УДК 004.7

Mykola Khudyntsev, Candidate of Physical and Mathematic Science, Associated Professor, The Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine
ORCID ID: https://orcid.org/0000-0002-9324-6901 ***e-mail:*** nh@te.net.ua

Oleksii Khomenko, postgraduate, The Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine
ORCID ID: https://orcid.org/0009-0007-4866-8244 ***e-mail:*** oleksii.khomenko.sci@gmail.com

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

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

METHODOLOGICAL BASIS OF CYBERINSURANCE RISK ASSESSMENT

Abstract. *The main objective of the study is to formulate methodological foundations for assessing cyber insurance risks. The work defines the main terms related to cyber insurance, systematizes and analyzes cyber insurance risks, presents objects (processes) that will be subject to automation in the future, and cyber insurance algorithms. The objectives of the study are to determine the foundations of the methodology for assessing cyber insurance risks and cyber insurance within the framework of the proposed cyber insurance model, which considers the basic maturity levels of the main categories of participants in the insurance market of Ukraine and can be used in practical business activities.*

The methodological framework includes a description of the procedure for assessing cyber insurance (cyber insurance maturity), which complies with the provisions of the International Standard ISO/IEC 27102:2019(E) Information Security Management – Guidelines for Cyber Insurance and the Regulations on the Organization of Measures to Ensure Information Security and Cyber Protection by Financial Service Providers, approved by the Resolution of the Board of the National Bank of Ukraine dated 09.12.2025 No. 143. The basis of the procedure is the assessment of the development and implementation of cyber risk management processes and information security risks, as well as measures to ensure information security and cyber protection, considering the peculiarities of the functioning of the information and communication systems of the financial service provider within the framework of a risk-based approach.

The paper proposes a hybrid model for assessing information security risks, cyber risks and cyber insurance maturity (RA&CIMM), criteria for determining risks and the level of IT maturity of the cyber insurance model, as well as the domain structure of the cyber insurance index (cyber insurance maturity).

The results obtained can be used for planning and implementing cyber insurance by financial service providers (insurance market participants), as well as for comparative analysis with other approaches and insurance models, as well as the domain structure of the cyber insurance index (cyber insurance maturity).

Keywords: *cyber insurance; information security; cyber risks; information security risks; cyber risks and cyber insurance maturity model.*

М.М. Худинцев, О.А. Хоменко, О.А. Клименков

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

МЕТОДОЛОГІЧНІ ОСНОВИ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРСТРАХУВАННЯ

Анотація. *Основною метою дослідження є формулювання методологічних основ оцінювання ризиків кіберстрахування. В роботі виконане визначення основних термінів, пов'язаних з кіберстрахуванням, систематизовані та проаналізовані ризики кіберстрахування, наведені об'єкти (процеси), які у подальшому підлягатимуть автоматизації, алгоритми кіберстрахування. Завдання дослідження полягають у визначенні основ методології оцінювання ризиків кіберстрахування та кіберстрахування в рамках запропонованої моделі кіберстрахування, яка враховує базові рівні зрілості основних категорій учасників страхового ринку України та може бути використана у практичній господарській діяльності.*

Методологічні основи включають опис процедури оцінювання кіберстрахування (зрілості кіберстрахування), які відповідають положенням Міжнародного стандарту ISO/IEC 27102:2019(E) Управління інформаційною безпекою – Вказівки щодо кіберстрахування та Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг, затвердженого Постановою Правління Національного банку України від 09.12.2025 р. № 143. Основу процедури складає оцінювання розробляння та запровадження процесів управління кіберризиками та ризиками інформаційної безпеки, а також заходів із забезпечення інформаційної безпеки та кіберзахисту з урахуванням особливостей функціонування інформаційно-комунікаційних систем надавача фінансових послуг в межах ризик-орієнтованого підходу.

У роботі запропоновано гібридну модель оцінювання ризиків інформаційної безпеки, кіберризиків та зрілості кіберстрахування (RA&CIMM), критерії визначення ризиків та рівня IT-зрілості кіберстрахування моделі, а також доменну структуру індексу кіберстрахування (зрілості кіберстрахування).

Отримані результати можна використовувати для планування та здійснення кіберстрахування надавачами фінансових послуг (учасниками ринку страхування), а також для порівняльного аналізу з іншими підходами та моделями страхування.

Ключові слова: *кіберстрахування; інформаційна безпека; кіберризики; ризики інформаційної безпеки; модель ризиків та зрілості кіберстрахування.*

https://doi.org/10.32347/2411-4049.2026.2.251-261

Вступ

Питання кіберстрахування, відповідного оцінювання ризиків інформаційної безпеки та кіберризиків є предметом постійної уваги та розвитку [1-5]. Автоматизація процесів страхування і кіберстрахування у світі є головним технічним трендом останніх 5-10 років [6, 7]. Питання ризиків інформаційної безпеки та кібербезпеки в своїх роботах протягом того самого часу досліджували Д.В. Габбард, Р. Сейєрсен, К.Дж. Годсон, Е. Вілер, Б. Біджіо, Ф. Ролі, Дж.Р.К. Нерс, Б. Шнайєр, М. Кері, Дж.Дж. Лі, О. Сантос, Л. Каргілл,

Р. Росс, К. Мітнік, Р. Андерсон. Проблеми кіберстрахування та пов'язані з ними проблеми оцінювання ризиків вивчали Ж. Вольф, Г.С. Буп, Дж. Ребгольц, Р. Рутан, С. Романоський, Р. Теланг, Р. Парізі, Д. Вудс, Т. Мур, М. Елінг, В. Шнелль, Л. Аблон, А. Кюн, Т. Джонс. Серед українських авторів за цією тематикою можна зазначити А. Задорожну, Н. Нагайчук, М. Дубину, Ю. Калайду, О. Новицьку, Б. Орловського, А. Шкирю, В. Ємельянова.

Нормативну основу оцінювання ризиків та кіберстрахування складають національний стандарт ДСТУ IEC/ISO 31010:2013 (IEC/ISO 31010:2009, IDT) «Керування ризиком – Методи загального оцінювання ризику» [8], Міжнародний стандарт ISO/IEC 27102:2019(E) «Управління інформаційною безпекою – Керівні принципи кіберстрахування» [9], Рамка сертифікації кібербезпеки ЄС. Регламент (ЄС) 2019/881 [10], Рамка управління ризиками кібербезпеки Національного інституту стандартів і технологій (NIST CSWP 29, 2022) [11], постанови Національного банку України [12-15].

Актуальні питання моніторингу та управління ризиками інформаційної безпеки, кіберризиками, страхування та кіберстрахування активно обговорюються у світовій науковій та бізнес спільнотах, кількість відповідних публікацій зростає надзвичайно високими темпами (див. огляди [16-18]).

Основні визначення та терміни

- **Кіберстрахування** – це механізм захисту бізнесу від фінансових втрат, пов'язаних з кібератаками та витоком даних (Федеральна торгова комісія США / FTC) [20]. Поліси можуть покривати витрати на юридичний захист, відновлення даних, компенсацію збитків клієнтам та штрафи від регуляторів.
- **Кіберстрахування** – це фінансовий інструмент для зменшення ризиків, пов'язаних з порушеннями безпеки даних та кібератаками, який сприяє підвищенню обізнаності компаній про ризики та їх мінімізацію (Європейське агентство з кібербезпеки / ENISA) [21].
- **Ризик-орієнтований підхід** – прийняття управлінських рішень щодо впровадження заходів з інформаційної безпеки та кіберзахисту на підставі аналізу порівняння поточних ризиків інформаційної безпеки і кіберризиків з прийнятними (Національний банк України / НБУ) [12].
- **Кіберризик** – ризик виникнення збитків та/або додаткових втрат внаслідок реалізації кіберзагроз щодо інформаційних ресурсів та/або інформаційної інфраструктури. Кіберризик є складовою операційного ризику (Національний банк України / НБУ) [12, 22].
- **Операційний ризик** – ризик того, що недоліки інформаційних систем або внутрішніх процесів, людські помилки, операційні збої (помилки чи затримки під час оброблення, перебої в роботі систем, кіберінциденти, недостатня пропускна спроможність), втрата або витік інформації, шахрайство або порушення в управлінні внаслідок зовнішніх подій призведуть до скорочення, погіршення або зупинення надання послуг (Національний банк України / НБУ) [22].

- **Ризик інформаційної безпеки** (складова операційного ризику) – імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах кредитної спілки, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, включаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик (Національний банк України / НБУ) [23].

Ризики інформаційної безпеки та кіберризики

- Несанкціонований доступ
- Витік конфіденційної інформації
- Фішинг (Phishing)
- Шкідливе програмне забезпечення (Malware)
- Атаки вимагачів (Ransomware)
- DDoS-атаки
- Вразливості програмного забезпечення
- Zero-day уразливості
- Внутрішні загрози (Insider Threats)
- Компрометація облікових записів
- Атаки на ланцюги постачання (Supply Chain Attacks)
- Помилки конфігурації
- Втрата доступності інформації
- Порушення цілісності даних
- Недостатній контроль доступу
- Ризики хмарних технологій
- Кіберризики критичної інфраструктури
- AI та LLM-ризики
- Репутаційні втрати
- Регуляторні ризики (Regulatory & Compliance Risks)

Модель оцінювання ризиків інформаційної безпеки, кіберризиків та зрілості кіберстрахування

Модель оцінювання ризиків інформаційної безпеки, кіберризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model / RA&CIMM) – це гібридна модель оцінювання ризиків інформаційної безпеки, кіберризиків, кіберстрахування (зрілості кіберстрахування) суб'єктів (учасників) ринку страхування та надавачами фінансових послуг[1].

Домени RA&CIMM:

- Експертна модель оцінювання ризиків інформаційної безпеки та кіберризиків
- Мережева модель оцінювання ризиків інформаційної безпеки та кіберризиків
- Модель оцінювання кіберстрахування (зрілості кіберстрахування)

[1] терміни «учасники ринку страхування» та «надавачі фінансових послуг» визначаються законодавством України

RA&CIMM базується на принципах системного підходу, ризик-орієнтованого управління та багаторівневої верифікації результатів. Основною метою моделі є визначення інтегрального індексу, що характеризує суб'єкта (організацію) або інформаційну (комунікаційну) систему в цілому, на основі сукупності часткових індикаторів (підіндексів), кожен з яких характеризує окремий домен моделі.

Індекс моделі I можна представити у наступному вигляді:

$$I = \sum_{l} I_l = \sum_{jl} \alpha_{jl} p_j d_l \ ,$$

де $p_j d_l$ визначають окремі внески (для окремих ризиків або показників зрілості), l – номер домену моделі d_l, перехресні вагові коефіцієнти α_{jl} визначаються для окремих внесків до підіндексів моделі I_l експертним методом. Зазначимо, що наведений перелік доменів d_l у загальному випадку може змінюватися.

Модель передбачає чотири послідовні рівні оцінювання, що забезпечують поступове підвищення точності та достовірності результатів:

- Самооцінювання (self-assessment)
- Зовнішнє оцінювання (external assessment)
- Експертна оцінка (expert review)
- Повторне оцінювання (re-assessment)

В рамках моделі розроблені та запропоновані оригінальні опитувальники [24-26], адаптовані під вимоги [9-12] та особливості моделі. Результати оцінювання складають основу відповідних підіндексів.

Початковий експертний профіль індексу моделі (з поясненнями) наведено у *Таблиці 1*.

Таблиця 1. Початковий експертний профіль індексу RA&CIMM

Основні підіндекси	Додаткові підіндекси	Початкове значення	Пояснення
Оцінювання ризиків (експертний)	Governance Risk	0,08	Характеризує якість управління кібербезпекою, наявність політик, розподіл відповідальності та участь керівництва
	Technical Vulnerability Risk	0,10	Оцінює технічні вразливості, швидкість патч-менеджменту та рівень захищеності інфраструктури
	Threat Exposure Risk	0,07	Визначає рівень зовнішнього впливу загроз та доступність організації для потенційного нападника
	Operational Resilience Risk	0,05	Характеризує резервування (backup, disaster recovery) та стійкість до інцидентів
	Human Factor Risk	0,05	Враховує рівень обізнаності персоналу, фішингові (fishing) вразливості та загрози від внутрішнього порушника (insider threats)

	Third-Party and Supply Chain Risk	0,05	Пов'язаний із ризиками постачальників та залежністю від зовнішніх сервісів
	Compliance Risk	0,05	Відображає відповідність нормативним вимогам
	Financial and Insurance	0,05	Оцінює очікувані збитки, страхове покриття та загальну можливість страхування
Оцінювання ризиків (мережевий)	Penetration testing	0,10	Оцінює рівень захищеності шляхом моделювання реальних кібератак та визначення можливості експлуатації вразливостей
	Vulnerability assessment	0.10	Відображає наявність, критичність і кількість технічних вразливостей у програмному забезпеченні, мережах та інфраструктурі
	OSINT-automatic	0,02	Оцінює рівень зовнішньої інформаційної експозиції за даними у відкритому доступі
	Attack surface management	0,03	Враховує масштаб, видимість та рівень захищеності зовнішньої цифрової поверхні
Оцінювання зрілості	Self-assessment	0,10	Використовує внутрішню оцінку на основі власного аналізу політик, процесів, контролів та ресурсів організації
	External assessment	0,10	Оцінює фактичний стан шляхом незалежної перевірки та аудиту зовнішніми експертами або спеціалізованими організаціями
	Re-assessment	0,05	Оцінює динаміку змін рівня ризику та ефективність впроваджених заходів захисту

Визначення вагових коефіцієнтів здійснювали за допомогою методу Analytic Hierarchy Process (AHP) [27]. Процедура передбачає формування експертної групи з подальшим формуванням матриці парних порівнянь та перевіркою узгодженості через коефіцієнт послідовності (consistency ratio).

Основні етапи оцінювання:

- ідентифікація (інвентаризація) активів
- ідентифікація загроз
- визначення вразливостей
- оцінювання ймовірності реалізації та впливу загроз
- оцінювання зрілості
- визначення базового ризику
- коригування ефективності засобів захисту
- інтеграція показників зрілості
- визначення індексу, загальне оцінювання.

Використання інформаційних технологій, засобів автоматизації у відповідних бізнес-процесах досліджено у [6, 7].

Критерії визначення ризиків інформаційної безпеки та кіберризиків (100 – максимальний ризик):

- 0–20 – дуже низький
- 21–40 – низький
- 41–60 – середній
- 61–80 – високий
- 81–100 – критичний.

Критерії визначення рівнів IT-зрілості кіберстрахування (100 – максимальний рівень):

- 0–20 – початковий (хаотичний)
- 21–40 – повторюваний
- 41–60 – встановлений
- 61–80 – керований
- 81–100 – оптимізований.

Відповідно до ризиків та рівнів IT-зрілості кіберстрахування формуються рекомендації щодо пріоритетності заходів реагування, розміру страхового покриття, рівня франшизи, обсягу інвестицій тощо.

Висновки

Розроблено методологічні основи оцінювання ризиків кіберстрахування, які базуються на ризик-орієнтованому підході та враховують положення стандарту ISO/IEC 27102:2019(E), а також національні нормативні вимоги щодо забезпечення інформаційної безпеки та кіберзахисту у фінансовому секторі України. Основу розробки складає алгоритм оцінювання рівня впровадження процесів управління кіберризиками, ризиками інформаційної безпеки та заходів кіберзахисту з урахуванням особливостей функціонування інформаційно-комунікаційних систем суб'єктів ринку страхування та фінансових послуг.

Запропонована гібридна модель оцінювання ризиків інформаційної безпеки, кіберризиків та зрілості кіберстрахування (RA&CIMM), яка поєднує ризиковий і maturity-підходи. У межах моделі визначено критерії оцінювання ризиків та рівнів IT-зрілості кіберстрахування, а також сформовано доменну структуру інтегрального індексу зрілості кіберстрахування. Це дозволяє здійснювати комплексне оцінювання стану кіберстрахування, визначати слабкі місця в системі управління ризиками та формувати обґрунтовані рекомендації щодо підвищення рівня кіберстійкості.

Результати роботи можуть бути використані у практичній діяльності надавачів фінансових послуг та учасників ринку страхування для планування, впровадження та вдосконалення процесів кіберстрахування. Запропонована модель також може бути застосована як інструмент порівняльного аналізу існуючих підходів і моделей кіберстрахування, а також як основа для подальшої автоматизації процедур оцінювання та прийняття рішень у сфері кіберстрахування.

СПИСОК ЛІТЕРАТУРИ

1. Munich Re. (2026, March 25). Cyber insurance: Risks and trends 2026. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2026.html
2. Silverfort. (2025). The new cyber insurance requirements: What to know & how to comply. https://www.silverfort.com/wp-content/uploads/2025/02/ebook-cyber-insurance-identity-security.pdf
3. Federation of European Risk Management Associations (FERMA). (2025, October 6). Demystifying cyber insurance: Today's trends & tomorrow's challenges. https://ferma.eu/wp-content/uploads/2025/10/Demystifying-Cyber-Insurance-todays-trends-tomorrows-challenges.pdf
4. American Academy of Actuaries. (2025, May). Reinsurance. https://www.actuary.org/wp-content/uploads/2025/05/6Reinsurance.pdf
5. Keyfactor. (2025). NIS2 directive solution brief. https://www.keyfactor.com/resources/nis2-directive-info/nis2-solution-brief
6. Худинцев, М. М., & Хоменко, О. А. (2026). Інформаційні технології кіберстрахування. *Електрон. Моделювання*, 48 (1), 33-50. ISSN 0204–3572. ISSN 0204–3572. https://doi.org/10.15407/emodel.48.01.033
7. Khudyntsev, M., & Khomenko, O. (2025). Automation of standardized cyber insurance processes. *Environmental Safety and Natural Resources*, 54(2), 143-153. https://doi.org/10.32347/2411-4049.2025.2.143-153
8. Міністерство економічного розвитку і торгівлі України. (2015). Керування ризиком. Методи загального оцінювання ризику (ДСТУ IEC/ISO 31010:2013). https://wiki.nazk.gov.ua/wp-content/uploads/2020/10/UA-dstu-31010.pdf
9. International Standard ISO/IEC 27102:2019(E) Information security management – Guidelines for cyber-insurance. First edition 2019-08.
10. EU Cybersecurity Certification Framework (Regulation (EU) 2019/881). https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
11. National Institute of Standards and Technology. (2022). *Framework for Cybersecurity Risk Management* (NIST CSWP 29). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
12. Національний банк України (2025). Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг, Постанова Правління НБУ № 143 (2025, 09 грудня). https://zakon.rada.gov.ua/laws/show/v0143500-25#Text
13. Національний банк України (2023). Про затвердження Положення про авторизацію надавачів фінансових послуг та умови здійснення ними діяльності з надання фінансових послуг, Постанова Правління НБУ № 199 (2023, 29 грудня). https://zakon.rada.gov.ua/laws/show/v0199500-23#Text
14. Національний банк України (2023). Про затвердження Положення про вимоги до системи управління страховика, Постанова Правління НБУ № 194 (2023, 27 грудня). https://zakon.rada.gov.ua/laws/show/v0194500-23#Text
15. Національний банк України (2023). Про затвердження Положення про застосування Національним банком України коригувальних заходів, заходів раннього втручання, заходів впливу у сфері державного регулювання діяльності на ринках небанківських фінансових послуг, Постанова Правління НБУ № 183 (2023, 25 грудня). https://zakon.rada.gov.ua/laws/show/v0183500-23#Text
16. Adriko, R., & Nurse, J.R. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review. *Inf. Comput. Secur., 32*, 691-710. https://kar.kent.ac.uk/105932/1/ICS-2024-CyberInsurance-Security-AN.pdf
17. McGregor, R., Reaiche, C., Boyle, S., & Zubielqui, G.C. (2023). Cyberspace and Personal Cyber Insurance: A Systematic Review. *Journal of Computer Information Systems, 64*, 157-171. https://www.semanticscholar.org/paper/Cyberspace-and-Personal-Cyber-Insurance%3A-A-Review-Mcgregor-Reaiche/adec9dbb542cec686ca77c49094355f215755b54

18. Nobanee, H., Alodat, A.Y., Dilshad, M.N., El Sayah, A., Alas'ad, S.N., Al Shalabi, B.O., Alsadi, S.F., Al Marri, N.M., & Fiza, F.K. (2023). Mapping cyber insurance: a taxonomical study using bibliometric visualization and systematic analysis. *Global Knowledge, Memory and Communication*. https://www.semanticscholar.org/paper/Mapping-cyber-insurance%3A-a-taxonomical-study-using-Nobanee-Alodat/43250d49df871cfdbf7024c2a03b2c1007c55ec9
19. 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.
20. Federal Trade Commission (FTC) (2024). Cyber insurance. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance
21. European Union Agency for Cybersecurity (ENISA) (2024). Cyber Insurance - Models and methods and the use of AI. https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai
22. Національний банк України (2024). Про затвердження Інструкції з оцінювання на відповідність міжнародним стандартам оверсайту суб'єктів, які виконують функції центрального депозитарію цінних паперів, центрального контрагента, торгового репозиторію та системи розрахунків у цінних паперах в Україні, Постанова Правління НБУ № 38 (2024, 5 квітня). https://zakon.rada.gov.ua/laws/show/v0038500-24/ed20240405#n35
23. Національний банк України (2024). Про затвердження Положення про вимоги до системи управління кредитною спілкою, Постанова Правління НБУ № 15 (2024, 02 лютого). https://zakon.rada.gov.ua/laws/show/v0015500-24/ed20240202#n63
24. Худинцев, М. М., & Хоменко, О. А. (2026). *Оцінювання рівня цифрової зрілості та кіберстрахування учасників страхового ринку України* [Questionnaire]. Google Forms. https://docs.google.com/forms/d/e/1FAIpQLSeg0pw-c4t2--OUvOA9fYxINCKHMNJ2exQACTv1zsZwLh-bQA/viewform?usp=publish-editor
25. Худинцев, М. М., & Хоменко О. А. (2026). *Оцінювання рівня цифрової зрілості страхувальників України* [Questionnaire]. Google Forms. https://docs.google.com/forms/d/e/1FAIpQLSeX_nBDb8fBtc73wbouZ-wCBZS5cwUF7Llxk3VKOy62Kjvzgg/viewform?usp=publish-editor
26. Khudyntsev, M. M., & Khomenko, O. A. (2026). *Assessment of the Digital Maturity and Cyber Insurance of Participants in the Global Insurance Market* [Questionnaire]. Google Forms. https://docs.google.com/forms/d/e/1FAIpQLSeE0Z3oQL4UtFho5DuatvWavPQNh78zL8C_hRi0DwZ22p7dtA/viewform?usp=publish-editor
27. Saaty, T. L. (2019). Теорія аналітичинх ієрархічних процесів. Частина 2.1. The National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". https://harvester.nas.gov.ua/Record/journaliasakpiua-article-175311/Description?sid=154879518

Стаття надійшла до редакції 27.02.2026, надійшла після рецензування 04.04.2026, прийнята 17.04.2026

REFERENCES

1. Munich Re. (2026, March 25). Cyber Insurance: Risks and trends 2026. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2026.html
2. Silverfort. (2025). The new cyber insurance requirements: What to know & how to comply. https://www.silverfort.com/wp-content/uploads/2025/02/ebook-cyber-insurance-identity-security.pdf
3. Federation of European Risk Management Associations (FERMA). (2025, October 6). Demystifying cyber insurance: Today's trends & tomorrow's challenges. https://ferma.eu/wp-content/uploads/2025/10/Demystifying-Cyber-Insurance-todays-trends-tomorrows-challenges.pdf

4. American Academy of Actuaries. (2025, May). Reinsurance. https://www.actuary.org/wp-content/uploads/2025/05/6Reinsurance.pdf
5. Keyfactor. (2025). NIS2 directive solution brief. https://www.keyfactor.com/resources/nis2-directive-info/nis2-solution-brief
6. Khudyntsev, M. M., & Khomenko, O. A. (2026). Information technologies of cyber insurance. *Electronic. Modeling*, 48 (1), 33-50. ISSN 0204–3572. ISSN 0204–3572. https://doi.org/10.15407/emodel.48.01.033
7. Khudyntsev, M., & Khomenko, O. (2025). Automation of standardized cyber insurance processes. *Environmental Safety and Natural Resources*, 54(2), 143-153. https://doi.org/10.32347/2411-4049.2025.2.143-153
8. Ministry of Economic Development and Trade of Ukraine. (2015). Risk Management. General Risk Assessment Methods (DSTU IEC/ISO 31010:2013). https://wiki.nazk.gov.ua/wp-content/uploads/2020/10/UA-dstu-31010.pdf
9. International Standard ISO/IEC 27102:2019(E) Information security management – Guidelines for cyber-insurance. First edition 2019-08.
10. EU Cybersecurity Certification Framework (Regulation (EU) 2019/881). https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
11. National Institute of Standards and Technology. (2022). Framework for Cybersecurity Risk Management (NIST CSWP 29). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
12. National Bank of Ukraine (2025). On approval of the Regulation on the organization of measures to ensure information security and cyber protection by financial service providers, Resolution of the NBU Board No. 143 (2025, December 09). https://zakon.rada.gov.ua/laws/show/v0143500-25#Text
13. National Bank of Ukraine (2023). On approval of the Regulation on the authorization of financial service providers and the conditions for their activities with provision of financial services, Resolution of the NBU Board No. 199 (2023, December 29). https://zakon.rada.gov.ua/laws/show/v0199500-23#Text
14. National Bank of Ukraine (2023). On approval of the Regulation on requirements for the insurer's management system, Resolution of the NBU Board No. 194 (2023, December 27). https://zakon.rada.gov.ua/laws/show/v0194500-23#Text
15. National Bank of Ukraine (2023). On approval of the Regulation on the application by the National Bank of Ukraine of corrective measures, early intervention measures, and influence measures in the field of state regulation of activities in the markets of non-banking financial services, Resolution of the NBU Board No. 183 (2023, December 25). https://zakon.rada.gov.ua/laws/show/v0183500-23#Text
16. Adriko, R., & Nurse, J. R. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic review. *Inf. Comput. Secur.*, 32, 691-710. https://kar.kent.ac.uk/105932/1/ICS-2024-CyberInsurance-Security-AN.pdf
17. McGregor, R., Reaiche, C., Boyle, S., & Zubielqui, G. C. (2023). Cyberspace and Personal Cyber Insurance: A Systematic Review. *Journal of Computer Information Systems*, 64, 157-171. https://www.semanticscholar.org/paper/Cyberspace-and-Personal-Cyber-Insurance%3A-A-Review-Mcgregor-Reaiche/adec9dbb542cec686ca77c49094355f215755b54
18. Nobanee, H., Alodat, A.Y., Dilshad, M.N., El Sayah, A., Alas'ad, S.N., Al Shalabi, B.O., Alsadi, S.F., Al Marri, N.M., & Fiza, F.K. (2023). Mapping cyber insurance: a taxonomical study using bibliometric visualization and systematic analysis. Global Knowledge, Memory and Communication. https://www.semanticscholar.org/paper/Mapping-cyber-insurance%3A-a-taxonomical-study-using-Nobanee-Alodat/43250d49df871cfdbf7024c2a03b2c1007c55ec9
19. Khudyntsev, M. M., Zhilin, A. V., & Davydyuk, A. V. (2021). World Cybersecurity Indices: Overview and Methods of Formation (Global Report / Catalog). Kyiv: International Cybersecurity University, Institute of Modeling Problems in Energy named after G. E. Pukhov NAS of Ukraine. ISBN 978-966-136-887-2. 240 p.
20. Federal Trade Commission (FTC) (2024). Cyber Insurance. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

21. European Union Agency for Cybersecurity (ENISA) (2024). Cyber Insurance - Models and methods and the use of AI. https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai
22. National Bank of Ukraine (2024). On approval of the Instructions for assessing compliance with international standards of oversight of entities performing the functions of a central securities depository, central counterparty, trade repository and securities settlement system in Ukraine, Resolution of the NBU Board No. 38 (2024, April 5). https://zakon.rada.gov.ua/laws/show/v0038500-24/ed20240405#n35
23. National Bank of Ukraine (2024). On approval of the Regulation on requirements for the credit union management system, Resolution of the NBU Board No. 15 (2024, February 02). https://zakon.rada.gov.ua/laws/show/v0015500-24/ed20240202#n63
24. Khudyntsev, M. M., & Khomenko O. A. (2026). Assessment of the level of digital maturity and cyber insurance of participants in the insurance market of Ukraine [Questionnaire]. Google Forms. https://docs.google.com/forms/d/e/1FAIpQLSeg0pw-c4t2--OUvOA9fYxINCKHMNJ2exQACTv1zsZwLh-bQA/viewform?usp=publish-editor
25. Khudyntsev, M. M., & Khomenko O. A. (2026). Assessment of the level of digital maturity of Ukrainian policyholders [Questionnaire]. Google Forms. https://docs.google.com/forms/d/e/1FAIpQLSeX_nBDb8fBtc73wbouZ-wCBZS5cwUF7Llxk3VKOy62Kjvzgg/viewform?usp=publish-editor
26. Khudyntsev, M. M., & Khomenko, O. A. (2026). Assessment of the Digital Maturity and Cyber Insurance of Participants in the Global Insurance Market [Questionnaire]. Google Forms. https://docs.google.com/forms/d/e/1FAIpQLSeE0Z3oQL4UtFho5DuatvWavPQNh78zL8C_hRi0DwZ22p7dtA/viewform?usp=publish-editor
27. Saaty, T. L. (2019). Theory of Analytic Hierarchical Processes. Part 2.1. The National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". https://harvester.nas.gov.ua/Record/journaliasakpiua-article-175311/Description?sid=154879518

The article was received 27.02.2026, received after revision 04.04.2026, accepted 17.04.2026

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

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

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