ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Фінанси, банківська справа страхування та фондовий ринок

УДК 004.056.5:336.71

DOI https://doi.org/10.5281/zenodo.16509500

Інструменти аналізу даних для оцінки кіберризиків у фінансових послугах

Боженко Вікторія Володимирівна
кандидат економічних наук, доцент, доцент кафедри економічної кібернетики, Сумський державний університет, м. Суми, Україна,
https://orcid.org/0000-0002-9435-0065

Пахненко Олена Михайлівна
кандидат економічних наук, доцент, доцент кафедри фінансових технологій і підприємництва, Сумський державний університет, м. Суми, Україна,
https://orcid.org/0000-0002-4703-4078

Яровенко Ганна Миколаївна
доктор економічних наук, доцент, доцент кафедри економічної кібернетики, Сумський державний університет, м. Суми, Україна,
https://orcid.org/0000-0002-8760-6835

Койбічук Віталія Василівна
кандидат економічних наук, доцент, завідувач кафедри економічної кібернетики, Сумський державний університет, м. Суми, Україна,
https://orcid.org/0000-0002-3540-7922

Прийнято: 09.07.2025| Опубліковано: 20.07.2025

Анотація. Мета. *Метою статті є аналіз підходів до оцінки кіберризиків у фінансовому секторі та дослідження можливостей застосування сучасних інструментів аналізу даних для підвищення ефективності кіберзахисту фінансових установ.* ***Методи.*** *У дослідженні використано метод системного аналізу нормативних актів, а також структурований підхід до класифікації кіберзагроз відповідно до ENISA. Проведено огляд кількісних і якісних метрик оцінювання ризиків, таких як частота інцидентів, фінансові втрати, показники VaR та ES. Використано порівняльний аналіз превентивних і адаптивних інструментів управління кіберризиками.* ***Результати.*** *У результаті дослідження встановлено, що ефективне управління кіберризиками вимагає інтеграції превентивних та адаптивних підходів до кіберзахисту. До превентивних віднесено інструменти виявлення вразливостей, тестування на проникнення, моніторинг уразливих компонентів, кіберрозвідку. Адаптивні методи включають SIEM-системи, системи запобігання вторгненням (IDPS), засоби поведінкової аналітики, інструменти штучного інтелекту та машинного навчання. Описано інструменти для виявлення фішингу, шахрайства, атаки типу DoS/DDoS, а також заходи реагування на витоки даних. Наведено приклади використання аналітичних платформ для прогнозування кіберзагроз і виявлення аномалій на основі шаблонів поведінки користувачів. Зазначено, що багатофакторна оцінка кіберзагроз дозволяє підвищити точність виявлення потенційно небезпечних подій і мінімізувати шкоду від інцидентів.* ***Висновки.*** *Результати дослідження підтверджують, що багаторівнева стратегія кіберзахисту, яка поєднує інструменти аналізу даних, оперативний моніторинг та дотримання нормативних вимог, є ключовою для ефективного управління кіберризиками у фінансовому секторі. Інтеграція інтелектуальних інструментів оцінки кіберзагроз значно підвищує цифрову*

стійкість і безпеку фінансових установ в умовах зростання кількості та складності кіберзагроз.

Ключові слова: *кіберризики, кіберзагрози, кібербезпека, банківська безпека, захист інформації, оцінка ризиків, фінансова аналітика.*

Data mining tools for cyber risk assessment in financial services

Victoria Bozhenko

PhD in Economics, Associate Professor, Associate Professor of the Economic Cybernetics Department, Sumy State University, Sumy, Ukraine,
https://orcid.org/0000-0002-9435-0065

Olena Pakhnenko

PhD in Economics, Associate Professor, Associate Professor of the Department of Financial Technologies and Entrepreneurship, Sumy State University, Sumy, Ukraine,
https://orcid.org/0000-0002-4703-4078

Ganna Yarovenko

Doctor of Economics, Associate Professor, Associate Professor of the Economic Cybernetics Department, Sumy State University, Sumy, Ukraine,
https://orcid.org/0000-0002-8760-6835

Vitalia Koybichuk

PhD in Economics, Associate Professor, Head of the Economic Cybernetics Department, Sumy State University, Sumy, Ukraine,
https://orcid.org/0000-0002-3540-7922

Abstract. ***Purpose.*** *The purpose of this article is to analyse current approaches to cyber risk assessment in the financial sector and to explore the applicability of modern data analysis tools for enhancing the effectiveness of cybersecurity in financial institutions.* ***Methods.*** *The study is based on a comprehensive review of international regulatory frameworks (including the NIST Cybersecurity Framework, Basel Committee principles, DORA), analysis of quantitative and qualitative cyber risk metrics (e.g., incident frequency, financial losses, VaR, ES), and a structured classification of cyber threats according to ENISA. A comparative approach is employed to identify preventive and adaptive technologies used in cyber risk management.* ***Results.*** *The research identifies artificial intelligence, machine learning, and behavioural analytics as key technologies for cyber threat detection, incident prediction, and real-time response. The study outlines a detailed taxonomy of cyber threats – ransomware, malware, social engineering, insider threats, DDoS, and disinformation – and maps each to corresponding assessment tools, such as SIEM systems, EDR, IDPS, threat intelligence platforms, penetration testing, and vulnerability scanning. Additionally, compliance assessment tools supporting adherence to GDPR, ISO/IEC 27001, and PCI DSS standards are examined. The role of fraud detection, Darknet monitoring, and AI-based access protection is emphasized, along with predictive analytics as a means of anomaly detection and behavioural verification.* ***Conclusions.*** *The findings demonstrate that a multi-layered cybersecurity strategy that integrates real-time monitoring, advanced data analytics, and regulatory compliance tools is essential for managing cyber risks in the financial sector. The adoption of intelligent cyber risk assessment instruments significantly enhances the digital resilience and operational continuity of financial institutions in the context of growing cyber threats.*

Keywords: *cyber risks, cyber threats, cybersecurity, banking security, information protection, risk assessment, financial analytics.*

Постановка проблеми. Сучасний фінансовий сектор значною мірою залежить від інформаційних технологій, що робить його вразливим до кіберзагроз. Банки, страхові компанії, біржі та інші фінансові установи використовують цифрові платформи для проведення транзакцій, управління активами, обробки персональних даних клієнтів тощо. Відповідно, будь-яка вразливість в IT-інфраструктурі може призвести до масштабних фінансових втрат, витоку конфіденційної інформації або навіть підриву довіри до всієї фінансової системи.

З кожним роком кількість атак на фінансовий сектор зростає. За даними звіту IBM [1] у 2024 році фінансовий сектор зазнав суттєвого зростання витрат, пов'язаних з кіберінцидентами – середній обсяг збитків сягнув 6,08 млн доларів США, що перевищує відповідний показник 2023 року (5,9 млн доларів США) та є на 22% вищим від показника збитків від кіберінцидентів в інших галузях. Такі втрати сигналізують про критичну необхідність системного підходу до кіберзахисту у сфері фінансових послуг, що включає застосування ефективних методів оцінки кіберризиків та своєчасне виявлення й нейтралізацію потенційних загроз.

Аналіз останніх досліджень і публікацій. Оцінювання кіберризиків у фінансовому секторі регулюється низкою міжнародних стандартів і нормативних документів, які визначають принципи управління ризиками, вимоги до кібербезпеки та заходи щодо захисту інформаційних систем. В банківському секторі застосовуються рекомендації Базельського комітету (BCBS), зокрема «Principles for Operational Resilience», в яких визначено підходи до забезпечення операційної стійкості банків, включаючи управління кіберризиками, та «Sound Practices: Implications of fintech developments for banks and bank supervisors», що містить рекомендації щодо кібербезпеки в умовах цифрової трансформації фінансових послуг. Для банків, що працюють у країнах ЄС, обов'язковим є дотримання Директиви NIS2 та регламенту

DORA, які визначають вимоги до кібербезпеки, стрес-тестування IT-систем та управління цифровими ризиками. У США та багатьох інших країнах використовується рамкова модель NIST Cybersecurity Framework (CSF) для оцінювання та управління кіберризиками. Також одним із широко визнаних стандартів, що може використовуватися для сертифікації систем управління інформаційною безпекою банків, є ISO/IEC 27001.

Питання оцінки кіберризиків у сфері фінансових послуг є також предметом активних наукових досліджень. Вітчизняні та іноземні автори розглядають питання ідентифікації, оцінювання, управління та моніторингу кіберризиків, а також впливу цифрових загроз на фінансову стабільність банків і небанківських установ. Серед вітчизняних вчених дослідження у даному напрямку здійснюють Гончаренко І. [2], Криклій О. [3], Кришталь Г. та ін. [4], Тищенко С., Пархоменко О., Дармосюк В. [5], Трусова Н., Чкан І. [6] та інші. Вагомий внесок у дослідження оцінки кіберризиків у фінансовому секторі зробити такі іноземні науковці як Бувере А. (Bouveret A.) [7], Дюпон Б. (Dupont B.) [8], Маккой Е. (McCoy E.) [9], Шехаб Р. (Shehab R.) [10] та інші.

Виділення невирішених раніше частин загальної проблеми. Попри високий рівень наукового інтересу до тематики кібербезпеки у фінансовому секторі, у науковій літературі все ще недостатньо уваги приділяється прикладним аспектам інтеграції інструментів аналізу даних у процес оцінки кіберризиків. Зокрема, слабо висвітленими залишаються практичні підходи до використання превентивних і адаптивних інструментів кіберзахисту, що базуються на штучному інтелекті, поведінковій аналітиці, тестуванні на проникнення, розвідці загроз та інструментах оцінки вразливостей. У більшості наявних досліджень бракує систематизації інструментів за етапами реагування на кіберінциденти, а також конкретного зіставлення типів загроз із відповідними технологічними рішеннями. Таким чином, дана стаття покликана заповнити прогалину між нормативним баченням управління

кіберризиками та їхньою фактичною оцінкою за допомогою сучасних цифрових технологій, що дозволяє сформувати підґрунтя для побудови проактивної та технологічно обґрунтованої стратегії кіберзахисту у фінансовому секторі.

Формулювання цілей статті (постановка завдання). Метою статті є аналіз підходів до оцінки кіберризиків у фінансовому секторі та дослідження можливостей застосування сучасних інструментів аналізу даних для підвищення ефективності кіберзахисту фінансових установ.

Виклад основного матеріалу дослідження. У сфері фінансових послуг реалізація кіберзагроз може завдати значної шкоди як фінансовим установам та користувачам фінансових послуг, так і фінансовому сектору загалом. Негативними наслідками реалізації кіберзагроз у фінансовому секторі можуть бути прямі фінансові збитки, втрата даних, порушення операційної діяльності, втрата ділової репутації та зниження конкурентоспроможності, юридична відповідальність, дестабілізація банківської системи. У зв'язку з цим, національні регулятори приділяють значну увагу питанням кібербезпеки та управління кіберризиками у фінансовому секторі.

Національний банк України встановлює вимоги до організації системи управління кіберризиками в банках через низку нормативних документів. Зокрема, згідно із Положенням про організацію кіберзахисту в банківській системі України [11] банки зобов'язані:

– розробити та впровадити політики і процедури кіберзахисту, які охоплюють ідентифікацію, оцінку, моніторинг та контроль кіберризиків;

– призначити відповідальних осіб за кібербезпеку, які координуватимуть заходи з управління кіберризиками та реагування на інциденти;

– забезпечити безперервність діяльності, розробивши плани реагування на кіберінциденти та відновлення після них;

– проводити навчання та підвищення кваліфікації персоналу щодо питань кібербезпеки та управління кіберризиками.

Щодо оцінювання кіберризиків у банках, НБУ встановлює чіткі вимоги та надає рекомендації, спрямовані на підвищення рівня кібербезпеки та стійкості банківської системи України. Зокрема, банки зобов'язані щорічно проводити самооцінку стану інформаційної безпеки та кіберзахисту, складати відповідний звіт і подавати його до НБУ. Методичні рекомендації щодо управління операційним ризиком включають управління кіберризиком та передбачають необхідність ідентифікації, оцінки та моніторингу ризиків інформаційної безпеки. НБУ здійснює контроль за дотриманням банками вимог щодо кібербезпеки, зокрема шляхом перевірок та аналізу звітів про оцінку ризиків інформаційної безпеки.

У міжнародній практиці для оцінки кіберризиків застосовуються різні кількісні та якісні показники. Найбільш застосовуваними (через відносну простоту вимірювання та високу інформативність) є показники, що стосуються частоти кіберінцидентів та обсягу фінансових втрат. До таких показників, зокрема, належать [7]:

– кількість атак на рік;

– середні втрати від однієї кібератаки;

– агреговані втрати через кібератаки за рік;

– ризикові показники (VaR – Value at Risk, ES – Expected Shortfall) для оцінки максимальних можливих втрат.

У документі Базельського комітету з банківського нагляду [12] кількісні та якісні показники кіберстійкості банків класифіковані за етапами реагування на кіберзагрози: показники до компрометації (попереджувальні метрики), показники під час компрометації та показники після компрометації (табл. 1).

Таблиця 1

Показники оцінки кіберстійкості банків за етапами реагування на кіберзагрози

Етапи реагування на кіберзагрози	Групи метрик	Приклади метрик
До компрометації	Виявлення вразливостей	- кількість нових вразливостей (за типами OWASP); - вразливості на 1000 рядків коду; - кількість додатків, які вводяться в експлуатацію з вразливостями
	Захист від шкідливих програм	- кількість зупинених шкідливих програм; - унікальні зразки шкідливого програмного забезпечення, орієнтовані на банк;
	Захист від фішингу	- відомі фішингові сайти, що націлені на банк; - час до видалення фішингового сайту (години у відкритому доступі); - частка персоналу, що реагує на фішингові тести (% від загального складу);
	Система управління доступом та конфігурацією	- кількість систем, захищених IAM (Identity and Access Management); - відсоток відповідності налаштувань інформаційної безпеки; - частка пройдених перевірок доступу користувачів
	Тестування безпеки	- проведені тестування на проникнення (за типом і рівнем ризику); - перевірки безпеки постачальників за останні 12 місяців (% покриття); - відстеження застарілих патчів (у днях за критичністю)
Під час компрометації	Виявлення та аналіз інцидентів	- кількість кінцевих точок із виявленим шкідливим ПЗ; - кількість серверів із виявленим шкідливим ПЗ; - кількість витоків даних; - типи інцидентів (відмова в обслуговуванні, зловмисний код, соціальна інженерія тощо)
	Підготовленість до інцидентів	- наявність планів відновлення та реагування (за типами загроз); - кількість репетицій реагування на інциденти
Після компрометації	Моніторинг загроз та наслідків	- кількість атак типу APT (Advanced Persistent Threat); - заблоковані підключення до шкідливих веб-сайтів; - загальні фінансові втрати банку; - втрати клієнтів

Джерело: складено авторами на основі [12]

ISSN: 2786-9431

Оцінка кіберризиків у сфері фінансових послуг вимагає надійних інструментів аналізу даних, які можуть обробляти величезні обсяги даних, виявляти вразливості в інформаційній безпеці фінансових установ, на основі чого впроваджувати проактивні заходи для мінімізації можливих кібератак. Використовуючи передові технології, такі як штучний інтелект, машинне навчання та поведінкова аналітика, інструменти оцінки кіберзагроз дозволяють фінансовим установам залишатися кіберстійкими. За результатами опитування 32 представників центральних банків з різних країн світу виявлено, що 57% респондентів вважають ефективним використання генеративного штучного інтелекту для виявлення кіберзагроз [13]. Разом з цим, підвищення рівня кіберзахисту за допомогою штучного інтелекту також може допомогти зменшити нестачу експертів з кібербезпеки, заощадити кошти та оптимізувати стратегії кіберзахисту фінансових установ [14].

Оцінка кіберризиків фінансових установ ґрунтується на використанні різних інструментів, які можна поділити на превентивні та адаптивні (рис. 1). Превентивні методи спрямовані на випередження загроз та їх запобігання ще до того, як вони зможуть завдати шкоди фінансовим установам. Адаптивні інструменти дозволяють фінустановам реагувати на загрози в режимі реального часу та мінімізувати можливі наслідки атак. Застосування комбінації превентивних і адаптивних інструментів дозволяє фінансовим установам значно знизити ризики кібератак, забезпечуючи безпеку своїх клієнтів та активів.

ISSN: 2786-9431

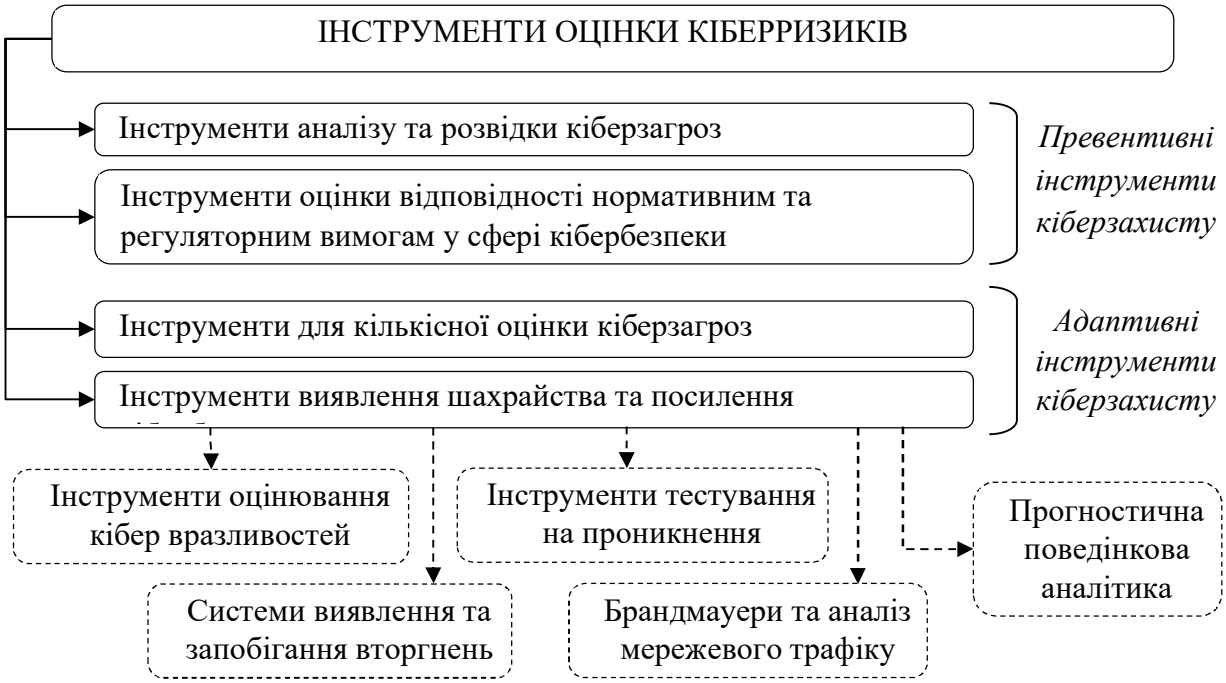

Рис. 1. Основні типи інструментів оцінки кіберризиків

Джерело: власна розробка авторів

Критичну роль у забезпеченні безпеки та стійкості фінансових установ до кіберзагроз відіграють інструменти аналізу та розвідки кіберзагроз (превентивний етап), які дозволяють ідентифікувати небезпеки на ранніх стадіях, попереджати можливі атаки та зміцнювати захист критично важливих систем. Для розвідки кіберзагроз можуть бути використані різні підходи:

– агрегація кіберзагроз, що передбачає збір розвідданих про загрози з відкритих джерел (OSINT) та власних каналів безпеки;

– аналіз і кореляція кіберзагроз, що передбачає використання штучного інтелекту та машинного навчання для аналізу даних, виявлення закономірностей і кореляції індикаторів компрометації (підозрілі IP-адреси, підозрілі домени та URL-адреси, аномальний мережевий трафік, хеші файлів, фішингові email-адреси тощо);

– моніторинг Darknet, що дозволяє виявляти витоки облікових даних, схеми фінансового шахрайства та викрадену банківську інформацію на веб-сайтах, що мають приховані IP-адреси сервера, на якому вони розміщені.

Зокрема, банк може виявити скомпрометовані дані кредитних карток до того, як вони були використані в шахрайських цілях, і заздалегідь повідомити постраждалим клієнтам.

Фінансовий сектор суворо регулюється законами щодо кібербезпеки, захисту даних і управління ризиками. Інструменти оцінки відповідності (Compliance & Regulatory Framework Assessment Tools) допомагають організаціям відповідати міжнародним стандартам і нормативним вимогам, таким як General Data Protection Regulation, ISO 27001, Payment Card Industry Data Security Standard, Digital Operational Resilience Act, Basel III. Інструменти оцінки відповідності та нормативно-правових вимог широко використовуються фінансовими установами для запобігання штрафам та юридичним санкціям, виявлення та усунення вразливостей у системах безпеки, а також створювати аудиторські звіти для регуляторів.

У режимі реального часу фінансові установи використовують передові інструменти для виявлення шахрайства та посилення їх кібербезпеки, в основі яких алгоритми штучного інтелекту та машинного навчання. Вагому роль в виявленні кібершахрайства відіграє оцінювання вразливостей в IT-середовищі фінансових установ, що передбачає автоматичне сканування та аналіз систем для виявлення потенційних вразливостей, неправильних конфігурацій і застарілого програмного забезпечення. За результатами сканування відбувається пріоритизація вразливостей за рівнем їх потенційного впливу на функціонування фінансової установи та безперебійне надання послуг. У доповненні до оцінювання вразливостей фінансові установи можуть здійснювати тестування на проникнення (імітація кібератаки). На практиці може бути реалізовано зовнішнє (перевірка рівня захисту публічно доступних активів – веб-сайти, брандмауери та сервери електронної пошти, мобільні додатки тощо) та внутрішнє тестування (визначає слабкі місця в системі

керування доступом та мережі, оцінювання рівня кіберобізнаності співробітників тощо).

Для моніторингу, виявлення та реагування на зловмисну активність у мережі компанії можуть використовуватися системи виявлення та запобігання вторгненням (IDPS), які дозволяють відстежувати мережевий трафік на наявність підозрілої активності, попереджати команди безпеки про виявлення потенційних загроз, автоматично видаляти шкідливі пакети, блокувати IP-адреси або припиняти сесії.

Брандмауери діють як перша лінія захисту у фінансовій мережі, відстежуючи та контролюючи вхідний і вихідний трафік на основі правил безпеки. Вони допомагають запобігти несанкціонованому доступу, DDoS-атакам і проникненню шкідливих програм.

Аналіз мережевого трафіку передбачає моніторинг у реальному часі та глибоку перевірку фінансових транзакцій, передачу даних і шаблонів зв'язку для виявлення аномалій і потенційних кіберзагроз.

Одним із основних слабких місць у кібербезпеці фінансових установ є пристрої, через які відбувається зараження шкідливим програмним забезпеченням, програмами-вимагачами та розкриття інсайдерської інформації через випадкові, недбалі чи навмисні дії співробітників. Для протидії цим кіберзагрозам фінансові установи використовують технології з виявлення та реагування на загрози кінцевих точок (робочі станції співробітників, банкомати, мобільні банківські пристрої, сервери).

Інструменти для оцінювання безпеки інформації та подій (Security Information and Event Management, SIEM) збирають дані про безпеку з мережевих пристроїв, серверів і додатків, а потім використовують штучний інтелект, машинне навчання (ML) і поведінкову аналітику для виявлення та зменшення кіберризиків.

ISSN: 2786-9431

Предиктивна аналітика виявляє закономірності та аномалії в даних, таких як мережеві журнали, поведінка користувачів і канали розвідки загроз, щоб спрогнозувати потенційні кіберзагрози до того, як вони матеріалізуються. Передові аналітичні платформи аналізують унікальні патерни поведінки клієнтів, такі як швидкість набору тексту або рухи миші, для автентифікації користувачів і виявлення потенційного захоплення облікових записів. Крім цього, аналізуючи поведінку, вподобання та демографічні дані клієнтів, аналітичні платформи допомагають створювати більш цілеспрямовані та ефективні заходи безпеки для різних груп клієнтів [15].

Фінансові установ можуть самостійно оцінювати рівень їх кіберстійкості на основі розроблених методик за допомогою математичних та статистичних моделей, та виявляти вразливі місця в системі інформаційної безпеки та впроваджувати заходи безпеки для захисту конфіденційних даних і фінансових активів. Рамкова концепція кібербезпеки NIST (Cybersecurity Framework CSF) надає фінансовим організаціям структурований підхід до визначення, захисту, виявлення, реагування на кіберзагрози та відновлення після кібератак. Фінансові установи використовують цю систему для посилення своєї кібербезпеки та дотримання регуляторних вимог, таких як GLBA (Закон Грамма-Ліча-Блайлі) та рекомендації FFIEC (Федеральної ради з перевірки фінансових установ). У таблиці 2 подані основні інструменти оцінки кіберзагроз, які можуть протистояти найбільш поширеним видам кібершахрайств у сфері фінансових послуг.

Таблиця 2

Категорії кіберзагроз ENISA та відповідні інструменти оцінки кіберзагроз

Вид кіберзагроз	Інструменти оцінки кіберзагроз	Сфера дії
Програма-здирник	SIEM-інструменти, захист кінцевих точок, аналіз кіберзагроз на основі штучного інтелекту	Виявляє незвичайну активність шифрування даних, підозрілі файли та вимоги викупу
Шкідливе ПЗ	Розвідка загроз, оцінка вразливостей SIEM та аналіз загроз на основі штучного інтелекту	Визначає зразки шкідливого ПЗ, атаки нульового дня та вразливості системи
Соціальна інженерія (фішинг, BEC, дипфейки)	Виявлення шахрайства, захист електронної пошти, прогностична поведінкова аналітика	Аналізує поведінку користувачів, виявляє фішингові посилання та шахрайські дії
Внутрішні загрози	Аналіз поведінки стейкхолдерів, виявлення шахрайства на основі шаблонів	Моніторинг аномальної поведінки співробітників, виявлення зловживань обліковими даними і привілеями
Атаки відмови в обслуговуванні	Захист від DDoS, SIEM-інструменти та захист мережі	Ідентифікація масштабних кібератак, аналіз трафіку та захист критичних сервісів
Дезінформація та фейкові новини	Розвідка загроз, OSINT-інструменти	Розпізнавання фейкових новин, моніторинг загрози в даркнеті

Джерело: складено авторами на основі [16], [17], [18], [19]

Висновки. Інструменти оцінки кіберзагроз відіграють важливу роль у виявленні та зменшенні ризиків. Фінансові установи повинні застосовувати багаторівневий підхід, використовуючи SIEM, EDR, розвідку загроз та управління вразливостями для боротьби з постійно зростаючими загрозами. Інструменти виявлення на основі штучного інтелекту підвищують безпеку, виявляючи шкідливі програми, програми-вимагачі та експлойти «нульового дня». Інструменти для захисту електронної пошти та виявлення шахрайства, допомагають запобігти фішингу та атакам соціальної інженерії. Отже, проактивна стратегія кібербезпеки та системний підхід, що поєднує моніторинг у режимі реального часу, оцінку ризиків та реагування на

інциденти, сприятиме збереженню стабільності та довіри до фінансового сектору в умовах цифровізації.

Подяки. Роботу виконано в рамках проєкту Жан Моне (Модуль) «Практики ЄС щодо захисту фінансової системи від кіберзагроз» (EU_PITCH).

Список використаних джерел

1. Cost of a Data Breach Report 2024. IBM. URL: https://www.ibm.com/reports/data-breach (дата звернення: 03.05.2025).

2. Гончаренко І. Кіберзагрози фінансового сектора в умовах війни. *Економіка та суспільство*. 2023. № 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-82

3. Криклій О. А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. DOI: https://doi.org/10.32702/2307-2105-2020.10.50

4. Кришталь Г., Самофалова М., Сахно Л., Федина, В., Мокієнко Т., Єрмолаєва М. Кіберризики у фінансовій та банківській системі: аналіз прямих і систематичних втрат. *Financial and Credit Activity Problems of Theory and Practice*. 2025. № 2(61). С.125-140. DOI: https://doi.org/10.55643/fcaptp.2.61.2025.4672

5. Тищенко С. І., Пархоменко О. Ю., Дармосюк В. М. Моделювання та аналіз ризиків кібератак на фінансові установи з використанням методів математичної статистики та Python. *Modern Economics*. 2024. № 48. С.130-136. DOI: https://doi.org/10.31521/modecon.V48(2024)-16

6. Трусова Н. В., Чкан І. О. Кіберзахист банківської системи україни в умовах цифрових трансформацій. *Збірник наукових праць ТДАТУ імені Дмитра Моторного (економічні науки)*. 2023. № 1(47). С. 151-163. DOI: https://doi.org/10.31388/2519-884X-2023-47-151-163

7. Bouveret A. Cyber risk for the financial sector: A framework for quantitative assessment. *IMF Working Paper*. 2018. WP/18/143. URL: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924 (дата звернення: 03.06.2025).

8. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*. 2019. Vol. 5 (1). DOI: https://doi.org/10.1093/cybsec/tyz013

9. McCoy E. Cybersecurity Regulations and Risk Management in the Financial Sector: A Comparative Analysis. *Law, Economics and Society*. 2025. Vol. 1(1). P. 115. DOI: https://doi.org/10.30560/les.v1n1p115

10. Shehab R., Abrar S., Almaiah M., Alkhdour T., Belal M., Alwadi B., Alrawad M. (2024). Assessment of Cybersecurity Risks and Threats on Banking and Financial Services. *Journal of Internet Services and Information Security*. 2024. Vol. 14. P. 167-190. DOI: https://doi.org/10.58346/JISIS.2024.I3.010

11. Положення про організацію кіберзахисту в банківській системі України. Постанова НБУ № 178 від 12.08.2022. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text (дата звернення: 12.06.2025)

12. Cyber resilience: Range of practices. Basel Committee on Banking Supervision; Bank for International Settlements, 2018. URL: https://www.bis.org/bcbs/publ/d454.pdf (дата звернення: 03.05.2025)

13. Aldasoro I., Doerr S., Gambacorta L., Notra S., Oliviero T., Whyte D. Generative Artificial Intelligence and Cyber Security in Central Banking. *Journal of Financial Regulation.* 2025. Vol. 11(1). P. 119-128. DOI: https://doi.org/10.1093/jfr/fjae008

14. Leitner G., Singh J., van der Kraaij A., Zsámboki B. The rise of artificial intelligence: benefits and risks for financial stability. *Financial Stability Review*.

2024. Vol. 1. URL: https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html (дата звернення: 10.05.2025)

15. Advanced Analytics Banking: Transforming the Financial Landscape. Matellio. 2024. URL: https://www.matellio.com/blog/advanced-analytics-banking (дата звернення: 10.05.2025)

16. Leszczyna R. Review of cybersecurity assessment methods: Applicability perspective. *Computers and Security*. 2021. Vol. 108. DOI: https://doi.org/10.1016/j.cose.2021.102376

17. Roldán-Molina G., Almache-Cueva M., Silva-Rabadão C., Yevseyeva I., Basto-Fernandes V. A Comparison of Cybersecurity Risk Analysis Tools. *Procedia Computer Science*. 2017. Vol. 121. P. 568-575. DOI: https://doi.org/10.1016/j.procs.2017.11.075

18. Safitra M. F., Lubis M., Fakhrurroja H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability (Switzerland)*. 2023. Vol. 15(18). DOI: https://doi.org/10.3390/su151813369

19. Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F., Materne S. Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*. 2022. Vol. 47(3). P. 698-736. DOI: https://doi.org/10.1057/s41288-022-00266-6