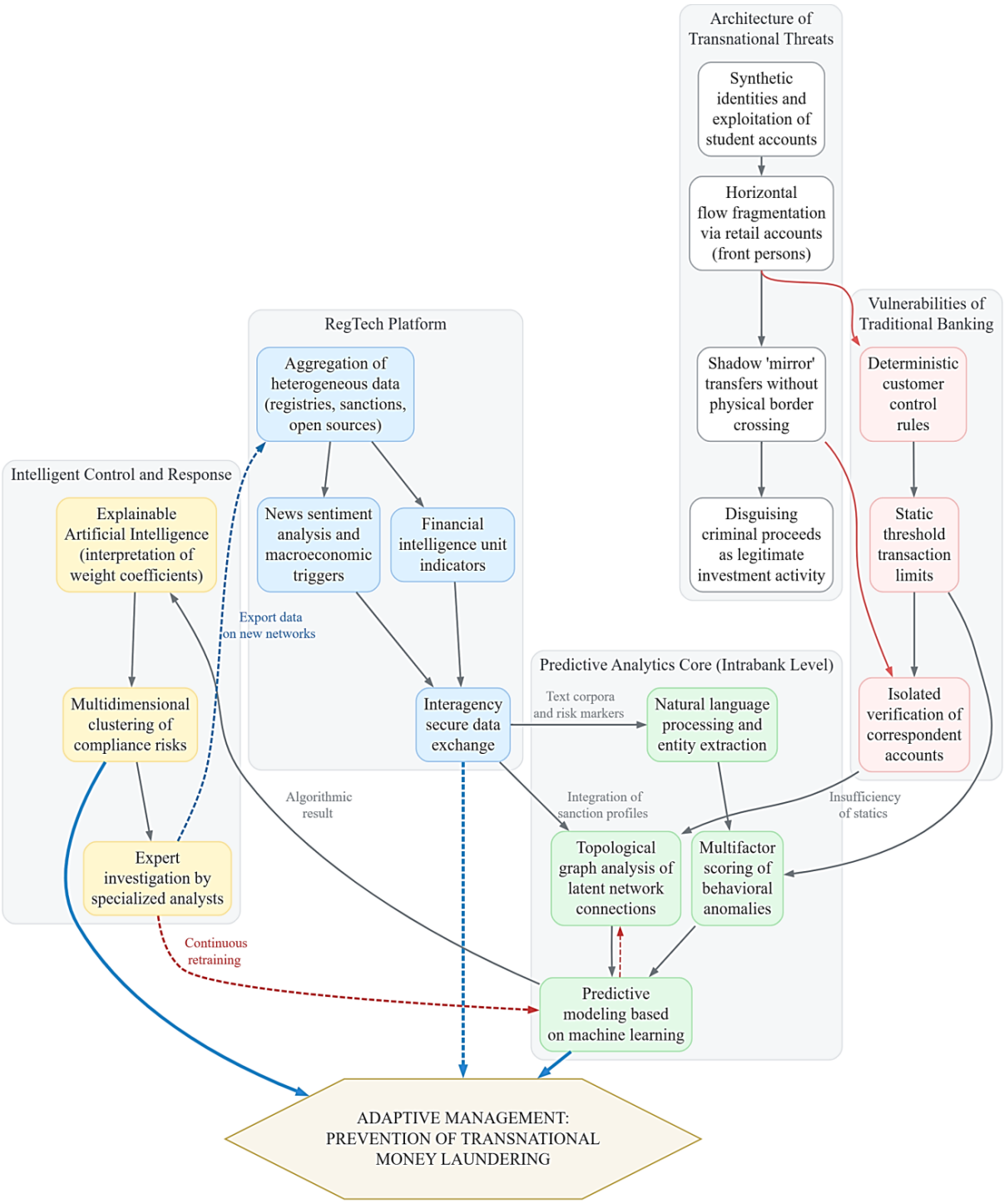

Fig. 2. Conceptual architecture of adaptive transactional risk management in a bank for the prevention of transnational money laundering

Source: compiled by the author

allow banking institutions to preemptively identify complex routing schemes of shadow financial flows even at the stage of their initiation. Furthermore, it appears that a critical factor for the successful implementation of self-learning algorithms within a strictly regulated compliance environment is the mandatory application of explainable artificial intelligence, which guarantees the transparency and auditability of algorithmic decisions.

Thus, the proposed conceptual framework with a continuous feedback loop provides banks with the ability to proactively mitigate the risks of integrating criminal proceeds into the legal economy, radically optimizing the operational workload for specialized analysts and establishing a resilient foundation for the global financial security architecture. The prospects for further scientific research in this direction are associated with the empirical verification of the developed model using large datasets of interbank transactional data, as well as with the in-depth integration of predictive analytics algorithms into the automated stress-testing frameworks of banks.

References:

1. Ercanbrack J. G. (2024) Hawala in criminal court: The role of law and commercial culture in informal financial exchange. *Crime, Law and Social Change*, vol. 82(3), pp. 659–683. DOI: https://doi.org/10.1007/s10611-024-10162-w

2. Financial Crimes Enforcement Network (FinCEN) (2025) *Chinese Money Laundering Networks: 2020–2024 Threat Pattern & Trend Information. Financial Trend Analysis.*

3. Kramer J.-A., Blokland A. A. J., Kleemans E. R., Soudijn M. R. J. (2024) Money laundering as a service: Investigating business-like behavior in money laundering networks in the Netherlands. *Trends in Organized Crime*, vol. 27 (3), pp. 314–341. DOI: https://doi.org/10.1007/s12117-022-09475-w

4. Nazzari M., Reuter P. (2025) How well does the money laundering control system work? *Crime and Justice*, vol. 54 (1), pp. 67–152. DOI: https://doi.org/10.1086/735665

5. Panasenko G., Hurochkina V. (2026) Intelligent Compliance as a Fundamental Tool for Ukraine's Economic Security. In: Semenov A., Yepifanova I., Kajanová J. (eds.) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol. 272. Springer, Cham. DOI: https://doi.org/10.1007/978-3-032-06608-4_1

6. Panasenko G., Hurochkina V., Shtovba S. (2026) Two-Level Model Information System for RegTech-Monitoring the Reporting Entities in Risk-Based Supervision. *Proceedings of the RS-2026: Resilient Systems: Secure Digital Technologies and Critical Infrastructure. CEUR Workshop Proceedings*, vol. 4225. CEUR-WS.org. Available at: https://ceur-ws.org/Vol-4225/

7. Raymond G. V. (2025) Explaining 'Grey Capital': The sociology of transnational Chinese companies and crime in Thailand. *Journal of Contemporary China*, vol. 34 (152), pp. 350–365. DOI: https://doi.org/10.1080/10670564.2024.2302485

8. State Administration of Foreign Exchange of the People's Republic of China (SAFE) (2025) *SAFE Releases China's Balance of Payments for the Fourth Quarter and for the Year 2024*.

9. Tsingou E. (2024) Outsourcing authority in global policy: Legitimating the anti-money laundering regime through professionalization. *Policy and Society*, vol. 43 (1), pp. 70–82. DOI: https://doi.org/10.1093/polsoc/puad031

10. U.S. Department of State (2022) *International Narcotics Control Strategy Report (INCSR), Volume II: Money Laundering. China, People's Republic of China.*

11. United Nations Office on Drugs and Crime (UNODC) (2011) *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*. Vienna: UNODC.

12. Kosova T. D., Mekh H. V., Orlov M. S. (2025) Rol finansovoho monitorynhu u ryzyk-menedzhmenti ta stres-testuvanni bankivskykh ustanov [The role of financial monitoring in risk management and stress-testing of banking institutions]. *Stalyi rozvytok ekonomiky – Sustainable Economic Development*, no. 4 (55), pp. 181–187. DOI: https://doi.org/10.32782/2308-1988/2025-55-25 (in Ukrainian)

13. Mordan Ye. Yu., Bondarenko Ye. K., Kalchenko Ya. I., Davydenko Yu. S. (2021) Bankivski ryzyky lehalizatsii dokhodiv, otrymanykh zlochynnym shliakhom: sutnist, vydy ta systema upravlinnia [Banking risks of money laundering: essence, types and management system]. *Ekonomika ta derzhava – Economy and State*, no. 1, pp. 115–123. DOI: https://doi.org/10.32702/2306-6806.2021.1.115 (in Ukrainian)

14. Fedyshyn M. P., Stuzhuk O. H. (2024) Systema finansovoho monitorynhu v bankakh Ukrainy: strukturna model ta mekhanizmy realizatsii ryzyk-oriientovanoho pidkhodu [Financial monitoring system in Ukrainian banks: structural model and mechanisms for implementing a risk-based approach]. *Naukovyi visnyk Chernivetskoho natsionalnoho universytetu imeni Yuriia Fedkovycha. Seriia Ekonomika – Scientific Bulletin of Yuriy Fedkovych Chernivtsi National University. Economics*, vol. 3–4, pp. 98–105. DOI: https://doi.org/10.32782/ecovis/2024-3-4-15 (in Ukrainian)

Бібліографічний список:

1. Ercanbrack J. G. Hawala in criminal court: The role of law and commercial culture in informal financial exchange. *Crime, Law and Social Change*. 2024. Vol. 82. № 3. P. 659–683. DOI: https://doi.org/10.1007/s10611-024-10162-w

2. Financial Crimes Enforcement Network (FinCEN). *Chinese Money Laundering Networks: 2020–2024 Threat Pattern & Trend Information. Financial Trend Analysis.* 2025.

3. Kramer J.-A., Blokland A. A. J., Kleemans E. R., Soudijn M. R. J. Money laundering as a service: Investigating business-like behavior in money laundering networks in the Netherlands. *Trends in Organized Crime*. 2024. Vol. 27. № 3. P. 314–341. DOI: https://doi.org/10.1007/s12117-022-09475-w

4. Nazzari M., Reuter P. How well does the money laundering control system work? *Crime and Justice*. 2025. Vol. 54. № 1. P. 67–152. DOI: https://doi.org/10.1086/735665

5. Panasenko G., Hurochkina V. Intelligent Compliance as a Fundamental Tool for Ukraine's Economic Security. *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*. Vol. 272 / A. Semenov, I. Yepifanova, J. Kajanová (eds). Springer, Cham, 2026. DOI: https://doi.org/10.1007/978-3-032-06608-4_1

6. Panasenko G., Hurochkina V., Shtovba S. Two-Level Model Information System for RegTech-Monitoring the Reporting Entities in Risk-Based Supervision. *RS-2026: Resilient Systems: Secure Digital Technologies and Critical Infrastructure: CEUR Workshop Proceedings.* Vol. 4225. CEUR-WS.org, 2026. URL: https://ceur-ws.org/Vol-4225/

7. Raymond G. V. Explaining 'Grey Capital': The sociology of transnational Chinese companies and crime in Thailand. *Journal of Contemporary China.* 2025. Vol. 34. № 152. P. 350–365. DOI: https://doi.org/10.1080/10670564.2024.2302485

8. State Administration of Foreign Exchange of the People's Republic of China (SAFE). *SAFE Releases China's Balance of Payments for the Fourth Quarter and for the Year 2024*. 2025.

9. Tsingou E. Outsourcing authority in global policy: Legitimating the anti-money laundering regime through professionalization. *Policy and Society*. 2024. Vol. 43. № 1. P. 70–82. DOI: https://doi.org/10.1093/polsoc/puad031

10. U.S. Department of State. *International Narcotics Control Strategy Report (INCSR), Volume II: Money Laundering. China*, People's Republic of China. 2022.

11. United Nations Office on Drugs and Crime (UNODC). *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*. Vienna : UNODC, 2011.

12. Косова Т. Д., Мех Г. В., Орлов М. С. Роль фінансового моніторингу у ризик-менеджменті та стрес-тестуванні банківських установ. *Сталий розвиток економіки.* 2025. № 4 (55). С. 181–187. DOI: https://doi.org/10.32782/2308-1988/2025-55-25

13. Мордань Є. Ю., Бондаренко Є. К., Кальченко Я. І., Давиденко Ю. С. Банківські ризики легалізації доходів, отриманих злочинним шляхом: сутність, види та система управління. *Економіка та держава.* 2021. № 1. С. 115–123. DOI: https://doi.org/10.32702/2306-6806.2021.1.115

14. Федишин М. П., Стужук О. Г. Система фінансового моніторингу в банках України: структурна модель та механізми реалізації ризик-орієнтованого підходу. *Науковий вісник Чернівецького національного університету імені Юрія Федьковича. Серія Економіка.* 2024. Вип. 3–4. С. 98–105. DOI: https://doi.org/10.32782/ecovis/2024-3-4-15

Дата надходження статті: 12.08.2026
Дата прийняття статті до публікації: 21.09.2026
Дата публікації статті: 30.09.2026