

УДК 336.71:339.72

DOI: <https://doi.org/10.30838/EP.218.113-120>**Panasenko Ganna**

Dr. of Economic Sc.

State Tax University

Панасенко Г.О.

доктор економічних наук

Державний податковий університет

<https://orcid.org/0000-0002-6743-6728>

THE MISUSE OF CORRESPONDENT BANKING AS A CHANNEL FOR SANCTIONED ENTITIES TO ACCESS RESERVE CURRENCIES

The article addresses the misuse of correspondent banking by sanctioned entities utilizing shadow banking networks to access reserve currencies. Traditional discrete AML methods are inadequate against complex beneficiary concealment schemes. The study aims to uncover these exploitation mechanisms and establish a paradigm of algorithmic risk-based supervision (RegTech). The research proves that the core of modern evasion is the uncontrolled exposure of "nested relationships" via transit nodes in free economic zones. To resolve this, two metrics were developed: the Composite Reserve-Currency Clearing Exposure index and the Fee-Escalation index. Integrated into a two-tier RegTech model, they enable continuous near-real-time threat scoring. This allows regulators to transition from retrospective violation recording to proactive risk mitigation, significantly reducing compliance costs and protecting the global market from sanctions arbitrage.

Keywords: correspondent banking, sanctions evasion, shadow banking, AML compliance, RegTech, algorithmic supervision, nested activity, composite risk index.

JEL Classification: G21, G28, F31, F38.

ЗЛОВЖИВАННЯ КОРЕСПОНДЕНТСЬКИМ БАНКІНГОМ ЯК КАНАЛОМ ДОСТУПУ САНКЦІЙНИХ СТРУКТУР ДО РЕЗЕРВНИХ ВАЛЮТ

У статті розглядається проблема зловживання інститутом кореспондентського банкінгу з боку санкційних структур, які використовують мережі тіньового банкінгу для доступу до клірингу в резервних валютах. Актуальність теми зумовлена тим, що на тлі політики де-рискінгу та посилення санкцій, традиційні дискретні методи АМЛ-комплаєнсу не здатні ефективно протидіяти складним схемам приховування бенефіціарів через транзитні вузли. Метою дослідження є виявлення механізмів використання кореспондентських рахунків підсанкційними суб'єктами та формування парадигми алгоритмічного ризик-орієнтованого нагляду (RegTech) для блокування незаконних потоків. Методологічну основу становить комплексний підхід: системно-структурний та мережевий аналіз, аналіз емпіричних прецедентів (кейс-метод), методи математичного моделювання та формалізації, науковий синтез і алгоритмізація. За результатами дослідження доведено, що ядром сучасного обходу санкцій є неконтрольована експозиція «вкладених відносин», коли розрахунки йдуть через обмінні пункти та фіктивні торгові компанії у вільних економічних зонах. Для вирішення проблеми розроблено дві метрики: композитний індекс експозиції клірингу резервної валюти та індекс аномального нарощування комісій. Вони дозволяють агрегувати розрізнені «червоні прапорці» в єдину вимірювану алгоритмічну сигнатуру. Сформовано дворівневу концептуальну модель інтеграції цих метрик у систему RegTech, яка використовує гранулярні дані для безперервного скорингу загроз у режимі, близькому до реального часу. Завдяки цьому банківські установи отримують дієвий інструмент для динамічного мережевого аналізу, що мінімізує інформаційну асиметрію та запобігає транскордонному перетоку тіньового капіталу. Практична цінність роботи полягає в тому, що алгоритмізація контролю на базі розроблених індексів дозволяє регуляторам перейти від ретроспективної фіксації порушень до проактивного управління ризиками. Це кардинально знижує транзакційні витрати банків на звітність, усуває міжсвідомче дублювання та формує міцний фундамент для захисту глобального ринку від санкційного арбітражу.

Ключові слова: кореспондентський банкінг, обхід санкцій, тіньовий банкінг, фінансовий моніторинг, RegTech, алгоритмічний нагляд, вкладені відносини, композитний індекс ризику.

Problem statement. The stability of the international financial system is largely determined by the architecture of cross-border settlements, the core of which is the institution of correspondent banking. Through a network of correspondent accounts, banks lacking a direct presence in the jurisdiction of a reserve currency issuer gain access to the clearing mechanisms of leading currencies. The dominant position of the US dollar preserves the exceptional significance of this channel: according to the International Monetary Fund, in the fourth quarter of 2025, the dollar accounted for 56.77% of global foreign exchange reserves, out of a total volume of \$13.14 trillion [1]. Such high concentration turns access to dollar clearing into a strategic resource, and correspondent relationships into a potential point of vulnerability exploited by actors seeking to bypass restrictive measures.

The relevance of the study is driven by the simultaneous effect of two diverging trends. On the one hand, the global network of correspondent relationships is contracting due to de-risking policies. As noted in the latest analytical review by the Bank for International Settlements (BIS) dedicated to this issue, the decline in the number of active correspondents and corridors continued up until 2022, and compliance risks continue to be articulated by banks as the primary reason for terminating correspondent relationships — primarily with countries having weaker regulatory oversight [2]. The BIS does not publish more recent annual quantitative data; however, the structural problem itself — being an active driver of the industry's de-risking policy rather than a statistical artifact — remains relevant in 2026.

The dynamics of sanctions pressure during this period have been uneven. According to an assessment by the Center for a New American Security, which aggregates the sanctions actions statistics of the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the number of entities added to the Specially Designated Nationals List (SDN List) grew from 2,502 in 2023 to a record 3,135 in 2024, before declining to 1,322 in 2025 amid the change of the U.S. presidential administration [3]. Despite the decrease in the annual rate of new designations, the aggregate volume of active restrictions — including entities added to the list in previous years — continues to create incentives for building circumvention schemes in correspondent banking.

In response to these challenges, international regulators within the framework of the G20 roadmap are developing models of "next-generation correspondent banking" and alternative settlement channels; however, the main burden of cross-border payments during the period under study still falls on the traditional correspondent network, which determines its vulnerability as a key link in the implementation of the sanctions deterrence policy.

The key mechanism of the abuse under consideration is described in the supervisory practice of financial regulators. Sanctioned entities and associated intermediaries — exchange houses, trading, and shell companies — rely on regional banks maintaining correspondent relationships with institutions in the reserve currency jurisdiction to convert foreign currency into dollars and gain access to the international payment system. Meanwhile, the source of the

funds is masked through forged documentation, and the acquired currency is directed toward financing prohibited activities outside the sanctioned jurisdiction. Characteristic features of the scheme include multi-layered transfers through chains of exchange houses and trading companies with the accumulation of fees inconsistent with normal commercial practice, as well as the use of shell companies with opaque ownership structures registered in the free trade zones of third countries [4].

The problem in this case lies in the fact that correspondent banking, being the infrastructural foundation of cross-border settlements, simultaneously acts as the most vulnerable link in the implementation of the sanctions deterrence policy. Existing studies primarily examine either the macroeconomic consequences of de-risking or specific typologies of sanctions evasion, whereas the systemic interrelationship between the contraction of the correspondent network, the escalation of sanctions pressure, and the adaptation of circumvention mechanisms remains insufficiently studied.

Analysis of publications on the research topic. The IMF report [5], as well as the publications by Matvos G. and Neiman B. [6], investigate the impact of economic sanctions on the macroeconomic stability of states and their access to global payment networks, using the example of Iran and other countries. The authors analyze how restrictions disrupt traditional correspondent banking relationships, forcing sanctioned institutions to use longer, indirect, and vulnerable chains of intermediaries to conduct cross-border transactions. Particular attention is paid to the macroeconomic consequences of the partial lifting and reimposition of sanctions, which require governments to implement comprehensive reforms in the financial sector to restore trust on the part of international banks. Furthermore, the trend of reorienting payments toward alternative currencies, such as the Chinese yuan, in response to the de-risking policies of Western financial institutions is examined.

However, the question of the long-term impact of the fragmentation of correspondent relationships on global financial stability and the effectiveness of monetary policy amidst the emergence of independent regional payment systems remains open.

International studies and analytical materials on the use of correspondent banking to circumvent sanctions restrictions and access reserve currencies [7-9] are focused on analyzing complex typologies of evading targeted financial sanctions, including the development of shadow banking networks and the use of shell companies. The reports of leading international agencies detail the mechanisms of terrorism financing and the proliferation of weapons of mass destruction, which involve unlicensed financial intermediaries, exchange houses, and cryptocurrency channels. They also examine specific examples of abuses of access to foreign exchange auctions, where financial institutions use forged documents and bogus companies to transfer funds in the interests of sanctioned groups. Researchers emphasize the importance of interagency coordination and the implementation of enhanced customer due diligence measures to identify hidden beneficial owners

and prevent illicit cross-border transactions.

At the same time, it remains unclear exactly how regulatory authorities should adapt their technological tools for the preventive and automated detection of multi-layered beneficiary concealment schemes involving the use of anonymous cryptocurrencies and decentralized platforms.

In the FATF «Guidance on proliferation financing risk assessment and mitigation» [10], global standards and methodologies for assessing the risks of financing the proliferation of weapons of mass destruction for the public and private sectors are examined. The document details approaches to identifying, monitoring, and mitigating risks arising from the potential breach or evasion of targeted financial sanctions mandated by United Nations Security Council Resolutions. The main emphasis is placed on the need to integrate proliferation financing risk assessment into the existing compliance and transaction monitoring programs of financial institutions and other reporting entities. The Guidance asserts that an effective countermeasure system requires not only asset freezing but also a deep analysis of vulnerabilities in critical sectors such as trade finance and correspondent banking.

Despite the conceptual significance of these recommendations, the question of exactly how to translate the descriptive FATF standards into measurable algorithmic metrics remains unresolved. In particular, there is a lack of a formalized framework allowing correspondent banks to aggregate disparate risk indicators for a systemic assessment of the uncontrolled exposure of "nested relationships" and the preventive blocking of sanctioned entities' access to clearing in reserve currencies.

The aim of the article is to identify the mechanisms of abuse in correspondent banking that provide sanctioned entities with access to reserve currencies, as well as to develop a methodology for algorithmic risk-based supervision (RegTech) to formalize and preventively detect hidden illicit flows.

Research Methods. The methodological basis of the research is based on a comprehensive approach. Systemic-structural and network analysis methods were applied to deconstruct shadow financial networks and investigate typologies of sanctions evasion. The study of beneficiary concealment mechanisms relied on the analysis of empirical precedents (case study method) drawn from current supervisory practice. The transformation of qualitative compliance risk indicators into computable variables was implemented using methods of mathematical modeling and formalization. The aggregation of disparate transactional anomalies into unified metrics was carried out through scientific synthesis and algorithmization, which enabled the formulation of a conceptual architecture for risk-based supervision (RegTech).

The Main Results of Research. The global contraction of correspondent banking networks and the unprecedented intensification of sanctions pressure have led to a qualitative transformation in the methods of integrating shadow sector capital into the international financial system. Financial institutions and state entities under blocking sanctions are increasingly resorting to the distributed architecture of "shadow banking" to maintain unauthorized access to

clearing mechanisms in reserve currencies, primarily the US dollar.

As noted in recent FATF studies, standard AML compliance systems based on static rules prove insufficiently effective against complex schemes for financing the proliferation of weapons of mass destruction and direct sanctions evasion [11]. In response to restrictions, transactional activity is artificially shifted to less transparent jurisdictions and purposefully diluted through chains of nominal intermediaries, while the policy of a total refusal to serve entire categories of clients often only exacerbates the problem, pushing capital into the unregulated segment.

AML supervisory practice clearly demonstrates that the structural core of the modern sanctions evasion architecture is the coordinated activity of regional clearing centers, exchange houses, and trading companies massively incorporated in key financial hubs such as Hong Kong and the free economic zones of the United Arab Emirates [12]. These entities purposefully exploit the active correspondent accounts of legal regional banks to convert local currencies into US dollars under the guise of ordinary foreign trade operations. The key specific feature of this scheme lies in the fact that settlements are carried out exclusively outside the sanctioned jurisdiction: transit shell companies are used both to accumulate export revenues and for the subsequent payment of foreign supplies. This allows the scheme participants to completely avoid the repatriation of funds and hide the ultimate beneficial owner from the compliance control systems of Western correspondent banks.

An empirical illustration of such multi-layered masking is the large-scale activity of the network controlled by Iranian financial operators — the Zarringhalam brothers. According to FinCEN materials, this entity used licensed exchange houses for the covert operational management of an extensive network of shell companies in the UAE and Hong Kong. These fictitious organizations massively opened multi-currency accounts in various financial institutions across the region, de facto acting as a single interface for conducting transactions in the interests of blocked entities (including military ones) for the sale of hydrocarbons and petrochemical products [2].

Such a pattern clearly crystallizes the problem of uncontrolled exposure to "nested relationships," in which a respondent bank's correspondent account is effectively used to clear high-risk transactions of third parties through the screen of nominal commercial counterparties.

The logical continuation of this scheme is the reinvestment of laundered export revenues into the procurement of dual-use technologies and weapons on international markets. An illustrative precedent is the activity of the company Sahara Thunder, which functioned as a key front agent for Iran's Ministry of Defense and Armed Forces Logistics (MODAFL). Utilizing state quotas for the sale of crude oil, the company relied on the so-called "shadow fleet" and methods of masking the origin of the cargo (forging bills of lading, ship-to-ship transfers on the high seas) to accumulate revenues in the accounts of international front entities. Subsequently, multi-layered payments were initiated through these same shadow banking nodes to procure critical electronic components and communication

systems necessary for the production of unmanned aerial vehicles.

A conceptual diagram of the described shadow banking

architecture, clearly demonstrating the isolation of sanctioned beneficiaries from compliance control systems, is presented in Figure 1.

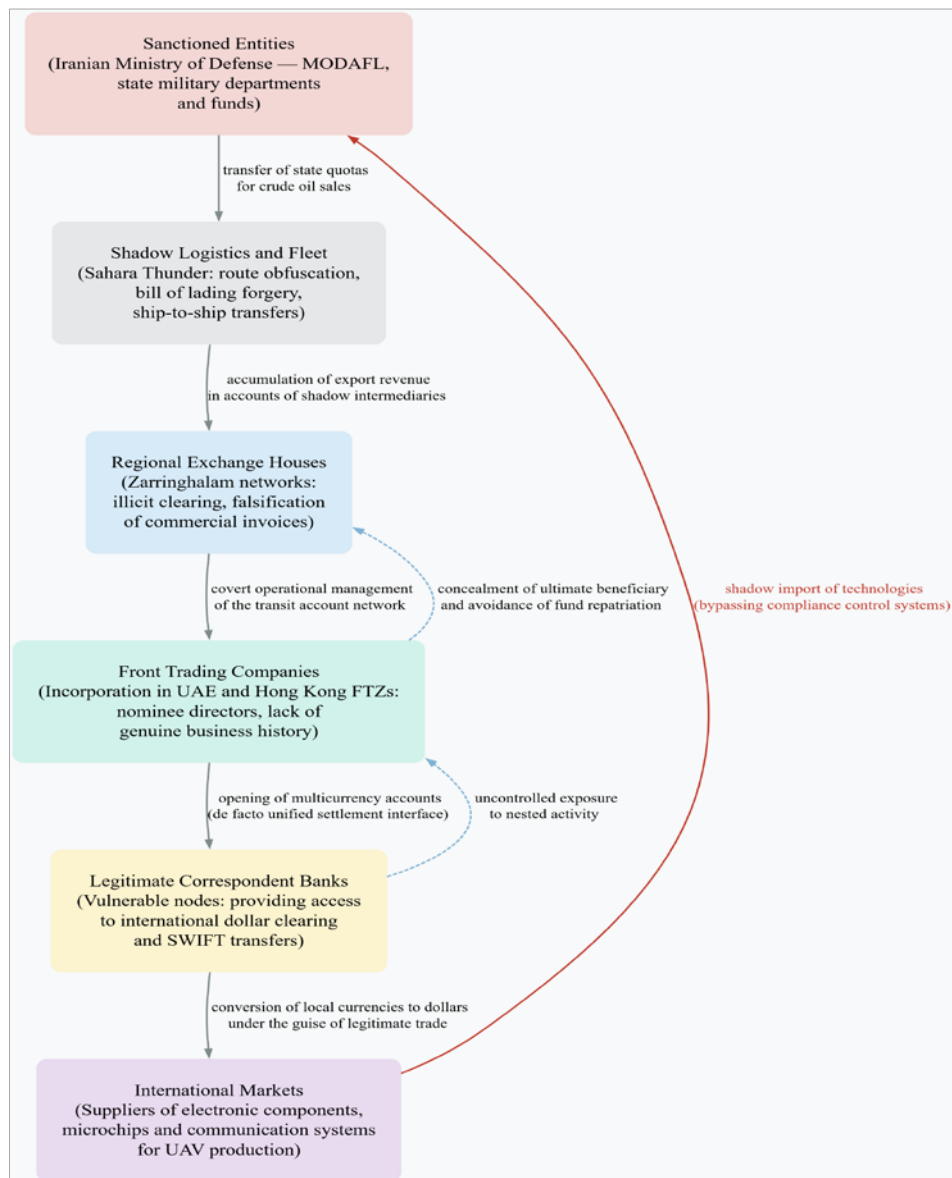


Fig. 1. Integration of sanctioned entities into the international settlement system using correspondent banks

Source: compiled by the author

At the operational level, the implementation of the described shadow banking architecture generates specific transactional anomalies, which in the supervisory practice of relevant regulators are classified as risk indicators, or «red flags».

According to supervisory practice materials, the first critical indicator is the specific nature of the incorporation and life cycle of transit nodes. Sanctions networks purposefully use companies recently registered in the free economic zones of the UAE, Hong Kong, and other financial hubs, which are characterized by opaque ownership structures, the use of nominee directors, and a complete lack of a verified commercial history. For traditional compliance, such counterparties often appear as ordinary startups or trade intermediaries, allowing them to successfully pass

initial screening at regional banks.

The second marker, directly indicating the exploitation of nested relationships, is the anomalous routing of payments with an atypical accumulation of transaction costs. In legal international trade, the settlement chain is optimized to reduce the commission burden. In sanctions schemes, however, funds are intentionally passed through a cascade of unaffiliated trading companies and regional exchange houses. Each link adds its own commission, leading to an economically unjustified increase in the cost of the payment, the sole purpose of which is to maximize the obfuscation of the financial trail and distance the source of funds from the correspondent bank.

The third fundamental red flag is related to the masking of ultimate beneficial owners through the falsification of

the commercial activity profile. Supervisory authorities record systematic discrepancies between a company's declared specialization and the nature of its actual settlements: for example, when a legal entity declaring income from trading agricultural products or hydrocarbons makes multimillion-dollar transfers to manufacturers of electronic components and microchips. The situation is exacerbated by the massive use of forged supporting documents (including bills of lading with altered ports of destination), which makes documentary control on the part of the correspondent bank practically ineffective.

However, as the analysis of typologies from Financial Intelligence Units around the world shows, the main vulnerability of legal correspondent banks lies in the fact that they see these indicators not systemically, but in a fragmented manner — at the level of individual, artificially isolated payments. As a result, the fundamental problem of the current AML monitoring paradigm lies in the discrete approach to assessing these indicators. In the context of mass transactional flows, this leads either to overlooking complex multi-layered schemes or to the generation of a critical volume of false positives. The mere detection of an "immature company in an SEZ" or an "opaque beneficiary" is no

longer capable of ensuring the preventive halt of illicit clearing.

Thus, current international AML standards set out lists of disparate risk indicators but do not offer a formalized model for their aggregation that is specific to reserve currency clearing. The methodology proposed in this article fills this gap by translating the descriptive indicators of supervisory practice into measurable values through the introduction of two calculation tools — the composite index of reserve currency clearing exposure and the index of anomalous commission accumulation in the payment chain. The weights, thresholds, and normalizations presented below are illustrative in nature and are subject to empirical calibration using the data of a specific institution; the methodology describes the calculation structure rather than asserting specific empirical values.

Composite index of reserve currency clearing exposure (R)

For the relationship with respondent bank i , a composite index of reserve currency clearing exposure is proposed, aggregating normalized risk factors into a single metric:

$$R_i = \sum_{k=1}^n w_k x_{k,i} \quad \sum_{k=1}^n w_k = 1 \quad x_{k,i} \in [0,1]$$

where:

$x_{k,i}$ is the value of the k -th risk factor for respondent i normalized to the $[0,1]$ interval;

w_k is the weight coefficient of this factor.

The application of the normalization procedure ensures the comparability of heterogeneous features, while constraining the sum of the weight coefficients to one guarantees that the final value of the index lies within the strict

boundaries of the $[0,1]$ interval. The specification of the base components of the composite index, their operationalization, and the distribution of weights are presented in Table 1.

Table 1

Factors of the composite index R (illustrative specification)

Factor	Operationalization (normalization to $[0,1]$)	Weight (w)
Immaturity of counterparties in free economic zones	Share of the respondent's counterparties incorporated less than 12 months ago in free trade zones	0.2
Concentration in contracting corridors	Share of payments through correspondent corridors with a decline in connections above the median	0.15
Repetition of amounts	Share of transactions with near-identical amounts (coefficient of variation below the threshold)	0.15
Beneficiary opacity	Share of recipients without a disclosed ultimate beneficial owner or with matching attributes	0.25
Exposure to nested relationships	Share of turnover servicing the respondent's own clients (nested activity)	0.15
Flow dollarization	Share of clearing in the reserve currency in the total turnover of relationships	0.1

Source: compiled by the author

The final value of the R index serves as a criterion for classifying the risk level and is compared with threshold

intervals determining the applicable compliance control regime:

$$Regime(i) = \begin{cases} \text{standart monitoring,} & R_i < 0,33 \\ \text{enhanced due diligence} & 0,33 \leq R_i < 0,66 \\ \text{escalation and reporting trigger,} & R_i \geq 0,66 \end{cases}$$

In the presented specification, the threshold values of 0.33 and 0.66 evenly segment the range of permissible values into three intervals. In practice, their final calibration

should be carried out based on the financial institution's retrospective data in order to optimize the balance between the completeness of risk profile detection and the

minimization of the share of false positives.

Index of anomalous commission accumulation in the payment chain (F)

For a payment chain P passing through a sequence of

intermediaries from node 1 to node m , an index of anomalous commission accumulation (F) is proposed, formalizing the qualitative feature of disproportionate costs into a measurable quantity:

$$F_p = \frac{1}{m-1} \sum_{j=1}^{m-1} \frac{f_{j+1} - f_j}{f_j} \cdot \mathbb{I} \left[\frac{f_{j+1} - f_j}{f_j} > \tau \right]$$

where:

f_j is the total commission burden at link j of the chain,

m is the number of nodes,

τ is the threshold of the economically justified relative commission increment,

indicator function $\mathbb{I}$ nullifies the contribution of links where the increment does not exceed the threshold.

The index reflects the average above-threshold relative accumulation of costs along the entire chain. A chain is

marked as potentially artificially extended upon the simultaneous fulfillment of two conditions:

$$F_p > \theta \wedge m > m_c^*$$

where:

θ is the threshold value of the index,

m_c^* is the standard chain length for corridor c given an unchanged economic function of intermediate counterparties.

The joint condition allows separating economically rational multi-link settlements from chains whose sole purpose is the obfuscation of the payment trail and the concealment of the ultimate beneficial owner. The values θ and m_c^* are also subject to calibration.

Summarizing the above, it should be noted that the two proposed indices form a two-level control scheme — the R index assesses the risk at the level of the relationship with the respondent and determines the due diligence regime, while the F index operates at the level of individual payment chains and serves as a trigger for transaction monitoring.

The scientific novelty of the methodology consists of three provisions.

First, the disparate red flags of supervisory practice are aggregated into a single normalized metric specific precisely to the risk of access to reserve currency clearing.

Second, the qualitative feature of disproportionate commission accumulation is formalized into a reproducible computable signature, reducing the dependence of detection on expert judgment.

Third, the control of nested relationships is reoriented from abstract opacity to the specific risk of the dollarization of sanctioned flows.

Thus, the methodology does not merely reproduce the content of international AML standards but offers a formal framework for their operationalization, suitable for subsequent empirical verification.

The practical applicability of the developed mathematical models — the composite index of reserve currency clearing exposure and the index of anomalous commission accumulation — is maximized upon their systemic integration into the architecture of algorithmic supervision and national RegTech platforms.

In modern economic realities, the traditional financial monitoring model, which relies on periodic, aggregated, and template-based reporting, demonstrates a critical lag behind the speed at which new money laundering

typologies are generated. The fundamental problem of current practice lies in the fragmentation of information flows, significant time lags in data acquisition, and the weak integration of structured registries with unstructured market signals. As a result, supervisory authorities and financial institutions themselves are forced to operate under conditions of severe information asymmetry, which allows sanctions networks to successfully exploit the vulnerabilities of correspondent banking.

To overcome these institutional limitations, the implementation of composite indices within a two-level conceptual model of an information-analytical system (RegTech) focused on risk-based supervision is proposed [13].

The first level of this model conceptualizes the abandonment of the "reporting as an end product" paradigm in favor of transitioning to granular data and information-sharing models. In the context of international settlements, the catalyst for such a transition is the global migration of payment systems to the ISO 20022 standard. The machine-readable fields of this standard provide precisely the data granularity — accurate identification of beneficiaries, transparency of commission deductions at each stage, and detailed payment purpose — that serves as the empirical basis for the automatic calculation of the R and F indices without involving manual audits.

The second level of the model reflects the mechanism for integrating information flows in near real-time, utilizing advanced analytics tools, network analysis, and multi-factor risk scoring. It is at this stage that the mathematical metrics R and F are integrated into a single analytical perimeter of financial monitoring. The R index performs the function of strategic profiling: the system automatically enriches the respondent bank's profile with granular data from state registries, international sanctions lists, corporate ownership databases, and arrays of market information. In turn, the F index functions as a dynamic network analysis tool, identifying transactional anomalies and atypical counterparty behavior within long payment chains.

From an AML perspective, integrating these algorithmic metrics into the RegTech ecosystem allows for the transformation of disparate discrete signals into a comprehensive early warning system that continuously correlates regulatory reporting with databases on ultimate beneficial owners and external unstructured sources, forming a dynamic heat map of vulnerabilities. When threshold values are exceeded (for example, when the *R* index reaches the escalation zone), the system automatically generates a risk score and routes the signal to the appropriate financial intelligence units for the adoption of preventive measures.

The macroeconomic and institutional effect of implementing such a two-level algorithmic supervision platform is expressed in a qualitative change in the compliance architecture.

First, banks' transaction costs for search, verification, and reporting preparation are drastically reduced.

Second, interagency duplication of requests is eliminated through the formation of a unified information space.

Third, the reaction time of supervisory authorities to the emergence of new transnational capital concealment schemes is significantly reduced.

Thus, the algorithmization of control through the calculation of composite indices forms a reliable foundation for predictive analytics, allowing regulators to transition from the retrospective recording of violations to the proactive prevention of cross-sectoral contagion and the protection of the global market from sanctions arbitrage and the shadow clearing of reserve currencies.

Conclusions. As a result of the conducted study, a relevant scientific and methodological problem related to countering shadow schemes of financial sanctions evasion within the correspondent banking system has been

resolved. Based on a systemic analysis of transactional anomalies, it has been established that the structural core of modern sanctions arbitrage is the uncontrolled exposure of «nested relationships», implemented via fictitious transit nodes in free economic zones. To overcome the limitations of discrete compliance control, a novel methodological framework has been developed, formalizing qualitative risk indicators into measurable mathematical values. Within this framework, a composite reserve-currency clearing exposure index and a fee-escalation index have been constructed, which collectively form a reproducible algorithmic signature for detecting hidden beneficiaries and artificially convoluted payment chains.

As a foundation for the application of this mathematical apparatus, a conceptual two-tier model of risk-based algorithmic supervision (RegTech) has been formulated. It has been theoretically substantiated that integrating the proposed calculation metrics into a unified analytical perimeter, utilizing the granular data of the ISO 20022 standard, eliminates information asymmetry in correspondent networks. Consequently, the study lays the conceptual groundwork for a qualitative transformation of the financial monitoring architecture, enabling regulators to transition from retrospective violation recording to preventive dynamic threat scoring.

Declaration on the use of artificial intelligence tools.

In preparing this article, artificial intelligence tools (in particular, Gemini 2026) were used to format the reference list in accordance with APA style. No part of the author's text containing scientific novelty, research findings or conclusions was generated using artificial intelligence. The author bears full responsibility for the scientific validity, accuracy of the data and integrity of the article's content.

References:

1. Bank for International Settlements. (2023). CPMI correspondent banking chartpack. https://www.bis.org/cpmi/paysysinfo/corr_bank_data/chartpack_2305.pdf
2. Financial Crimes Enforcement Network. (2025, June 6). FinCEN advisory FIN-2025-A002: FinCEN advisory on the Iranian regime's illicit oil smuggling activities, shadow banking networks, and weapons procurement efforts. U.S. Department of the Treasury. <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2025-a002>
3. Hume, E., & Rutter, K. (2026, January 29). Sanctions by the numbers: 2025 year in review. Center for a New American Security. <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-2025-year-in-review>
4. International Monetary Fund. (2026, March 27). IMF data brief: Currency composition of official foreign exchange reserves. <https://data.imf.org/en/news/imf%20data%20brief%20march%2027>
5. International Monetary Fund. (2017). Islamic Republic of Iran: Selected issues (IMF Country Report). International Monetary Fund. <https://doi.org/10.5089/9781475583083.002>
6. Matvos, G., & Neiman, B. (2026, March 27). Financial sanctions and the global payments network. SSRN. <https://doi.org/10.2139/ssrn.6501663>
7. Australian Sanctions Office, & Australian Transaction Reports and Analysis Centre (AUSTRAC). (2025). Identifying sanctions risks in Iran's shadow banking network (Advisory Note). Australian Government. <https://www.dfat.gov.au/international-relations/security/sanctions/guidance/identifying-sanctions-risks-irans-shadow-banking-network>
8. Financial Action Task Force. (2025). Complex proliferation financing and sanctions evasion schemes. FATF. <https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html>
9. Financial Crimes Enforcement Network. (2024). Imposition of special measure regarding Al-Huda Bank as a financial institution of primary money laundering concern. Federal Register, 89(128), 55051–55059. <https://www.fincen.gov/resources/statutes-regulations/federal-register-notices/imposition-special-measure-regarding-al>
10. Financial Action Task Force. (2021). Guidance on proliferation financing risk assessment and mitigation. FATF. <https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment>

mitigation.html

11. FATF. (2025, June 20). Complex proliferation financing and sanctions evasion schemes. <https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html>
12. U.S. Department of the Treasury. (2025, September 19). Treasury sanctions Iranian network laundering billions for regime through shadow banking scheme. <https://home.treasury.gov/news/press-releases/sb0159>
13. Panasenکو, G., Hurochkina, V., & Shtovba, S. (2026). Two-level model information system for RegTech-monitoring the reporting entities in risk-based supervision. In Proceedings of the RS-2026: Resilient Systems: Secure Digital Technologies and Critical Infrastructure (Vol. 4225). CEUR-WS. <https://ceur-ws.org/Vol-4225/>

Список використаних джерел:

1. Bank for International Settlements. CPMI correspondent banking chartpack. 2023. URL: https://www.bis.org/cpmi/paysysinfo/corr_bank_data/chartpack_2305.pdf (дата звернення: 11.06.2026).
2. Financial Crimes Enforcement Network. FinCEN Advisory FIN-2025-A002: FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts. U.S. Department of the Treasury. 2025. URL: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2025-a002> (дата звернення: 07.07.2026).
3. Hume E., Rutter K. Sanctions by the numbers: 2025 year in review. Center for a New American Security. 2026. URL: <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-2025-year-in-review> (дата звернення: 18.06.2026).
4. International Monetary Fund. IMF Data Brief: Currency Composition of Official Foreign Exchange Reserves. 2026. URL: <https://data.imf.org/en/news/imf%20data%20brief%20march%2027> (дата звернення: 10.05.2026).
5. International Monetary Fund. Islamic Republic of Iran: Selected Issues. IMF Country Report. International Monetary Fund. 2017. DOI: <https://doi.org/10.5089/9781475583083.002>
6. Matvos G., Neiman B. Financial sanctions and the global payments network. SSRN. 2026. DOI: <https://doi.org/10.2139/ssrn.6501663>
7. Australian Sanctions Office, Australian Transaction Reports and Analysis Centre (AUSTRAC). Identifying sanctions risks in Iran's shadow banking network. Advisory Note. Australian Government. 2025. URL: <https://www.dfat.gov.au/international-relations/security/sanctions/guidance/identifying-sanctions-risks-irans-shadow-banking-network> (дата звернення: 18.06.2026).
8. Financial Action Task Force. Complex proliferation financing and sanctions evasion schemes. FATF. 2025. URL: <https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html> (дата звернення: 23.06.2026).
9. Financial Crimes Enforcement Network. Imposition of special measure regarding Al-Huda Bank as a financial institution of primary money laundering concern. Federal Register. 2024. Vol. 89, No. 128. Pp. 55051–55059. URL: <https://www.fincen.gov/resources/statutes-regulations/federal-register-notice/imposition-special-measure-regarding-al> (дата звернення: 11.06.2026).
10. Financial Action Task Force. Guidance on proliferation financing risk assessment and mitigation. FATF. 2021. URL: <https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html> (дата звернення: 07.06.2026).
11. Financial Action Task Force. Complex proliferation financing and sanctions evasion schemes. FATF. 2025. URL: <https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html> (дата звернення: 03.07.2026).
12. U.S. Department of the Treasury. Treasury sanctions Iranian network laundering billions for regime through shadow banking scheme. 2025. URL: <https://home.treasury.gov/news/press-releases/sb0159> (дата звернення: 18.06.2026).
13. Panasenکو G., Hurochkina V., Shtovba S. 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-WS. 2026. Vol. 4225. URL: <https://ceur-ws.org/Vol-4225/> (дата звернення: 12.06.2026).

Дата надходження статті: 01.09.2026 р.

Дата прийняття статті до друку: 14.10.2026 р.

Дата публікації (оприлюднення) статті: 26.10.2026 р.

Стаття поширюється на умовах ліцензії Creative Commons Attribution License International CC-BY.