ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ INFORMATION TECHNOLOGY AND MATHEMATICAL MODELING

УДК 004.7

Oleksandr Turchynov, D.S. (Economic Science), Professor, Chief Researcher
ORCID ID: https://orcid.org/0009-0002-6014-2687 ***e-mail:*** oleksandr@turchynov.com

Mykola Khudyntsev, Candidate of Physical and Mathematic Science, Associated Professor, Senior Researcher
ORCID ID: https://orcid.org/0000-0002-9324-6901 ***e-mail:*** nh@te.net.ua

Oleg Klymenkov, Candidate of Engineering Sciences, Senior Researcher
ORCID ID: https://orcid.org/0000-0001-7664-5225 ***e-mail:*** oleg@klymenkov.com

Oleksii Khomenko, postgraduate
ORCID ID: https://orcid.org/0009-0007-4866-8244 ***e-mail:*** oleksii.khomenko.sci@gmail.com

Igor Palazhchenko, postgraduate
ORCID ID: https://orcid.org/0009-0000-0491-7068 ***e-mail:*** palazhchenko.ihor@gmail.com

The Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, Ukraine

NETWORK AND ECONOMIC COMPONENT OF FINANCIAL CYBERSECURITY INDICES

Abstract. *The main goal of the study is to develop approaches to using financial (stock exchange) cybersecurity indices to assess cybersecurity and the level of maturity of corporate information assets. The objectives of the study are to analyze existing financial (stock exchange) cybersecurity indices, the methodology for their formation, the application of indices to assess the state of national cybersecurity systems and markets, the development of approaches for modeling the behavior of individual financial cybersecurity indices, and to substantiate their application. The paper examines the methodological foundations of the formation of financial cybersecurity indices depending on network and economic indicators. The methodologies for the formation of existing financial (stock exchange) cybersecurity indices are analyzed, and a model of a generalized financial cybersecurity index is proposed. The application of individual index indicators in the national cybersecurity system is investigated, and their use for collecting and processing cyber statistics data is proposed. The possibility of using game-theoretic resource cooperative models to predict the behavior of individual financial cybersecurity indices is analyzed. To assess cybersecurity and the level of maturity of corporate information assets, an independent use of the cyber insurance index (cyber insurance maturity) is proposed, and the domain structure of the financial cybersecurity indices and the cyber insurance index is compared. The results obtained can be used to assess the state of corporate information resources in order to optimize decision-making.*
Keywords: *financial (stock) cybersecurity indices, network and economic indicators (indicators), methodology.*

О.В. Турчинов, М.М. Худинцев, О.А. Клименков, О.А. Хоменко, І.Л. Палажченко

Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, м. Київ, Україна

МЕРЕЖЕВА ТА ЕКОНОМІЧНА СКЛАДОВА ФІНАНСОВИХ ІНДЕКСІВ КІБЕРБЕЗПЕКИ

Анотація. *Основною метою дослідження є розробка підходів використання фінансових (біржових) індексів кібербезпеки для оцінювання кібербезпеки та рівня зрілості корпоративних інформаційних активів. Завдання дослідження полягають в аналізі існуючих фінансових (біржових) індексів кібербезпеки, методології їх формування, застосування індексів для оцінювання стану національних систем та ринків кібербезпеки, розробці підходів для моделювання поведінки окремих фінансових індексів кібербезпеки та обґрунтуванні їх застосування. У роботі розглядаються методологічні основи формування фінансових індексів кібербезпеки у залежності від мережевих та економічних показників. Проаналізовано методології формування існуючих фінансових (біржових) індексів кібербезпеки, запропоновано модель узагальненого фінансового індексу кібербезпеки. Досліджено застосування окремих показників індексів у національній системі кібербезпеки, а також запропоновано їх використання для збору та обробки даних кіберстатистики. Проаналізовано можливість використання теоретико-ігрових ресурсних кооперативних моделей для прогнозування поведінки окремих фінансових індексів кібербезпеки. Для оцінювання кібербезпеки та рівня зрілості корпоративних інформаційних активів запропоновано незалежне використання індексу кіберстрахування (зрілості кіберстрахування), проведено порівняння доменної структури фінансових індексів кібербезпеки та індексу кіберстрахування. Отримані результати можна використовувати для оцінки стану корпоративних інформаційних ресурсів з метою оптимізації прийняття рішень.*

Ключові слова: *фінансові (біржові) індекси кібербезпеки, мережеві та економічні показники (індикатори), методологія.*

https://doi.org/10.32347/2411-4049.2025.4.102-113

Вступ

Дослідження процесів у екосистемах кібербезпеки, як правило, обмежується мережевим рівнем. Але цікавим напрямом досліджень є оцінка впливу подій і інцидентів у кіберпросторі на економіку на макро- і мікрорівні. Окрім розмірів загальних збитків, які несуть суб'єкти економічної діяльності, галузеві та національні економіки від кіберінцидентів, адекватним інструментом такої оцінки на макроскопічному (інтегральному) рівні також є фінансові (біржові) індекси кібербезпеки (*Financial Stock Cybersecurity Indices*, скор. – FSCI) [1, 2].

Відповідна категорія індексів є підгрупою категорії набори даних – індексів, які формуються за допомогою автоматичної візуалізації даних, у даному випадку фінансових (у т.ч. біржових). Показово, що поведінка FSCI помітно залежить від зміни мережевих індексів кібербезпеки, які, в свою чергу, визначаються мережевими даними, зокрема індикаторами кіберподій та індикаторами компрометації.

Аналіз методології формування індексів та їх показників (*objectives*) свідчить про те, що переважна більшість з FSCI формуються автоматично на підставі біржової інформації та даних мережевої активності (у т.ч. зловмисної). Усі індекси мають складну структуру, доменами якої є спеціалізовані економічні або мережеві субіндекси. Переважна більшість індексів формується резидентами США.

Дані індексів у більшості випадків є відкритими. Прогностичний та кореляційний аналіз FSCI, біржових та мережевих субіндексів, а також побудова відповідних моделей дозволяє формувати адекватні методи дослідження організаційно-технічних показників кібербезпеки високого рівня.

У той же час FSCI недостатньо використовуються у практиці оцінювання загроз та збитків у кіберпросторі. В Україні відповідні підходи досліджені недостатньо, теоретично не розвинуті, практично не використовуються. Це пов'язано, насамперед, з недостатнім розвитком та імпорт-орієнтованістю національного ринку кібербезпеки.

Основною метою даного наукового дослідження є розроблення та теоретико-методологічне обґрунтування підходів до використання FSCI як інструменту комплексного оцінювання рівня кібербезпеки та ступеня зрілості корпоративних інформаційних активів. Зазначені індекси розглядаються як кількісні інтегральні показники, що відображають динаміку стану кіберзахисту в умовах функціонування цифрової економіки та глобалізованих фінансових ринків.

Для досягнення поставленої мети у дослідженні визначено низку взаємопов'язаних завдань. Зокрема, здійснюється системний аналіз існуючих FSCI, досліджуються принципи та методології їх формування, а також оцінюються можливості практичного застосування таких індексів для аналізу стану національних систем кібербезпеки та відповідних ринків. Окрему увагу приділено розробленню підходів до моделювання поведінки окремих FSCI, виявленню закономірностей їх змін у часі та обґрунтуванню доцільності використання цих індексів у процесах стратегічного планування й управління кіберризиками.

У роботі розглядаються методологічні засади формування фінансових індексів кібербезпеки з урахуванням сукупності мережевих, технологічних та економічних показників, які відображають як рівень захищеності інформаційних систем, так і фінансово-економічні аспекти діяльності суб'єктів ринку. Проаналізовано підходи та алгоритми побудови наявних FSCI, визначено їх переваги та обмеження, а також запропоновано гібридну модель фінансового індексу кібербезпеки, що дозволяє інтегрувати різнорідні показники в єдину аналітичну метрику.

Крім того, у дослідженні вивчено можливості застосування окремих індикаторів фінансових індексів у межах національної системи кібербезпеки, зокрема для моніторингу її стану та оцінювання ефективності реалізації державної політики у сфері кіберзахисту. Запропоновано використання таких індексів як джерела даних для збору, узагальнення та аналітичної обробки кіберстатистики, що створює передумови для підвищення обґрунтованості управлінських рішень і розвитку інструментарію кількісної оцінки кібербезпеки на макро- та мікрорівнях.

Ринок кібербезпеки в Україні

У 2025 році було проведено перше комплексне дослідження ринку кібербезпеки України DataDriven за ініціативою підкомітету з кібербезпеки EBA та CyberTech комітету Асоціації IT Ukraine за сприяння Aspen Institute (Київ) та за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» [3].

Згідно з [3], український ринок кібербезпеки продемонстрував суттєве зростання, збільшившись у чотири рази протягом останніх восьми років і досягнувши у 2024 році обсягу близько 138 млн доларів США. Показовим є практично двократне зростання в умовах повномасштабної агресії та кібервійни російської федерації. Згідно з прогнозами, у середньостроковій перспективі (до 2029 року) очікується подальше зростання ринку приблизно на 50%, що дозволить йому досягти рівня 209 млн доларів США. Провідним сегментом залишається мережева безпека, водночас найбільш динамічний розвиток демонструють напрями хмарної безпеки, захисту даних та кінцевих точок, що відображає зростаючий попит на сучасні технологічні рішення в умовах цифрової трансформації.

Встановлено, що повномасштабна війна спричинила істотне зростання інтенсивності та складності кібератак, що, своєю чергою, зумовило підвищений попит на автоматизовані та інноваційні засоби захисту, на відміну від глобального ринку, де домінують безпекові послуги. Основними об'єктами атак та захисту залишаються державні органи, підприємства оборонно-промислового комплексу, телекомунікаційний сектор, фінансові установи та енергетика. За перше півріччя 2025 року в Україні зафіксовано 3018 кіберінцидентів, що на 17% перевищує показник попереднього року. Найбільш поширеними типами атак є атаки програм-здирників (*ransomware*), фішинг (*phishing*) та відмова в обслуговуванні (*DDoS*).

Світовий ринок кібербезпеки за підсумками 2024 року сягнув 186 млрд доларів США, при цьому частка України залишається меншою за 0.1%. Водночас темпи зростання українського ринку кібербезпеки випереджають світові (практично, удвічі). Також Україна відіграє роль важливого інноваційного центру, випереджаючи низку країн за рівнем кіберекспертизи завдяки розвитку R&D-напряму та створенню прикладних рішень.

Ключовими драйверами розвитку українського ринку кібербезпеки є цифровізація економіки, зростання ризиків фінансових і репутаційних втрат від кібератак, постійний тиск на критичну інфраструктуру, активніше використання технологій штучного інтелекту, а також підтримка з боку міжнародних програм технічної допомоги. Інновації, у першу чергу, застосування штучного інтелекту та блокчейн-технологій, формують нові підходи до кіберзахисту, в той час, як концепція «нульової довіри» визначає нові моделі поведінки користувачів.

Методологічні основи формування фінансових (біржових) індексів кібербезпеки

Методологічні основи формування FSCI спираються на аналіз методології формування окремих індексів, наведених у *Таблиці 1*. Аналіз методології формування експертних індексів кібербезпеки раніше проводився авторами статті, а також О. Трофимчуком, А. Давидюком, А. Жиліним та іншими, в термінах мережевих показників кібербезпеки.

Таблиця 1. Фінансові (біржові) індекси кібербезпеки

Index		1st Edition	Editions/ year	Indicators Qty	Rate Entities Qty
Кіберіндекс BVP Nasdaq Emerging Cloud [4]	BVPCI	2011	multi	1	68
Індекс кібербезпеки MSCI [5]	CSI	2017	4	6	49
Індекс ефективності кібербезпеки [6]	CSPI	2016	multi	6	14
Індекс кібербезпеки Evolve Fund [7]	ECSIF	2017	multi	3	38
Індикатор кіберризиків FICO [8]	FCRS	2001	multi	5	>21 mil.
Індекс кібербезпеки та безпечності даних Foxberry [9]	FXCI	2013	2	2	49
Індекс кібербезпеки ISE [10]	HXR	2010	multi	3	60
Оперативний глобальний індекс кібербезпеки [11]	IECSI	2017	2	9	10-50
«Чистий» кіберіндекс [12]	IPCI	2015	1	3	30
Індекс кібербезпеки S&P [13]	KCSI	2013	Multi	5	n/a
Індекс майбутньої безпеки S&P [14]	KSEC UREP	2013	Multi	7	n/a
Індекс кібербезпеки Nasdaq [15]	NQC YBR	2015	Multi	6	>10
Перший індекс кіберзахисту [16]	PCDI	2017	4	3	58
Глобальний індекс кібербезпеки Soloactive [17]	SGCSI	2017	Multi	n/a	-

У межах дослідження проаналізовано 14 інформаційних джерел, що охоплюють біржові індекси, індексні методології, тематичні фінансові продукти та аналітичні матеріали провідних міжнародних індекс-провайдерів (Nasdaq, MSCI, Solactive, Indxx, SGX, Foxberry, S&P Dow Jones Indices тощо).

Nasdaq CTA Cybersecurity Index (NQCYBR™) є одним з найбільш репрезентативних галузевих індексів, який відстежує динаміку публічних компаній, що здійснюють основну діяльність у сфері кібербезпеки. Методологія індексу базується на галузевій класифікації Consumer Technology Association (CTA) та використовує ринково-капіталізаційне зважування з періодичним переглядом складу. Індекс має глобальне охоплення та використовується як базовий індикатор для низки біржових фондів (ETF).

Indxx Cybersecurity Index застосовує більш жорсткий підхід до відбору компаній, вимагаючи, щоб щонайменше 50% їхньої виручки генерувалося у сфері кібербезпеки. Ваги компонентів визначаються за модифікованою ринковою капіталізацією з обмеженням концентрації, що знижує домінування найбільших емітентів.

MSCI Cybersecurity Index формує склад на основі власної тематичної класифікації MSCI та поєднує критерії галузевої приналежності, ліквідності та ринкової капіталізації. Методологія MSCI є детально формалізованою та орієнтованою на інституційних інвесторів, що підвищує стабільність індексу, але водночас зменшує його чутливість до швидких технологічних змін.

Solactive Cybersecurity Index (у тому числі ESG-орієнтовані версії) поєднує класичні принципи ринково-капіталізаційного зважування з додатковими фільтрами сталого розвитку. У результаті склад індексу формується не лише з урахуванням технологічної спеціалізації компаній, але й їх відповідності ESG-критеріям, що впливає на структуру ризиків та дохідності.

iEdge–FactSet Thematic Indices (SGX) та Foxberry Thematic Cybersecurity Indices представляють підхід тематичного індексування, за якого компанії включаються до індексу на основі аналітичних моделей експозиції до певної теми (кібербезпеки), незалежно від формальної галузевої класифікації. Такий підхід підвищує гнучкість, але знижує прозорість критеріїв добору.

Інші розглянуті джерела (Vontobel, Evolve ETFs, S&P Kensho Cyber Security Index) здебільшого описують індексні фінансові продукти або похідні інструменти, що відтворюють поведінку базових індексів кібербезпеки, а не формують власні незалежні індексні методології.

Спільні риси:

- використання тематичного або галузевого підходу до відбору компаній;
- домінування ринково-капіталізаційного або модифікованого ринково-капіталізаційного зважування;
- використання автоматизованих технічних засобів для формування окремих показників індексів;
- регулярне ребалансування та перегляд складу (квартальний або піврічний);
- орієнтація на публічні компанії з достатньою ліквідністю;
- глобальний характер індексів.

Відмінності:

- критерії включення (виручка від кібербезпеки, тематична експозиція, галузева класифікація);
- використання або відсутність ESG-фільтрів;
- ступінь концентрації портфеля;
- різна прозорість алгоритмів тематичного відбору;
- чутливість до технологічних інновацій проти фінансової стабільності.

На основі синтезу проаналізованих підходів пропонується узагальнений підхід для формування фінансового індексу кібербезпеки, який включає такі етапи і може бути використаний у національній системі кібербезпеки:

- Визначення цільового призначення індексу (інвестиційний, аналітичний, регуляторний);
- Формування наборів активів або показників (публічні компанії, ADR/GDR, мінімальні вимоги до ліквідності);
- Тематична ідентифікація (частка доходів від кібербезпеки, продуктова спеціалізація, експертна класифікація);
- Фільтрація ризиків (капіталізаційні пороги, ESG-обмеження за потреби);
- Визначення ваг (ринкова або модифікована капіталізація з обмеженням концентрації);
- Ребалансування та перегляд складу з фіксованою періодичністю (не рідше 1 разу на рік);
- Публікація та прозорість методології для забезпечення відтворюваності результатів.

Аналіз доступних даних свідчить про обмежену можливість емпіричних досліджень, оскільки відкриті джерела забезпечують доступ до методології, складу індексів та агрегованих показників, однак історичні часові ряди значень індексів у більшості випадків є обмежено доступними або платними. Це унеможливлює повноцінне відтворення динаміки індексів та проведення кількісного кореляційного аналізу без використання ліцензованих фінансових баз даних (Bloomberg, Refinitiv, FactSet). Разом з тим, аналіз публічно доступних агрегованих даних свідчить про високу кореляцію індексів кібербезпеки, а також про відмінності у поведінці ESG-орієнтованих та чисто тематичних індексів у періоди підвищеної ринкової волатильності. Приклад доступних для аналізу індексів групи NASDAQ наведено на *Рис. 1*.

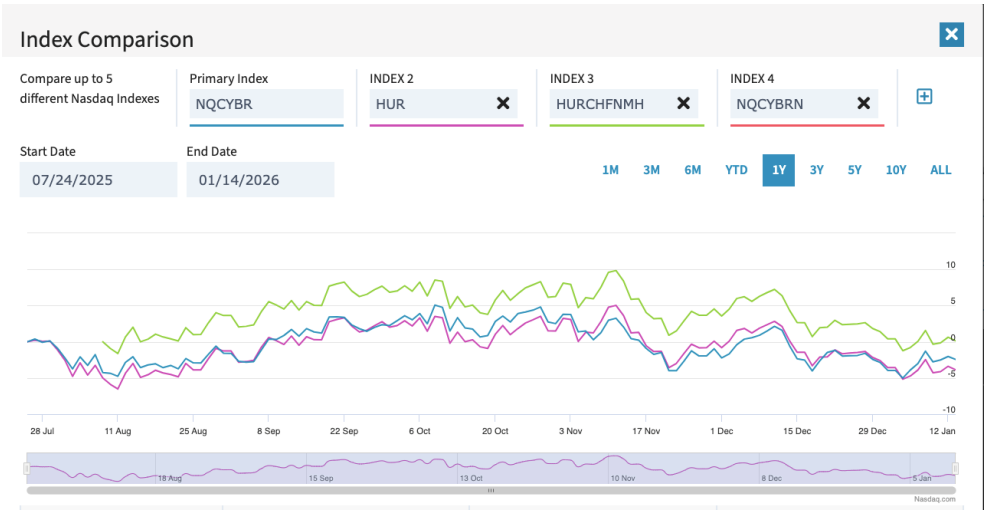

Рис. 1. Індекси групи NASDAQ
(24.07.2025-14.01.2026, взято з https://indexes.nasdaqomx.com/)

Синхронізована поведінка індексів свідчить про єдине джерело походження даних та використання однотипної методології їх формування.

Проведений аналіз свідчить про те, що фінансові (біржові) індекси кібербезпеки можуть виступати ефективним інструментом оцінки розвитку галузі та фінансових очікувань.

Сфери використання:

- у корпоративному управлінні (бенчмаркінг інвестицій у кіберзахист, управління масивами даних про учасників ринку для прийняття рішень, зокрема на ринку страхування);
- у наукових дослідженнях (аналіз зрілості ринку кібербезпеки та його інтеграції у глобальний ринок, кореляція між мережевими та економічними показниками);
- у державній політиці (індикатор інноваційного та технологічного розвитку).

Гібридна модель FSCI з мережевою складовою

Гібридна модель індексу кібербезпеки ґрунтується на припущенні, що фінансова оцінка кібербезпеки є відображенням як реального технічного стану цифрових активів, так і здатності організації управляти цими ризиками з економічної точки зору. Таким чином, модельний FSCI інтегрує мережеві показники, які фіксують фактичний рівень експозиції до кіберзагроз, та фінансово-управлінські показники, що характеризують стійкість, масштабованість і комерційну ефективність системи кібербезпеки.

Домени моделі:

- Мережево-операційний домен (Network & Exposure Domain, NED);
- Фінансово-стратегічний домен (Financial & Governance Domain, FGD).

Кожен домен формує окремий субіндекс, які разом утворюють інтегральний фінансовий індекс кібербезпеки.

Склад мережево-операційного домену (NED) (запропоновано у спрощеному вигляді Monitoring Network Index з [18]):

- мережевий трафік (DNS-запити та відповіді, BGP-з'єднання);
- наявність шкідливого або аномального трафіку (DDoS, brute force);
- експозиція відкритих сервісів (Open DNS, Open NTP, Open SNMP, Open SSDP, Open CHARGEN);
- ідентифікація компрометованих систем;
- цифрова ідентичність і репутація (IP/Domain Reputation, Brand Monitoring);
- активність (зловмисна активність) на кінцевих пристроях та IoT;
- показники атак (Attack Surface, Digital Footprint).

Ці показники мають переважно кількісну природу та оновлюються з високою частотою.

Склад фінансово-стратегічного домену (FGD) (запропоновано на основі аналізу та узагальнення показників FSCI з [4-17]):

- точність даних і прозорості процесів, інституційна довіра (Data accuracy, Process transparency);
- управління ризиками та інцидентами (Risk context, Issue management);
- інтеграція та масштабованість (Integration, Breadth of use case);
- стратегічний розвиток (Product roadmap, Go-to-market strategy);
- комерційна ефективність (Commercial strategy, Pricing innovation);
- екосистемна зрілість (Customers, Community support, API extensibility).

Ці показники можуть деталізуватися у залежності від ринкових умов та задач і мають низьку частоту оновлення, але вищу прогностичну цінність.

Зазначимо, що доменна структура FSIB в рамках гібридної моделі відповідає аналогічній структурі індексу кіберстрахування (зрілості кіберстрахування), запропонованого у [19].

Розрахунок індексу відбувається в рамках загального підходу для індексів кібербезпеки, викладеного у [1].

Запропонована модель може бути використана для формування біржових та тематичних біржових інвестиційних механізмів (зокрема, ETF), порівняльного аналізу компаній і секторів, оцінювання зрілості національної системи кібербезпеки в цілому, виявлення фінансових ризиків та проведення ринкових корекцій, пов'язаних із кіберінцидентами.

FSCI відображають агреговані ринкові очікування щодо вартості компаній у секторі кібербезпеки. Проте поведінка цих індексів є результатом взаємодії численних суб'єктів ринку (інвесторів, корпорацій, державних та міжнародних організацій). У такому середовищі з метою подальшого моделювання процесів можливо використовувати кооперативні ігрові моделі [20] (зокрема, теоретико-ігрові ресурсні кооперативні моделі [21] можуть моделювати не лише конфлікти, але й стратегічну кооперацію між агентами у створенні цінності). Ресурсами моделі в контексті кібербезпеки можуть бути: технологічні ноу-хау та інтелектуальна власність, людський капітал, спеціалізовані інфраструктурні рішення, інформаційні активи (наприклад, у задачі оптимізації ресурсів страхування або кіберстрахування). Однак класичні теоретико-ігрові рішення можуть бути непрактичними без адаптації для систем з великою кількістю агентів з розподілом за ролями.

З урахуванням наведених міркувань теоретико-ігрові кооперативні моделі можуть використовуватися для моделювання стратегічних взаємодій агентів, що впливають на поведінку фінансових індексів кібербезпеки за умов їх подальшої адаптації до реалій фінансових ринків, включно з визначенням релевантних характеристичних функцій і способів емпіричної валідації.

Висновки

У роботі розглянуті методологічні основи формування фінансових (біржових) індексів кібербезпеки, проаналізовано методології формування існуючих індексів та запропоновано гібридну модель фінансового індексу кібербезпеки з мережевою складовою. Запропоновано застосування окремих показників індексів у національній системі кібербезпеки, а також їх використання для збору та обробки даних кіберстатистики.

Проаналізовано можливість використання теоретико-ігрових ресурсних кооперативних моделей для прогнозування поведінки окремих фінансових індексів кібербезпеки, а також спільне використання фінансових індексів кібербезпеки разом з індексом кіберстрахування (зрілості кіберстрахування) у практичних задачах.

Отримані результати можна використовувати для оцінки стану корпоративних інформаційних активів (ресурсів) з метою оптимізації прийняття рішень.

СПИСОК ЛІТЕРАТУРИ

1. Худинцев, М.М., Жилін, А.В., & Давидюк, А.В. (2021). Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог). Київ: Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. ISBN 978-966-136-887-2. 240 с.
2. Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., & Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-031-46880-3_17
3. European Business Association. (2024). Український ринок кібербезпеки зріс у чотири рази за вісім років. https://eba.com.ua/ukrayinskyj-rynok-kiberbezpeky-zris-u-chotyry-razy-za-visim-rokiv/
4. Nasdaq OMX. (n.d.). NASDAQ OMX Cloud Computing Index (EMCLOUD): Index overview. https://indexes.nasdaqomx.com/Index/Overview/EMCLOUD
5. MSCI Inc. (n.d.). MSCI Cybersecurity Index methodology. https://www.msci.com/eqb/methodology/meth_docs/MSCI_CyberSecurity_Index_Methodology.pdf
6. Vontobel. (n.d.). Tracker certificate on cybersecurity thematic index (CH0292584718). https://markets.vontobel.com/en-ch/products/thematic/tracker-certificates/CH0292584718
7. Evolve ETFs. (2020). Evolve Cyber Security Index Fund (CYBR): Fact sheet (February 28, 2020). https://evolveetfs.com/wp-content/uploads/2020/03/CYBR-FactSheet-February-28-2020.pdf
8. Fair Isaac Corporation. (n.d.). FICO® score: How it works. https://www.myfico.com/products/fico-score-how-it-works
9. Foxberry Ltd. (n.d.). Cybersecurity & data privacy thematic index. https://www.foxberry.com/indices/thematics/cybersecurity_data_privacy_pr
10. Nasdaq OMX. (n.d.). NASDAQ Healthcare Index (HXR): Methodology. https://indexes.nasdaqomx.com/docs/Methodology_HXR.pdf
11. Singapore Exchange. (2020). iEdge–FactSet thematic indices: Index methodology (Version 2.2). https://api2.sgx.com/sites/default/files/2020-01/SGX%20Index%20Services_iEdge-FactSet%20Thematic%20Indices%20-%20Index%20Methodology_v2.2_20200117_1.pdf
12. INDXX. (n.d.). INDXX Cybersecurity Index. https://www.indxx.com/index/indxx-cybersecurity-index
13. S&P Dow Jones Indices. (n.d.). S&P Kensho™ Cyber Security Index. https://www.spglobal.com/spdji/en/indices/equity/sp-kensho-cyber-security-index/
14. Nasdaq OMX. (n.d.). NASDAQ Cybersecurity Index: Fact sheet (NQCYBRT). https://indexes.nasdaqomx.com/docs/FS_NQCYBRT.pdf
15. Nasdaq OMX. (n.d.). NASDAQ Cybersecurity Index: Methodology (NQCYBR). https://indexes.nasdaqomx.com/docs/Methodology_NQCYBR.pdf
16. Solactive AG. (n.d.). Solactive cybersecurity index: Fact sheet (DE000SLA3UE7). https://www.solactive.com/wp-content/uploads/solactiveip/en/Factsheet_DE000SLA3UE7.pdf
17. Solactive AG. (n.d.). Solactive cybersecurity index (DE000SLA3WC7). https://www.solactive.com/Indices/?index=DE000SLA3WC7
18. Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., & Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. https://doi.org/10.1007/978-3-031-46880-3_17
19. Худинцев, М.М., & Хоменко О.А. (2025). Інформаційні технології кіберстрахування. *Електрон. Моделювання*, *47*(6), 100-111. https://doi.org/10.15407/emodel.47.06

20. Branzei, R., Dimitrov, D., & Tijs, S. (2005). Models in cooperative game theory: Crisp, fuzzy, and multi-choice games (Lecture Notes in Economics and Mathematical Systems, Vol. 556). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-28509-1
21. Горда, С. Є. (2018). Методи ресурсного теоретико-ігрового аналізу процесів регіонального розвитку (Автореф. дис. на здобуття наукового ступеня кандидата технічних наук). Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України. https://itgip.org/wp-content/uploads/2019/01/a_regorda-1111.pdf

Стаття надійшла до редакції 23.08.2025 і прийнята до друку після рецензування 06.11.2025

REFERENCES

1. Khudyntsev, M.M., Zhylin, A.V., & Davydiuk, A.V. (2021). World Cybersecurity Indices: Overview and Formation Methods (Global Report / Catalog). Kyiv: International Cybersecurity University, G.E. Pukhov Institute for Modelling in Energy Engineering of the NAS of Ukraine. ISBN 978-966-136-887-2. [in Ukrainian].
2. Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., & Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-031-46880-3_17
3. European Business Association. (2024). Ukrainian cybersecurity market has grown fourfold in eight years. https://eba.com.ua/ukrayinskyj-rynok-kiberbezpeky-zris-u-chotyry-razy-za-visim-rokiv/
4. Nasdaq OMX. (n.d.). NASDAQ OMX Cloud Computing Index (EMCLOUD): Index overview. https://indexes.nasdaqomx.com/Index/Overview/EMCLOUD
5. MSCI Inc. (n.d.). MSCI Cybersecurity Index methodology. https://www.msci.com/eqb/methodology/meth_docs/MSCI_CyberSecurity_Index_Methodology.pdf
6. Vontobel. (n.d.). Tracker certificate on cybersecurity thematic index (CH0292584718). https://markets.vontobel.com/en-ch/products/thematic/tracker-certificates/CH0292584718
7. Evolve ETFs. (2020). Evolve Cyber Security Index Fund (CYBR): Fact sheet (February 28, 2020). https://evolveetfs.com/wp-content/uploads/2020/03/CYBR-FactSheet-February-28-2020.pdf
8. Fair Isaac Corporation. (n.d.). FICO® score: How it works. https://www.myfico.com/products/fico-score-how-it-works
9. Foxberry Ltd. (n.d.). Cybersecurity & data privacy thematic index. https://www.foxberry.com/indices/thematics/cybersecurity_data_privacy_pr
10. Nasdaq OMX. (n.d.). NASDAQ Healthcare Index (HXR): Methodology. https://indexes.nasdaqomx.com/docs/Methodology_HXR.pdf
11. Singapore Exchange. (2020). iEdge–FactSet thematic indices: Index methodology (Version 2.2). https://api2.sgx.com/sites/default/files/2020-01/SGX%20Index%20Services_iEdge-FactSet%20Thematic%20Indices%20-%20Index%20Methodology_v2.2_20200117_1.pdf
12. INDXX. (n.d.). INDXX Cybersecurity Index. https://www.indxx.com/index/indxx-cybersecurity-index
13. S&P Dow Jones Indices. (n.d.). S&P Kensho™ Cyber Security Index. https://www.spglobal.com/spdji/en/indices/equity/sp-kensho-cyber-security-index/
14. Nasdaq OMX. (n.d.). NASDAQ Cybersecurity Index: Fact sheet (NQCYBRT). https://indexes.nasdaqomx.com/docs/FS_NQCYBRT.pdf
15. Nasdaq OMX. (n.d.). NASDAQ Cybersecurity Index: Methodology (NQCYBR). https://indexes.nasdaqomx.com/docs/Methodology_NQCYBR.pdf

16. Solactive AG. (n.d.). Solactive cybersecurity index: Fact sheet (DE000SLA3UE7). https://www.solactive.com/wp-content/uploads/solactiveip/en/Factsheet_DE000SLA3UE7.pdf
17. Solactive AG. (n.d.). Solactive cybersecurity index (DE000SLA3WC7). https://www.solactive.com/Indices/?index=DE000SLA3WC7
18. Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., & Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. https://doi.org/10.1007/978-3-031-46880-3_17
19. Khudyntsev, M.M., & Khomenko, O.A. (2025). Information technologies of cyber insurance. *Electronic modeling*, *47*(6), 100-111. https://doi.org/10.15407/emodel.47.06
20. Branzei, R., Dimitrov, D., & Tijs, S. (2005). Models in cooperative game theory: Crisp, fuzzy, and multi-choice games (Lecture Notes in Economics and Mathematical Systems, Vol. 556). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-28509-1
21. Gorda, S. Ye. (2018). Methods of resource-theoretical game analysis of regional development processes (Author's dissertation for the degree of Candidate of Technical Sciences). Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine. https://itgip.org/wp-content/uploads/2019/01/a_regorda-1111.pdf [in Ukrainian].

The article was received 23.08.2025 and was accepted after revision 06.11.2025

Турчинов Олександр Валентинович
доктор економічних наук, професор, головний науковий співробітник Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: 03186, Україна, м. Київ, Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0009-0002-6014-2687 ***e-mail:*** oleksandr@turchynov.com

Худинцев Микола Миколайович
кандидат фізико-математичних наук, доцент, академік Академії зв'язку України, старший науковий співробітник Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: 03186, Україна, м. Київ, Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0000-0002-9324-6901 ***e-mail:*** nh@te.net.ua

Клименков Олег Анатолійович
кандидат технічних наук, старший науковий співробітник Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: 03186, Україна, м. Київ, Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0000-0001-7664-5225 ***e-mail:*** oleg@klymenkov.com

Хоменко Олексій Антонович
аспірант Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: 03186, Україна, м. Київ, Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0009-0007-4866-8244 ***e-mail:*** oleksii.khomenko.sci@gmail.com

Палажченко Ігор Леонідович
аспірант Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: 03186, Україна, м. Київ, Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0009-0000-0491-7068 ***e-mail:*** palazhchenko.ihor@gmail.com