3.3. Методи й моделі оцінювання фінансової безпеки банківської системи

(В. В. Британ, здобувач третього (освітньо-наукового) рівня вищої освіти, Державний податковий університет)

Критичної гостроти набуває проблематика забезпечення фінансової безпеки банківської системи в умовах геополітичної нестабільності, економічної невизначеності та інтенсифікації кіберзагроз. Методологічна недосконаліть існуючого інструментарію діагностики фінансової безпеки банківської системи, відсутність ефективних механізмів раннього детектування гібридних загроз і дефіцит адекватних моделей антикризового менеджменту в умовах воєнного стану генерують системні ризики для стабільності фінансового сектору.

Проблематика ускладнюється потребою в синхронному вирішенні стратегічно важливих завдань: забезпечення операційної резильєнтності в умовах воєнних дій, адаптації до нових парадигм кібербезпеки, інтеграції принципів сталого розвитку (ESG) у банківську практику та підготовки до євроінтеграційних процесів. Принципи екологічного, соціального та корпоративного управління (ESG) набувають парадигмального значення в українському банківському секторі через імплементацію міжнародних стандартів, що детермінує потребу в розробці нових методологічних підходів до оцінювання фінансової безпеки з урахуванням чинників сталого розвитку.

Інституційна недосконаліть нормативно-правового забезпечення регулювання фінансової безпеки в умовах надзвичайних ситуацій, нечіткість розмежування компетенцій регуляторних органів під час воєнного стану та відсутність транспарентних механізмів відповідальності за управлінські рішення створюють додаткові ризики для ефективного забезпечення фінансової стабільності. Потреба в методологічній адаптації підходів до оцінювання фінансової безпеки банківської системи детермінується також активною імплементацією міжнародних стандартів банківського регулювання, зокрема Базельських принципів, що вимагає розробки релевантного інструментарію моніторингу й контролю рівня фінансової безпеки з урахуванням специфіки функціонування вітчизняного банківського сектору в екстремальних умовах.

Актуальні виклики та невирішені проблеми формування ефективної архітектури забезпечення фінансової безпеки банківської системи детермінує потребу в кардинальному переосмисленні методологічних підходів до її діагностики з урахуванням нових реалій функціонування фінансового сектору. В умовах експоненціальної цифрової трансформації фінансового сектору, емерджентності нових типів кіберзагроз і гібридних ризиків проблематика розробки адекватного інструментарію оцінювання фінансової безпеки набуває стратегічної актуальності.

Наукові дослідження підтверджують трансформаційний вплив цифровізації на архітектуру фінансової безпеки банківських установ, що обґрунтовує потребу в поглибленому аналізі цієї проблематики. Водночас критичний аналіз наукових праць, нормативних документів та аналітичних матеріалів демонструє відсутність консенсусу щодо визначення оптимальних параметрів фінансової безпеки й методології її комплексного оцінювання в умовах мультифакторних викликів сучасності.

Особливої наукової уваги потребують недостатньо досліджені аспекти, зокрема: методологія оцінювання впливу технологій штучного інтелекту та процесів автоматизації на параметри фінансової безпеки; інструментарій real-time детектування й нейтралізації кіберзагроз; моделі прогнозування системних ризиків в умовах підвищеної волатильності та інформаційного протиборства; підходи до діагностики резільєнтності банківської системи в кризових умовах з інтеграцією ESG-факторів; методології інкорпорації геополітичних ризиків у систему оцінювання фінансової безпеки.

Четверта промислова революція, синергетично поєднана з воєнними діями та санкційним тиском, детермінує потребу у відповідній адаптації методології оцінювання фінансової безпеки з урахуванням технологічних викликів, військових ризиків та інноваційних форм економічного протиборства. Актуалізується попит розробки інтегрованих оціночних моделей, які б забезпечували системний аналіз взаємозв’язків між традиційними фінансовими ризиками, кіберзагрозами, геополітичними чинниками та імперативами сталого розвитку.

Крім того, недостатньо концептуалізованими залишаються питання адаптації міжнародних стандартів оцінки фінансової безпеки до специфіки функціонування банківської системи в умовах воєнного

стану, розробки механізмів оперативного реагування на гібридні загрози та створення систем раннього попередження про системні ризики в умовах інформаційних обмежень і підвищеної невизначеності.

Діагностика фінансової безпеки відіграє парадигмальну роль у забезпеченні стабільності як індивідуального банківського інституту, так і банківської системи загалом. Враховуючи мультиаспектність і багатовимірність цього конструкту, його оцінювання детермінує застосування комплексного міждисциплінарного підходу, що синергетично поєднує кількісні та якісні методи аналізу з урахуванням динамічної природи сучасного фінансового середовища. Математичний апарат такого оцінювання має бути одночасно практико-орієнтованим для формування стратегій безпеки й достатньо універсальним для адекватного відображення реальності, особливо в контексті еволюції вимог Базельського комітету та імплементації принципів фінансової стабільності. Критичний аналіз наукових джерел демонструє відсутність консенсусу щодо уніфікованої методики оцінювання фінансової безпеки, водночас кожен з існуючих підходів характеризується специфічними перевагами й методологічними обмеженнями. Систематизація наукового доробку дає змогу структурувати всі методи й моделі оцінювання фінансової безпеки банків у такі концептуальні групи:

1. Традиційні методи оцінювання. Методи та моделі, що ґрунтуються на використанні економічних нормативів, представляють класичний підхід до діагностики фінансової стійкості банківських установ. Ці методи базуються на аналізі дотримання регуляторних вимог щодо капіталу, ліквідності, кредитних ризиків та операційної ефективності, проте їхня обмеженість полягає в ретроспективному характері аналізу й недостатній чутливості до нових типів ризиків. Методи та моделі, що базуються на коефіцієнтах і показниках, включно із інтегральними методами оцінювання, забезпечують комплексну діагностику фінансового стану через систему фінансових індикаторів. Інтегральні підходи дають змогу агрегувати множину показників у єдиний індекс, проте викликають методологічні дискусії щодо вагових коефіцієнтів і релевантності отриманих результатів[384].

[384] Muath A., Alia T. Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon.* 2024. № 10 (17). URL : https://www.sciencedirect.com/science/article/pii/S240584402413602X (дата звернення: 24.10.2024).

2. Статистичні та математичні методи. Статистичні методи й моделі оцінювання банківських ризиків охоплюють широкий спектр інструментарію: метод Монте-Карло для симуляції сценаріїв, Z-модель Альтмана для прогнозування банкрутства, модель Дюрана для аналізу кредитних ризиків, VAR-методи для квантифікації ринкових ризиків. Ці підходи характеризуються високим ступенем формалізації, проте вимагають значних обсягів статистичних даних і можуть бути чутливими до структурних змін у фінансовому середовищі. Методи економіко-математичного моделювання забезпечують побудову формалізованих моделей взаємозв'язків між чинниками фінансової безпеки, даючи змогу здійснювати прогностичний аналіз і сценарне планування. Водночас складність таких моделей може створювати проблеми їхньої практичної імплементації та інтерпретації результатів[385].

3. Експертні та аналітичні підходи. Методи експертних оцінювань містять метод Делфі, рейтингові системи, методи перехресного впливу, ієрархічний аналіз Сааті, метод аналогій і сценарний підхід. Ці методи є незамінними в разі відсутності статистичних даних для нових або малоймовірних ризиків і можуть застосовуватись як експліцитно (мережі Байєса, нечіткі моделі), так і імпліцитно в складних моделях прийняття рішень. Аналітичні методи диференціюються на дві категорії: перша охоплює дюрацію, стрес-тестування та GAP-аналіз для оцінювання відсоткового й ліквідного ризиків; друга – методи інтелектуального аналізу даних і нечіткої логіки, включно із скоринговими моделями для кредитного аналізу[386; 387].

4. Інноваційні технологічні підходи. Методи, засновані на машинному навчанні та штучному інтелекті, представляють новітній напрям у діагностиці фінансової безпеки банків. Дослідження демонструють ефективність застосування машинного навчання в управлінні банківськими ризиками, охоплюючи кредитні, ринкові, операційні та ліквідні ризики. Машинне навчання пропонує потужні можливості

---

[385] Давиденко Н. М., Колодяжна В. О. Оцінювання фінансової безпеки банківської системи України. *Науковий вісник Херсонського державного університету. Серія «Економічні науки».* 2020. Вип. 40. С. 51–58.

[386] Martin L., Suneel Sh., Maddulety K. Machine learning in banking risk management: a literature review. *Risks.* 2019. № 7 (1), 29. URL : https://doi.org/10.3390/risks7010029 (дата звернення: 24.10.2024).

[387] Nishant B. Top 8 machine learning use cases in fintech for 2025 / Codiste Blog. 2024. URL : https://www.codiste.com/machine-learning-use-cases-in-fintech (дата звернення: 24.10.2024).

обробки даних, які є критично важливими для обробки значних обсягів інформації, типових для фінансової сфери, та оптимізує операції за рахунок автоматизації рутинних завдань. Сучасні алгоритми машинного навчання дають змогу виявляти складні нелінійні залежності у фінансових даних, що традиційні статистичні методи можуть не розпізнати. Використання машинного навчання в управлінні ризиками забезпечує предиктивну аналітику й моніторинг у реальному часі, що дає банкам нагоду проактивно ідентифікувати та реагувати на ризики, які виникають. Методи оцінювання кібербезпеки та інформаційної безпеки набувають критичного значення в умовах цифровізації банківської діяльності. Кібербезпека продовжує залишатися важливою проблемою для фінансових установ з огляду на швидкий розвиток технологій і зростаючу адаптацію цифрових рішень. ЄЦБ провів першу в історії перевірку стійкості до кіберризиків 2024 року, яка оцінювала, як банки реагують на кібератаки та відновлюються після них[388].

5. Комбіновані та гібридні методи. Комбіновані методи, що охоплюють динамічне оцінювання, методи заповнення пропусків і ймовірнісно-статистичні підходи, дають змогу долати обмеження окремих методів через їхнє синергетичне поєднання. Такі підходи забезпечують більш робоче та всебічне оцінювання фінансової безпеки, проте вимагають значних обчислювальних ресурсів і експертизи для коректної інтерпретації результатів[389].

Сучасні виклики та перспективні напрями полягають в тому, що еволюція методологічного апарату оцінювання фінансової безпеки детермінується новими викликами сучасності. Стрес-тестування прагне забезпечити достатню стійкість банківської системи для продовження підтримки домогосподарств і бізнесу в умовах серйозних, але правдоподібних комбінацій несприятливих шоків. Стрес-тести оцінюють, чи можуть фінансові компанії витримати економічні шоки за різними сценаріями, включно із тими, що виникають від кліматичних змін. Інтеграція ESG-факторів у систему оцінювання фінансової безпеки стає обов’язковою вимогою сучасного банківського регулювання.

[388] Davydenko N. Genesis of enterprise financial security. *Economic processes management* : international scientific E-journal. 2015. № 2. URL : http://epm.fem.sumdu.edu.ua/download/2015_2/2015_2_3.pdf (дата звернення: 24.10.2024).

[389] Muath A., Alia T. Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon.* 2024. № 10 (17). URL : https://www.sciencedirect.com/science/article/pii/S240584402413602X (дата звернення: 24.10.2024).

Кліматичні стрес-тести, які впроваджуються провідними центральними банками світу, демонструють потребу у врахуванні довгострокових екологічних і соціальних ризиків у системі фінансової безпеки банків. Перспективним напрямом розвитку є створення інтегрованих платформ оцінювання фінансової безпеки, що поєднують традиційні методи з інноваційними технологіями штучного інтелекту, машинного навчання та блокчейн-технологій для забезпечення комплексного, динамічного й прогностичного аналізу фінансової стійкості банківських установ в умовах цифрової трансформації та геополітичної нестабільності.

Забезпечення фінансової безпеки банків являє собою критично важливу передумову підтримання стабільності національної фінансової системи та ефективного захисту інтересів усіх категорій клієнтів. У сучасних умовах зростаючої геополітичної невизначеності, кліматичних змін і прискореної трансформації глобального фінансового ландшафту ключовими детермінантами досягнення належного рівня фінансової безпеки банківських установ існують такі стратегічні напрями: впровадження комплексної системи ризик-менеджменту нового покоління, що охоплює не лише традиційні фінансові ризики, а й сучасні виклики, включно із кліматичними ризиками, ESG-факторами, кіберзагрозами та репутаційними ризиками; забезпечення оптимального рівня ліквідності й капіталізації відповідно до міжнародних стандартів Basel III / IV і майбутніх вимог Basel V; підтримання високих стандартів якості кредитного портфеля з урахуванням ESG-критеріїв і сталого фінансування; неухильне дотримання регуляторних вимог, включно із новими директивами ЄС щодо цифрової операційної стійкості (DORA); стратегічне впровадження фінансових інновацій, охоплюючи штучний інтелект, квантові технології та блокчейн, з одночасним забезпеченням кібербезпеки й операційної стійкості; формування інституційної культури управління ризиками та етичного корпоративного управління відповідно до принципів сталого розвитку[390].

Особливої уваги в контексті сучасних викликів заслуговує здатність банківських установ до швидкої адаптації до регуляторних змін і ефективного управління новими типами ризиків в умовах прискореної

[390] Basel Committee on Banking Supervision. Climate-related risk drivers and their transmission channels. 2021. P. 45. URL : https://www.bis.org/bcbs/publ/d517.pdf (дата звернення: 24.10.2024).

цифрової трансформації фінансової галузі. Згідно із методологічним підходом Національного банку України оцінювання фінансової безпеки банків базується на порівняльному аналізі ключових характеристик банківської установи із встановленими нормативними рівнями та експертному оцінюванні за критерієм відсутності негативних індикаторів фінансової нестабільності. Розробка сучасної методології оцінювання фінансової безпеки банків має ґрунтуватися на системі фундаментальних принципів, які доцільно розширити додатковими концептуальними засадами, релевантними для сучасного фінансового середовища: принцип об'єктивності, що передбачає використання достовірної та верифікованої інформації, яка адекватно відображає реальну ринкову ситуацію й базується на надійних і незалежних джерелах даних; принцип кількісної вимірюваності, що забезпечує можливість точного кількісного виміру показників та їх придатність для проведення економіко-статистичного аналізу з використанням сучасних методів математичного моделювання; принцип всебічності та комплексності, що гарантує максимально повне відображення всіх аспектів фінансово-економічної діяльності банку через систему взаємопов'язаних і взаємодоповнюючих критеріїв оцінювання[391]; принцип узагальненості, що дає змогу зведення множини різнорідних показників до єдиного інтегрального значення з чітко визначеними межами й градаціями оцінювання; принцип оперативності та реалтайм-моніторингу, що забезпечує здатність проведення оцінювання в режимі реального часу з активним використанням інноваційних аналітичних інструментів і технологій штучного інтелекту; принцип періодичності та систематичності, що передбачає регулярне проведення оцінювання з урахуванням можливостей машинного навчання й адаптивних алгоритмів; принцип можливості вдосконалення, що забезпечує гнучкість методологічного апарату щодо внесення змін, модифікацій і покращень; принцип прозорості та відкритості, що гарантує забезпечення доступності релевантної інформації для всіх зацікавлених сторін з відповідною диференціацією даних для різних категорій користувачів; принцип інтерактивності й зворотного зв'язку, що передбачає наявність ефективних механізмів впливу зовнішніх суб'єктів на процес удосконалення методики оцінювання; принцип економічної доцільності, що забезпечує значне перевищення отриманих результатів над витратами

[391] Cyber resilience and financial market infrastructures / European Central Bank. URL : https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html (дата звернення: 12.07.2024).

на їхнє досягнення з урахуванням довгострокової вартості управління ризиками; принцип регуляторної сумісності, що гарантує відповідність методології міжнародним стандартам і національним регуляторним вимогам. Сучасні виклики цифрової епохи та посилення геополітичних ризиків обумовлюють потребу в доповненні традиційних принципів новими концептуальними засадами: принцип цифрової адаптивності, що забезпечує здатність методології до швидкого пристосування до динамічних змін у цифровому фінансовому середовищі, включно із розвитком цифрових валют центральних банків (CBDC)[392]; принцип антикризової адаптивності, що гарантує можливість оперативного врахування нових типів ризиків, охоплюючи пандемічні, військові та санкційні загрози; принцип кіберстійкості, що забезпечує захист від кіберзагроз і підтримання операційної стійкості відповідно до стандартів ISO 27001/27032; принцип ESG-інтеграції, що передбачає врахування чинників екологічної, соціальної та управлінської відповідальності в процесі оцінювання. Фундаментальні принципи формування комплексної системи оцінювання фінансової безпеки банків охоплюють такі ключові елементи: системну погодженість і взаємозв'язаність методологічних підходів; процедурну повноту охоплення всіх етапів оцінювального процесу; функціональну ортогональність незалежних аналітичних модулів; інформаційну взаємозалежність і консистентність отриманих результатів; цілеспрямовану відповідність критеріїв оцінювання поставленим завданням; функціональну раціональність без дублювання процедур та інструментів; багатоцільову універсальність і адаптивність методологічного апарату; процедурну відкритість для постійного вдосконалення та модернізації; раціональну доповнюваність системи новими методами й підходами. У контексті останніх міжнародних практик і зростаючих кіберзагроз особливої актуальності набуває впровадження гібридної системи оцінювання фінансової безпеки, що органічно поєднує традиційні методи фінансового аналізу з передовими технологіями квантового шифрування, розподіленого реєстру (blockchain), штучного інтелекту й хмарних обчислень[393].

[392] Martin L., Suneel Sh., Maddulety K. Machine learning in banking risk management: a literature review. *Risks.* 2019. № 7 (1), 29. URL : https://doi.org/10.3390/risks7010029 (дата звернення: 24.10.2024).

[393] Cyber resilience and financial market infrastructures / European Central Bank. URL : https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html (дата звернення: 12.07.2024).

Такий підхід уже успішно апробовано та впроваджено провідними міжнародними банками, включно із Goldman Sachs, Morgan Stanley та європейськими системно важливими банками, що демонструє його практичну ефективність і перспективність. Зокрема, інтеграція технологій машинного та глибинного навчань (deep learning) дає змогу виявляти складні нелінійні взаємозв'язки між різними чинниками ризику, прогнозувати потенційні загрози на основі патерн-аналізу й забезпечувати раннє попередження про системні ризики[394].

Проведений системний аналіз сучасних досліджень у сфері оцінювання фінансової безпеки банків, здійснений провідними вітчизняними та зарубіжними дослідниками, засвідчує, що переважна більшість існуючих методик базується на традиційному економічному й фінансовому аналізі, зосереджуючись на комплексному оцінюванні таких ключових параметрів: структури та якості активів банку; достатності капіталу відповідно до міжнародних стандартів; рівня ліквідності та її управління; спектру й рівня ризиків; показників прибутковості та ефективності; якості корпоративного управління й ризик-менеджменту. Основні методологічні підходи до оцінювання охоплюють: інтегральний метод, що дає змогу об'єднати різнорідні показники в єдиний комплексний індикатор; коефіцієнтний аналіз, заснований на розрахунку й інтерпретації системи фінансових коефіцієнтів; рейтинговий підхід, що передбачає ранжування та порівняльний аналіз; експертний метод, що базується на професійних судженнях і якісній оцінці спеціалістів. Для забезпечення комплексності та об'єктивності оцінювання широко використовується таксономічний аналіз, методологія якого охоплює такі етапи: побудову матриці спостережень із релевантними показниками; стандартизацію елементів матриці для забезпечення порівнянності; формування вектора-еталону як базису для порівняння; визначення статистичних відстаней між досліджуваними елементами; розрахунок інтегрального показника фінансової безпеки. Варто особливо зазначити, що сучасний міжнародний досвід провідних фінансових установ світового рівня (як-от JP Morgan Chase, Deutsche Bank, HSBC, Santander, BNP Paribas тощо) демонструє критичну потребу в доповненні традиційних методів оцінювання

[394] Latest updates on the banking package / European Commission. 2023. URL : https://finance.ec.europa.eu/news/latest-updates-banking-package-2023-12-14_en (дата звернення: 24.10.2024).

фінансової безпеки банків сучасними інструментами предиктивної аналітики, заснованими на обробці великих даних (Big Data), технологіях штучного інтелекту та квантових обчислень. Такий інноваційний підхід дає змогу виявляти потенційні загрози й ризики на значно ранніх стадіях їхнього розвитку, ще до їхньої фактичної матеріалізації, що суттєво підвищує ефективність превентивних заходів та антикризового управління. Крім того, використання технологій Natural Language Processing (NLP) дає змогу аналізувати неструктуровані дані, охоплюючи новини, соціальні мережі й регуляторні повідомлення, для виявлення репутаційних та операційних ризиків[395].

На сучасному етапі розвитку банківської системи ефективний аналіз рівня фінансової безпеки потребує розробки та впровадження комплексного інтегрального показника, здатного адекватно відображати багатоаспектну природу фінансової безпеки. Відповідно до концептуального підходу провідних дослідників у цій сфері існуючі інтегровані показники можна систематизувати за двома основними групами: 1) показники комплексного оцінювання загального рівня фінансової безпеки банку як цілісної системи; 2) показники, що здійснюють оцінювання окремих структурних складників з подальшою їхньою інтеграцією в узагальнений індикатор.

Сучасний методологічний підхід вимагає значного розширення системи інтегрованих показників через охоплення таких інноваційних категорій: динамічні показники з урахуванням часових рядів і трендового аналізу з використанням ARIMA та GARCH-моделей; показники, засновані на результатах стрес-тестування та сценарного моделювання, включно із кліматичними стрес-тестами; показники оцінювання взаємозв'язків і системних ризиків з використанням мережевого аналізу; показники, що базуються на аналізі ринкових даних та альтернативних індикаторів (включно із супутниковими даними); показники кібербезпеки й операційної стійкості відповідно до стандартів NIST; показники ESG-факторів і сталого розвитку з урахуванням таксономії ЄС; показники геополітичних та санкційних ризиків. У контексті антикризового управління й підвищення резилієнтності банківської системи особливої актуальності набувають такі інноваційні методи:

[395] Achieving greater convergence in cyber incident reporting / Financial Stability Board. 2023. URL : https://www.fsb.org/2023/04/recommendations-to-achieve-greater-convergence-in-cyber-incident-reporting-final-report/ (дата звернення: 24.10.2024).

динамічне стрес-тестування з використанням Monte Carlo симуляцій і методів машинного навчання; сценарне моделювання з елементами штучного інтелекту, включно із нейронними мережами та алгоритмами глибинного навчання; комплексе оцінювання системної та кіберстійкості з використанням мережевого аналізу й теорії графів; всебічне оцінювання репутаційної стійкості з аналізом sentiment-аналізу та соціальних мереж; аналіз геополітичних і макроекономічних шоків з використанням Vector Autoregression (VAR) моделей; оцінювання кліматичних та ESG-ризиків із застосуванням satellite imagery та альтернативних даних[396].

Критичний аналіз існуючих інтегральних методик дає змогу ідентифікувати такі фундаментальні недоліки й обмеження: недостатню гнучкість та адаптивність до різких структурних змін у фінансовому середовищі; обмежену здатність враховувати складні нелінійні взаємозв'язки між різними чинниками ризику; недостатнє врахування системних, військових, геополітичних і кліматичних ризиків; обмежену прогностичну здатність та недостатнє врахування впливу інноваційних фінансових продуктів і технологій; відсутність механізмів реалтайм-моніторингу й раннього попередження. В умовах гібридних загроз, військової агресії та геополітичної нестабільності, включно із санкційними режимами й торговельними війнами, надзвичайно актуальним стає впровадження інтегральних методик оцінювання фінансової безпеки банків, які здатні в режимі реального часу враховувати військові, кібернетичні, геополітичні та санкційні ризики, забезпечуючи швидку адаптацію банківської системи до критичних змін зовнішнього середовища й підтримання фінансової стабільності в екстремальних умовах. Особливе значення має розробка систем раннього попередження, здатних детектувати каскадні ефекти та системні ризики[397].

Перспективним напрямом розвитку методології оцінювання фінансової безпеки банків є інтеграція технологій квантових обчислень для обробки надскладних багатофакторних моделей, використання блокчейн-технологій для забезпечення прозорості й незмінності

[396] Achieving greater convergence in cyber incident reporting / Financial Stability Board. 2023. URL : https://www.fsb.org/2023/04/recommendations-to-achieve-greater-convergence-in-cyber-incident-reporting-final-report/ (дата звернення: 24.10.2024).

[397] Basel Committee on Banking Supervision. Principles for the sound management of operational risk / Bank for International Settlements. 2021. URL : https://www.bis.org/bcbs/publ/d515.pdf# (дата звернення: 24.10.2024).

даних, впровадження систем штучного інтелекту для автоматизованого виявлення аномалій і прогнозування кризових сценаріїв, а також застосування технологій доповненої реальності (AR) та віртуальної реальності (VR) для візуалізації ризиків. Окрема увага приділяється розвитку федеративного навчання (federated learning) для співпраці між банками без розкриття конфіденційної інформації. Такий комплексний підхід дасть змогу створити принципово нову генерацію систем оцінювання фінансової безпеки, здатних ефективно функціонувати в умовах зростаючої складності та невизначеності сучасного фінансового ландшафту, охоплюючи виклики Web 3.0 і децентралізованих фінансів (DeFi)[398].

Відповідним дослідникам[399; 400; 401] вдалося помітити певні закономірності, що методика кількісного оцінювання фінансової безпеки банку базується на двох ключових групах показників: показники ефективності діяльності й показники рівня захищеності банку. Детальний аналіз наукових праць засвідчує, що показники ефективності діяльності охоплюють фінансові коефіцієнти рентабельності, ліквідності, капіталізації та якості активів, які характеризують спроможність банківської установи генерувати прибуток і підтримувати стабільне функціонування в конкурентному середовищі. Водночас показники рівня захищеності банку охоплюють індикатори кредитного ризику, операційного ризику, ринкового ризику та ризику ліквідності, які дають змогу оцінити стійкість фінансової установи до внутрішніх і зовнішніх загроз. Комплексний підхід до застосування цих двох груп показників дає нагоду сформувати цілісну картину фінансової безпеки

[398] Cyber resilience and financial market infrastructures / European Central Bank. URL : https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html (дата звернення: 12.07.2024).

[399] Analysis of the impact of state-owned banks on the sustainability of public finances / Davydenko N., Boiko S., Cherniavska O., Nehrey M. *Economies.* 2023. № 11 (9). P. 229. URL : https://doi.org/10.3390/economies11090229 (дата звернення: 24.10.2024).

[400] Informational and analytical systems for forecasting the indicators of financial security of the banking system of Ukraine / Davydenko N., Lutsyk Y., Buriak A., Vovk L. *Journal of Information Technology Management.* 2023. Vol. 2 (15). P. 1–13. URL : https://jitm.ut.ac.ir/article_92315_f5446ad0813cf2c7e8a457125265b371.pdf (дата звернення: 24.10.2024).

[401] Ключка О. В., Богріновцева Л. М., Федорчук Н. М. Особливості використання сучасних банківських продуктів та технологій в діяльності банків як суб'єктів фінансового ринку. *Актуальні проблеми економіки.* 2023. № 12 (270). С. 86–93. URL : https://eco-science.net/wp-content/uploads/2023/12/12.23._topic_Olha-V.-Kliuchka-Liudmyla-M.-Bohrinovtseva-Natalia-%D0%9C.-Fedorchuk-86-93.pdf (дата звернення: 07.10.2024).

банку, оскільки високі показники ефективності без належного рівня захищеності можуть призвести до надмірного ризику, а надмірна обережність може знизити прибутковість діяльності. Тому сучасні методології оцінювання фінансової безпеки банківської системи передбачають збалансоване використання обох категорій індикаторів з урахуванням їхнього взаємозв'язку та взаємозалежності в контексті макроекономічних умов і регуляторних вимог.

В умовах прогресуючої цифровізації фінансового сектору та впровадження технологій Industry 4.0 найбільш ефективним і науково обґрунтованим методом оцінювання інформаційних ризиків визнається побудова байєсових мереж з елементами нечіткої логіки, що дає змогу оптимально комбінувати суб'єктивні експертні оцінки зі статистичними даними та машинним навчанням, забезпечуючи високий рівень точності прогнозування й адаптивність до динамічних змін операційного середовища. Ця методологія особливо ефективна в контексті невизначеності та обмеженості історичних даних щодо нових типів цифрових загроз, включно із квантовими обчисленнями та їхнім потенційним впливом на криптографічні системи банків. Комплексний аналіз сучасних підходів дає змогу констатувати, що система оцінювання фінансової безпеки банківської системи базується на трьох фундаментальних групах показників з урахуванням принципів ESG (Environmental, Social, Governance) та сталого розвитку.

Перша група – фінансові результати – охоплює комплексне оцінювання загальних активів і їхньої якості з використанням алгоритмів штучного інтелекту для аналізу кредитоспроможності, структури кредитного портфеля з диференціацією корпоративного та роздрібного сегментів, включно із зеленими кредитами, депозитної бази юридичних і фізичних осіб з урахуванням цифрових депозитів і стейблкоїнів, співвідношення ключових показників до валового внутрішнього продукту, аналіз відсоткових та невідсоткових доходів від фінтех-сервісів, ефективності резервування й покриття ризиків з використанням динамічних моделей IFRS 9.

Друга група – фінансова стабільність – містить розширений аналіз достатності регулятивного капіталу першого та другого рівнів відповідно до міжнародних стандартів Basel IV і вимог до цифрового операційного ризику, якості кредитного портфеля та рівня непрацюючих кредитів з використанням машинного навчання для раннього виявлення проблемних активів, показників рентабельності активів

(ROA) і власного капіталу (ROE) з корекцією на кліматичні ризики, структури доходів і витрат, включно з інвестиціями в кібербезпеку, коефіцієнтів ліквідності (LCR, NSFR) з урахуванням криптоактивів, валютної позиції та валютних ризиків у контексті цифрових валют центральних банків (CBDC), концентрації великих ризиків, включно з технологічними провайдерами, операцій з деривативами та DeFi протоколами, операційної ефективності через призму автоматизації та cost-to-income ratio з урахуванням цифрової трансформації[402].

Третя група – макроекономічна стабільність – враховує динаміку реального ВВП з урахуванням цифрової економіки, інфляційні процеси, включно з криптоінфляцією, монетарну політику центрального банку в контексті цифрової валюти, стан зовнішнього боргу та його цифрову компоненту, стабільність валютного курсу щодо глобальних стейблкоїнів, платіжний баланс країни з урахуванням транскордонних цифрових платежів, а також геополітичні ризики та їхній вплив на кібербезпеку фінансової системи.

Водночас поточна методологічна основа оцінювання, закріплена в Методичних рекомендаціях щодо розрахунку рівня економічної безпеки України, затверджених наказом Міністерства розвитку і торгівлі України від 29.10.2013 № 1277, передбачає системний підхід через п’ять послідовних етапів: формування релевантної системи індикаторів з урахуванням специфіки національної банківської системи, визначення їхніх характеристичних значень і науково обґрунтованих допустимих меж, нормалізацію показників для забезпечення їхньої статистичної порівнянності, встановлення вагових коефіцієнтів значущості на основі експертних оцінок та емпіричного аналізу, а також розрахунок інтегрального індексу банківської безпеки з можливістю декомпозиції за окремими компонентами.

Можна з упевненістю стверджувати, що сучасні виклики цифрової трансформації та Четвертої промислової революції створюють принципово нові вектори загроз банківській безпеці, які потребують інноваційних підходів до оцінювання й управління на основі технологій real-time моніторингу. До таких загроз належать: ризики, пов’язані

[402] International Monetary Fund. Global Financial Stability Report: Crypto-assets and decentralized finance – navigating risks, regulation, and innovation. Washington DC : IMF Publications, 2024. URL : https://www.imf.org/en/Publications/GFSR (дата звернення: 24.10.2024).

з децентралізованими фінансовими протоколами (DeFi) та їхнім потенційним використанням для відмивання коштів і фінансування тероризму, експоненціальне зростання кількості та складності кібератак з використанням генеративного штучного інтелекту й квантових алгоритмів, шахрайство із застосуванням методів соціальної інженерії та deepfake-технологій нового покоління, критичні вразливості програмних інтерфейсів (API) і мультихмарних архітектур, ризики витоку й компрометації біометричних даних у контексті міжнародних стандартів приватності, загрози безперервності бізнесу через масштабні технологічні збої, кіберінциденти та потенційні квантові атаки на криптографічні системи, а також ризики маніпулювання алгоритмами машинного навчання (adversarial attacks)[403]. Не менш важливим аспектом сучасного банківського нагляду є ефективна інтеграція макро- та мікропруденційних підходів до регулювання банківської безпеки з використанням технологій RegTech і SupTech. Макропруденційний нагляд зосереджується на ідентифікації та мітигації системних ризиків через алгоритми раннього попередження, забезпеченні стабільності банківської системи загалом через динамічні антициклічні буфери капіталу й посилені вимоги до глобальних системно важливих банків (G-SIBs), тоді як мікропруденційний підхід забезпечує персоналізований контроль на рівні окремих фінансових установ через індивідуальні вимоги до капіталу, ліквідності й операційних ризиків з урахуванням їхнього цифрового профілю та інноваційної діяльності[404].

Сучасні тенденції у сфері оцінювання фінансової безпеки банківської системи характеризуються впровадженням технологій глибокого машинного навчання для прогнозування кредитних і операційних ризиків, використанням розширених регуляторних пісочниць (regulatory sandboxes) для тестування блокчейн-рішень і криптоактивів, розвитком комплексного стрес-тестування на основі кліматичних та кіберризиків відповідно до рекомендацій Групи двадцяти, впровадженням концепції відкритого банкінгу з посиленими вимогами до zero-trust-архітектури, розробкою міжнародних стандартів для оцінювання

[403] Assessment of risks to financial stability from crypto-assets / Financial Stability Board. 2022. URL : https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/ (дата звернення: 24.10.2024).

[404] Group of Twenty. Policy ɜriorities for ɸddressing climate-ĸelated ainancial ĸisks / G20 Sustainable Finance Working Group Report. 2024. URL : https://www.g20.org/content/dam/gtwenty/gtwenty_new/priorities_themes/sustainable_finance/ (дата звернення: 24.10.2024).

ризиків штучного інтелекту у фінансових послугах, а також створенням глобальних систем раннього попередження про трансскордонні фінансові загрози.

Комплексність оцінювання фінансової безпеки банківської системи потребує гіперконвергентної інтеграції традиційних і революційних методів, включно з моделюванням сценаріїв на основі генеративного штучного інтелекту для створення синтетичних сценаріїв стрес-тестування, цифровими двійниками банківських екосистем для симуляції та тестування в реальному часі, квантово-покращеним моделюванням Монте-Карло для підвищення точності ризикових прогнозів, застосуваннями нейроморфних обчислень для розпізнавання патернів у виявленні шахрайства, frameworks пояснювального штучного інтелекту для забезпечення регуляторної відповідності.

Сучасне ультрадинамічне та взаємопов'язане фінансове середовище вимагає постійної методологічної адаптації через інтеграцію розвідки загроз у реальному часі з глобальними потоками кібербезпеки, прогнозне моделювання геополітичних ризиків з використанням супутникових зображень та аналітики соціальних мереж, кліматично-скориговані моделі кредитних ризиків з урахуванням фізичних сценаріїв і сценаріїв переходу, оцінювання ризиків етики штучного інтелекту для виявлення та пом'якшення алгоритмічної упередженості, відстеження часової лінії квантових загроз із динамічним оновленням криптографічних вимог.

Критично важливим є розвиток автономних систем безпеки через архітектури безпеки, що самовідновлюються з можливостями автоматичного пом'якшення загроз, автономні системи реагування на інциденти з прийняттям рішень на основі штучного інтелекту, безперервну валідацію безпеки через автоматизоване тестування на проникнення, інтелектуальну оркестрацію безпеки з міжплатформенною інтеграцією, проактивне управління вразливостями з використанням алгоритмів полювання на загрози.

Розвиток автономної кіберстійкості передбачає створення самоадаптивних екосистем безпеки з використанням рійового інтелекту, AI-керованих кіберімунних систем з біологічно-інспірованими механізмами захисту, досліджень нейроморфних процесорів безпеки для виявлення загроз з ультранизькою затримкою. Впровадження колаборативних AI-агентів для розподіленого полювання на загрози охоплює

розробку вуглецево-нейтральних операцій безпеки з оптимізацією зелених обчислень, створення інтегрованих з ESG-моделей ризиків з аналізом кліматичних сценаріїв, дослідження принципів циркулярної економіки в управлінні ресурсами кібербезпеки, впровадження frameworks сталого управління штучним інтелектом.

Безпека банківської діяльності в метавсесвіті передбачає розвиток імерсивних інтерфейсів безпеки для віртуальних банківських середовищ, створення систем автентифікації на основі аватарів з верифікацією цифрової ідентичності, дослідження безпеки просторових обчислень для банківських застосувань віртуальної реальності, впровадження механізмів виявлення загроз у міжреальнісному просторі.

Біолого-цифрова конвергенція містить розробку зберігання даних на основі ДНК для ультрабезпечних систем резервного копіювання, створення синтезу біометрії та blockchain для незламних систем ідентичності, дослідження органічних обчислювальних елементів для посиленої обробки безпеки, впровадження біологічно-інспірованих алгоритмів штучного інтелекту для адаптивного реагування на загрози.

Ці революційні напрями досліджень у найближчому майбутньому дадуть змогу створити надійну, автономну та проактивну систему оцінювання фінансової безпеки банківської системи, що відповідатиме викликам уже П’ятої промислової революції та людино-центричної цифрової трансформації, забезпечить квантово-стійкі й кліматично-адаптивні банківські операції, сприятиме розвитку довірчого штучного інтелекту та етичних фінансових технологій, підтримуватиме сталі цифрові фінанси й принципи циркулярної економіки, гарантуватиме кіберсуверенітет і стратегічну технологічну незалежність.

Успішна імплементація цих стратегічних напрямів забезпечить еволюційний стрибок банківського сектору в нову еру цифрової фінансової безпеки, характеризовану автономністю, стійкістю та адаптивністю до майбутніх викликів П’ятої промислової революції.