УДК 336.76:004.8:35

https://doi.org/10.52058/3041-1254-2025-12(22)-981-989

Кондратенко Наталія Олегівна доктор економічних наук, професор, професор кафедри менеджменту і публічного адміністрування, Харківський національний університет міського господарства імені О. М. Бекетова, https://orcid.org/0000-0003-3305-9570

Коляда Тетяна Анатоліївна кандидат юридичних наук, доцент, доцент закладу вищої освіти кафедри менеджменту, маркетингу та забезпечення якості у фармації, Національний фармацевтичний університет, https://orcid.org/0000-0002-6929-8939

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ФІНАНСОВИХ ДАНИХ ЯК ЕЛЕМЕНТ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ЗЛОЧИННИХ ДОХОДІВ

Анотація. У статті досліджується роль кібербезпеки та захисту фінансових даних як невід'ємного елементу державної політики у сфері протидії легалізації доходів, отриманих злочинним шляхом.

Проаналізовано сучасні загрози, пов'язані з цифровізацією фінансового сектору, зокрема використання криптовалют, онлайн-платформ та високотехнологічних схем відмивання коштів.

Висвітлено міжнародний досвід інтеграції кіберзахисту у систему фінансового моніторингу, зокрема застосування ризик-орієнтованого підходу, автоматизованих аналітичних систем, технологій штучного інтелекту та Big Data для виявлення підозрілих транзакцій.

Розглянуто організаційні, правові та нормативні механізми забезпечення безпеки фінансових даних у різних країнах, включно з Європейським Союзом, Канадою та Ізраїлем, що дозволяє визначити кращі практики щодо стандартизації процедур, обміну інформацією та захисту персональних даних.

Особливу увагу приділено аналізу публічно-приватної співпраці, що сприяє ефективному контролю за фінансовими потоками та запобіганню фінансовим злочинам.

У статті також обґрунтовано необхідність удосконалення національної системи фінансового моніторингу в Україні шляхом впровадження сучасних аналітичних інструментів, посилення нормативно-правового регулювання кібербезпеки та використання міжнародного досвіду для підвищення ефективності протидії легалізації злочинних доходів.

Результати дослідження можуть бути використані для формування стратегії державного управління фінансовою безпекою, оптимізації процесів моніторингу

фінансових операцій та розробки комплексних підходів до захисту інформаційної інфраструктури фінансових установ.

Ключові слова: публічне управління, механізми публічного управління, протидія легалізації (відмивання) доходів, фінансовий моніторинг, державна політика, протидія відмиванню коштів отриманих злочинним шляхом, фінансова безпека.

Kondratenko Nataliia Olegivna Doctor of Economics, Professor, Professor of the Department of Management and Public Administration, O. M. Beketov National University of Urban Economy in Kharkiv, https://orcid.org/0000-0003-3305-9570

Koliada Tetiana Anatoliivna PhD, Associate Professor, Associate Professor at the institution of higher education, Department of Management, Marketing, and Quality Assurance in Pharmacy, National University of Pharmacy, https://orcid.org/0000-0002-6929-8939

CYBERSECURITY AND FINANCIAL DATA PROTECTION AS AN ELEMENT OF STATE POLICY TO COUNTERACT MONEY LAUNDERING

Abstract. This article examines the role of cybersecurity and financial data protection as an essential component of state policy aimed at counteracting the laundering of proceeds derived from criminal activities. The study highlights the accelerating digitalization of the financial sector, which has fundamentally transformed both legitimate financial transactions and criminal schemes that exploit technological innovations. Particular attention is paid to emerging threats associated with the use of cryptocurrencies, online payment platforms, decentralized finance instruments, and sophisticated cyberattacks targeting financial institutions. These developments significantly complicate the identification of illicit financial flows and require states to adopt new regulatory, technological, and organizational approaches.

The article presents an overview of international experience in integrating cybersecurity mechanisms into financial monitoring systems, focusing on countries that have successfully implemented risk-based approaches, automated systems for detecting suspicious transactions, advanced analytics, artificial intelligence, and large-scale data processing technologies. It also analyzes normative and institutional frameworks that regulate data protection, establish cybersecurity standards for financial organizations, and introduce accountability measures for violations. The examples of the European Union, Canada, Singapore, and Israel demonstrate the effectiveness of coordinated models of public sector management, cross-border information exchange, and partnerships between government bodies and private financial institutions.

In addition, the article emphasizes the importance of developing secure digital infrastructures, enhancing staff competence in cybersecurity, and creating unified national platforms for monitoring and analyzing financial operations. The study substantiates the need to strengthen Ukraine's national financial monitoring system through the implementation of advanced technological instruments, harmonization with global standards, and expansion of cooperation with international organizations. The research findings can serve as a basis for improving state financial security strategies, optimizing monitoring processes, and developing integrated approaches to protecting the information environment of financial systems.

Keywords: public administration, public administration mechanisms, anti-money laundering, financial monitoring, state policy, combating money laundering of proceeds of crime, financial security.

Постановка проблеми. Стрімка цифровізація фінансового сектору, розширення електронних платіжних систем, онлайн-банкінгу та фінтех-сервісів істотно підвищили ефективність економічних процесів, водночас створивши нові можливості для легалізації доходів, отриманих злочинним шляхом. Кіберзлочинці активно використовують вразливості інформаційних систем, викрадення та підміну фінансових даних, фішингові атаки, несанкціоноване втручання у роботу реєстрів і фінансових платформ для маскування незаконного походження коштів. Це актуалізує потребу в інтеграції сучасних механізмів кібербезпеки у систему державної політики протидії відмиванню злочинних доходів.

Незважаючи на наявність нормативно-правової бази у сфері кіберзахисту та фінансового моніторингу, на практиці простежуються проблеми фрагментарності цих механізмів, обмежена координація між державними органами, фінансовими установами та правоохоронними структурами, а також недостатній рівень технічної оснащеності суб'єктів первинного фінансового моніторингу. Крім того, розвиток технологій штучного інтелекту, блокчейну та криптоактивів створює нові ризики для системи AML (Anti-Money Laundering), які потребують переосмислення підходів до державної політики у сфері захисту фінансових даних.

За цих умов виникає необхідність комплексного дослідження ролі кібербезпеки та механізмів захисту фінансової інформації як ключових інструментів державної політики протидії легалізації злочинних доходів, визначення їхньої ефективності та перспектив подальшого удосконалення.

Аналіз останніх досліджень і публікацій. У сучасній науковій і практичній літературі все більше уваги приділяється взаємозв'язку між фінансовим моніторингом та кібербезпекою, зокрема захисту даних як ключового ресурсу для державної політики протидії легалізації доходів. Наприклад, нещодавнє дослідження PwC за результатами опитування в регіоні Центральної та Східної

Європи (CEE AML Survey 2024) виявило, що значна кількість фінансових установ розглядають впровадження нових технологій як пріоритет для підсилення AML-функцій. У доповіді зазначено, що організації інвестують у цифрові інструменти, які допомагають знизити ризики, пов'язані з фінансовими злочинами, а також підвищити управління відповідністю (compliance) [1].

Окремо актуальними є дослідження Державної служби фінансового моніторингу України, яка здійснює переклад і впровадження міжнародного методологічного досвіду у сфері AML/CFT. Зокрема, Держфінмоніторинг активно популяризує типологічні звіти FATF про віртуальні активи, стандарти бенефіціарної власності й оцінки ризиків, що прямо пов'язано з кіберризиками фінансових транзакцій [2].

Також зростає інтерес до застосування аналітичних технологій: у методологічних щотижневих дайджестах ПВК/ФТ Держфінмоніторингу відображаються тренди, пов'язані із впровадженням автоматизованих рішень на базі ШІ та машинного навчання для аналізу великих обсягів даних, що дозволяє підвищити ефективність виявлення підозрілих транзакцій [3].

З точки зору технологічного захисту, експерти Microsoft у своїх матеріалах звертають увагу на інтеграцію кібербезпеки з фінансовим комплаєнсом: їхні рішення для фінансових установ поєднують захист від шахрайства, AML-процедури та управління фінансовими даними, що свідчить про необхідність побудови політики, яка одночасно враховує кіберризики та фінансову злочинність [4].

Міжнародні стандарти також розвиваються: FATF випустила оновлене керівництво щодо викликів нових технологій (Opportunity & Challenges of New Technologies), у якому підкреслюється важливість стандартизації даних, безпеки інформаційних систем, прозорості алгоритмів і захисту персональних даних у контексті AML/CFT [5].

У практиці фінтех-компаній з'являються конкретні кейси, які демонструють успішне поєднання модулів KYC (know-your-customer) із техніками кібербезпеки: наприклад, у тестуванні безпеки KYC-модуля була застосована перевірка на спроби підробки, rate-limit, а також алгоритм на базі ШІ для виявлення deepfake, що знижує вразливість до шахрайства й відмивання коштів [6].

Попри позитивні тенденції, у публікаціях також виділяють низку проблем. Наприклад, у роботах, присвячених інфраструктурним аспектам, дослідники зазначають, що фінансові установи, особливо в країнах із середнім рівнем доходів, як Україна, мають обмежені ресурси для впровадження дорогих рішень з кібербезпеки та аналітики, що може обмежити масштаб їх застосування [7].

Сумарно, огляд останніх досліджень показує, що напрям кібербезпеки й захисту фінансових даних у контексті AML/CFT набуває дедалі більшої ваги як у національній, так і в міжнародній практиці. Основні тренди – це розвиток аналітичних технологій, інтеграція ШІ, підсилення стандартів даних, а також

синергія між кібербезпекою та державною AML-політикою. Водночас залишаються виклики, пов'язані з ресурсними обмеженнями, потребою у стандартизації та міжвідомчій координації. Ці питання відкривають важливі перспективи для подальших досліджень – як у теоретичній, так і в прикладній площинах.

Метою статті є дослідження ролі кібербезпеки та захисту фінансових даних як ключового інструменту державної політики у сфері протидії легалізації доходів, отриманих злочинним шляхом, зокрема визначення ефективних механізмів забезпечення інформаційної безпеки фінансових систем, оцінка сучасних загроз та викликів, а також пропозиція шляхів удосконалення національної системи фінансового моніторингу з урахуванням міжнародного досвіду та технологічних інновацій.

Виклад основного матеріалу. З розвитком цифровізації фінансових систем значно зростає роль кібербезпеки у забезпеченні національної фінансової безпеки. Досвід провідних країн світу демонструє, що ефективне протидіяння легалізації доходів, отриманих злочинним шляхом, неможливе без інтеграції сучасних інформаційно-аналітичних технологій та засобів кіберзахисту. У національній системі фінансового моніторингу кібербезпека виступає як комплекс заходів, спрямованих на захист даних фінансових транзакцій, конфіденційної інформації клієнтів та аналітичних баз від несанкціонованого доступу, маніпуляцій або витоків.

Аналіз сучасного стану інформаційної безпеки в українських фінансових установах свідчить про низку проблем, серед яких відсутність єдиних стандартів кіберзахисту, недостатній рівень інтеграції між державними органами та комерційними банками, а також обмеженість ресурсів для впровадження сучасних технологій аналізу фінансових ризиків. Значна кількість транзакцій сьогодні здійснюється у цифровому середовищі, що відкриває додаткові можливості для незаконних операцій з відмивання коштів та фінансування тероризму.

У міжнародній практиці багато держав вже реалізували подібні рішення, поєднуючи аналітичні та кібербезпекові інструменти для протидії відмиванню коштів. Однією з найбільш вагомих тенденцій є впровадження ризик-орієнтованого підходу (risk-based approach) у фінансових установах та відомствах, відповідальних за AML-моніторинг. Наприклад, Європейський Союз через Європейський банківський орган (EBA) та майбутню наднаглядову структуру AMLA активно розробляє нові ЄС-технічні стандарти (RTS) для AML/CFT, які включають вимоги до оцінки ризиків та цифрових технологій [8].

Крім цього, у ЄС розвиваються публічно-приватні партнерства для обміну важливою інформацією між державними органами та приватними банками з метою посилення виявлення складних фінансових злочинів. У пропозиціях Єврокомісії наведено, що такі партнерства можуть включати обмін операційними даними в реальному часі, за умови, що це відповідає нормам захисту персональних даних [9].

Ще один приклад – використання штучного інтелекту (ШІ) для підвищення аналітичної потужності систем AML та прозорості транзакцій. У спеціалізованих публікаціях підкреслюють, що ШІ дозволяє не лише підвищити точність виявлення підозрілих операцій, але й мінімізувати кількість хибнопозитивних спрацьовувань, що значно підвищує ефективність розслідувань [10].

На технологічному рівні компанії, такі як ThetaRay (Ізраїль / США / ЄС), пропонують рішення на основі математичних алгоритмів і Big Data, які використовують машинне навчання для аналізу транзакцій, виявлення аномалій і потенційно злочинних схем. Платформи такого типу вже впроваджуються світовими фінансовими установами та FIU для автоматизованого аналізу транзакцій [11].

Щодо регуляторного аспекту, у звіті ЄС (ESAs) за 2024 рік чітко ідентифіковано ризики, пов'язані з новими технологіями: віртуальними валютами, FinTech-рішеннями, RegTech та відсутністю уніфікованого контролю над кіберінфраструктурами фінансових установ [9]. Крім того, ці органи закликають до гармонізації підходів між державами для коректного обміну інформацією та застосування заходів кіберзахисту.

У країнах-членах ЄС вже є конкретні ініціативи щодо цифрових інструментів для фінансових розслідувань. Наприклад, FIU-нет, інструмент, який дозволяє обмінюватися інформацією про підозрілі транзакції в псевдонімізованому вигляді, дає змогу кільком фінансовим розвідувальним підрозділам відстежувати потенційні фінансові злочини й оперативно реагувати [9].

На рівні безпеки даних та кіберзахисту значною мірою розвиваються стандарти GDPR і заходи Європейської Ради із захисту даних (EDPB). У 2025 році заплановано запуск координованих дій по захисту права на стирання даних (right to erasure), що безпосередньо стосується збереження – або видалення чутливої інформації, включно з фінансовими транзакціями [8].

У технічних дослідженнях також наголошується на важливості генерації синтетичних даних для тренування моделей AML із гарантовано відомими підставами транзакцій. Наприклад, окремі фахівці пропонують генератор реалістичних фінансових транзакцій, який допомагає тестувати ефективність машинного навчання без використання конфіденційних або чутливих реальних даних [12].

Також, наукові роботи присвячені застосуванню глибокого навчання (deep learning) у контексті AML. Отже, вищезгадане дослідження демонструє можливість побудови AML-систем на основі deep learning, що аналізують центральність вузлів у мережах транзакцій і виявляють аномальні патерни [12].

Крім технологічних та аналітичних компонентів, міжнародний досвід підкреслює також важливий правовий та організаційний аспект. Ініціативи таких груп, як Wolfsberg Group (асоціація банків), спонукають фінансові установи розробляти правила щодо кібербезпеки, управління даними клієнтів (KYC), захисту від витоків та відповідального використання внутрішньої інформації [11].

Таким чином, міжнародний досвід свідчить про декілька узгоджених підходів, корисних для України:

– впровадження автоматизованих аналітичних систем (з AI, машинним навчанням) саме в AML-контексті;

–розвиток нормативної бази, яка формалізує стандарти кібербезпеки у фінансовій сфері;

–стимулювання публічно-приватної співпраці з обміну інформацією та спільних інструментів розслідування;

–використання синтетичних даних для тренування й тестування аналітичних систем;

–координація між державними та фінансовими інституціями щодо кіберзахисту та AML.

Ці підходи демонструють, що кібербезпека в рамках державної політики AML/CFT не може бути лише опцією – це стратегічний інструмент, який забезпечує інтеграцію технологій, управління ризиком та правове регулювання для протидії фінансовим злочинам. Для України адаптація таких моделей з урахуванням національного контексту (структури FIU, регуляторної функції, правового поля) може значно підвищити ефективність системи захисту фінансових даних та запобігання легалізації злочинних доходів.

В Україні формування національної системи кіберзахисту у фінансовому моніторингу розвивається у контексті адаптації до міжнародних стандартів FATF та рекомендацій MONEYVAL. Державна служба фінансового моніторингу України здійснює комплекс заходів з впровадження аналітичних та інформаційних систем, підвищення кваліфікації персоналу та інтеграції з міжнародними платформами обміну фінансовою інформацією. Водночас необхідно вирішити проблеми, пов’язані з координацією між відомствами, забезпеченням єдиного підходу до стандартизації кіберзахисту та модернізацією програмного забезпечення для аналізу великих обсягів даних.

Особливу увагу слід приділити вдосконаленню методів виявлення транскордонних операцій, які потенційно пов’язані з відмиванням доходів або фінансуванням тероризму. Важливим є поєднання технічних засобів контролю з аналітичними методиками, що дозволяє своєчасно реагувати на підозрілі транзакції та формувати комплексні профілі ризику. Також суттєве значення має розвиток міжнародної співпраці у сфері кібербезпеки, включно з обміном інформацією та досвідом, що сприяє підвищенню ефективності національної системи протидії фінансовим злочинам.

Таким чином, розвиток кібербезпеки та захисту фінансових даних стає ключовим елементом державної політики у сфері протидії легалізації злочинних доходів, оскільки інтеграція сучасних технологій, міжнародного досвіду та нормативних стандартів дозволяє підвищити ефективність фінансового моніторингу та зміцнити національну фінансову безпеку.

Висновки. У результаті дослідження встановлено, що кібербезпека та захист фінансових даних є невід'ємними складовими державної політики у сфері протидії легалізації доходів, отриманих злочинним шляхом. Забезпечення інформаційної безпеки фінансових систем дозволяє не лише ефективно виявляти та попереджувати підозрілі транзакції, але й формувати комплексні профілі ризику, що підвищує ефективність національної системи фінансового моніторингу.

Проаналізовано міжнародний досвід, який свідчить про необхідність інтеграції автоматизованих аналітичних платформ, ризик-орієнтованого підходу та технологій штучного інтелекту у практику державних органів. Встановлено, що успішне впровадження механізмів кіберзахисту потребує не лише технічного оснащення, а й нормативно-правового забезпечення, підвищення кваліфікації персоналу та координації між державними відомствами та фінансовими установами.

Системне удосконалення інструментів фінансового моніторингу з урахуванням сучасних кіберзагроз, інтеграція міжнародного досвіду та технологічних інновацій є ключовими умовами підвищення стійкості фінансової системи та зміцнення національної фінансової безпеки. Результати дослідження мають практичне значення для формування стратегії державного регулювання, розробки стандартів захисту фінансових даних та підвищення ефективності протидії легалізації злочинних доходів в Україні.

Література:

1. Третяк А. Результати CEE. AML дослідження у регіоні EMEA за 2024 рік. Фокус на ефективність. *PwC Україна*. URL: https://www.pwc.com/ua/uk/survey/2025/cee-emea-aml-survey.html

2. Держфінмониторинг пропонує до розгляду міжнародний методологічний досвід у сфері антилегалізаційного стримування. *Держфінмониторинг. Офіційний сайт*. URL: https://fiu.gov.ua/pages/funkcional/news/derzhfinmonitoring-proponuje-do-rozglyadu-mizhnarodnij-metodologichnij-dosvid-u-sferi-antilegalizaczijnogo-strimuvannya.html

3. Тижневий методологічний збірник ПВК/ФТ/ФР Weekly AML/CFT/CPF *Methodological Diges*.2024. URL: https://fiu.gov.ua/assets/userfiles/330/METHODOLOG ICAL% 20DIGESTS/CHERVEN/%5B17_ 06_2024_21_06_2024%5D.pdf

4. Керування ризиками фінансових злочинів і відповідністю вимогами. URL: https://www.microsoft.com/uk-ua/industry/financial-services/resources/managing-crime-financial-risk-compliance-cybersecurity

5. ФАТФ (2021), Можливості та виклики нових технологій для ПВК/ФТ, Париж, Франція, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges newtechnologies-aml-cft.html

6. Підготовка платформи до регуляторного аудиту. Практичні кейси з кібербезпеки. DATAMI. URL: https://datami.ee/ua/cases/kyc-module-security-testing-of-a-fintech-platform

7. Чуницька І. І. Дотримання AML/CFT стандартів у контексті реалізації інфраструктурного потенціалу фінансового ринку України. *Бізнесінформ*. 2020. № 6. С. 267-274.

8. CACEIS. *RegWatch – March 2025*. CACEIS Investor Services Regulatory Environment. URL: https://www.caceis.com/de/regwatch/march-2025/

9. European Commission. (2023, 18 October). *Communication from the Commission to the European Parliament and the Council on the EU roadmap to fight drug trafficking and organised crime* (COM 2023 641 final). Brussels. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52023DC0641&utm_

10. Дмитрієва Ю. Штучний інтелект у AML/CFT комплаєнсі: огляд нових можливостей. URL: https://rates.fm/ua-uk/expert-opinion/shtuchnij-intelekt-u-amlcft-komplayensi

11. ThetaRay. *Wikipedia the free encyclopedia*. URL: https://en.wikipedia.org/wiki/ThetaRay

12. Altman E., Blanuša J., von Niederhäusern L., Egressy B., Anghel A., Atasu K. (2023). *Realistic Synthetic Financial Transactions for Anti-Money Laundering Models*. arXiv preprint arXiv:2306.16424. URL: https://arxiv.org/abs/2306.16424

References:

1. Tretiak A. (2024). *Rezultaty SEE. AML doslidzhennia u rehioni EMEA za 2024 rik. Fokus na efektyvnist* [CEE & EMEA AML Survey 2024: Focus on Efficiency]. PwC Ukraina. URL: https://www.pwc.com/ua/uk/survey/2025/cee-emea-aml-survey.html [in Ukrainian].

2. Derzhfinmonitorynh proponuie do rozghliadu mizhnarodnyi metodolohichnyi dosvid u sferi antylehalizatsiinoho strymuvannia (2024) [The State Financial Monitoring Service Presents International Methodological Experience in AML Deterrence]. Derzhfinmonitorynh: Ofitsiinyi sait. URL: https://fiu.gov.ua/pages/funkcional/news/derzhfinmonitoring-proponuje-do-rozglyadu-mizhnarodnij-metodologichnij-dosvid-u-sferi-antilegalizaczijnogo-strimuvannya.html [in Ukrainian].

3. Weekly AML/CFT/CPF Methodological Digest (2024). *Tyzhnevyi metodolohichnyi zbirnyk PVK/FT/FR* [Weekly AML/CFT/CPF Methodological Digest]. URL: https://fiu.gov.ua/assets/userfiles/330/METHODOLOGICAL%20DIGESTS/CHERVEN/%5B17_06_2024_21_06_2024%5D.pdf [in Ukrainian].

4. Microsoft (2024). *Keruvannia ryzykamy finansovykh zlochyniv i vidpovidnist vymoham* [Managing Financial Crime Risk and Compliance]. URL: https://www.microsoft.com/uk-ua/industry/financial-services/resources/managing-crime-financial-risk-compliance-cybersecurity [in Ukrainian].

5. FATF (2021). *Mozhlyvosti ta vyklyky novykh tekhnolohii dlia PVK/FT* [Opportunities and Challenges of New Technologies for AML/CFT]. Paris: FATF. URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-newtechnologies-aml-cft.html [in English].

6. DATAMI (2024). *Pidhotovka platformy do rehuliatornoho audytu: praktychni keisy z kiberbezpeky* [Preparing a Platform for Regulatory Audit: Cybersecurity Case Studies]. URL: https://datami.ee/ua/cases/kyc-module-security-testing-of-a-fintech-platform [in Ukrainian].

7. Chunytska I. I. (2020). *Dotrymannia AML/CFT standartiv u konteksti realizatsii infrastruktury finansovoho rynku Ukrainy* [Compliance with AML/CFT Standards in the Context of Developing the Infrastructure of Ukraine's Financial Market]. Biznesinform, 6, 267–274 [in Ukrainian].

8. CACEIS. *RegWatch – March 2025*. CACEIS Investor Services Regulatory Environment. URL: https://www.caceis.com/de/regwatch/march-2025/ [in English / German].

9. European Commission. (2023). Communication from the Commission to the European Parliament and the Council on the EU roadmap to fight drug trafficking and organised crime. Brussels. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A 52023 DC0641&utm_ [in English]

10. Dmytriieva Yu. (2024). *Shtuchnyi intelekt u AML/CFT complaiensi: ohliad novykh mozhlyvostei* [Artificial Intelligence in AML/CFT Compliance: Overview of New Opportunities]. URL: https://rates.fm/ua-uk/expert-opinion/shtuchnij-intelekt-u-amlcft-komplayensi [in Ukrainian].

11. ThetaRay. *Wikipedia the free encyclopedia*. URL: https://en.wikipedia.org/wiki/ThetaRay

12. Altman E., Blanuša J., von Niederhäusern L., Egressy B., Anghel A., Atasu K. (2023). *Realistic Synthetic Financial Transactions for Anti-Money Laundering Models*. arXiv preprint arXiv:2306.16424. URL: https://arxiv.org/abs/2306.16424 [in English].