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

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

AUTOMATION OF STANDARDIZED CYBER INSURANCE PROCESSES

Abstract. *The study aims to develop a cyber insurance model that includes the main requirements of international regulatory documents and provides for the automation of individual processes of cyber insurance.*
The objectives of the study are to analyze existing standards, business processes of insurance of operational risks in cyberspace, means of automating insurance processes, forming a profile of cyber risks in the national cybersecurity system, critical information infrastructure, studying cyber insurance algorithms for their further automation, and substantiating the use of individual automation tools in practical activities.
The work contains a review of existing standards and processes of insurance of operational risks in cyberspace (cyber insurance) and an analysis of cyber insurance processes using information technologies. The state of the regulatory framework of cyber insurance in Ukraine is briefly analyzed. The cyber insurance processes provided for by the International Standard ISO / IEC 27102 Information Security Management – Guidelines for Cyber Insurance are studied in detail. Separate means of automating cyber insurance processes are also considered, and approaches to optimizing their use within the framework of a risk-based approach to the profile of risks in cyberspace (cyber risks) are proposed.
Analysis of cyber insurance and other preventive methods of reducing risks and the negative impact of threats in cyberspace indicates an unsatisfactory state of using such instruments in critical information infrastructure.
The work substantiates and proposes a systemized set of cyber insurance processes for effective automation of these processes and further practical application in the design tasks of relevant automated (information and communication) systems.
The results obtained can be used in cyber insurance scenarios and algorithms.
Keywords: *cyber insurance; information security; automation; cyber risks.*

М.М. Худинцев, О.А. Хоменко

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

АВТОМАТИЗАЦІЯ СТАНДАРТИЗОВАНИХ ПРОЦЕСІВ КІБЕРСТРАХУВАННЯ

Анотація. *Основною метою дослідження є розробка моделі кіберстрахування, яка враховує основні вимоги міжнародних нормативних документів та передбачає автоматизацію окремих процесів кіберстрахування.*

Завдання дослідження полягають в аналізі існуючих стандартів, процесів страхування операційних ризиків у кіберпросторі, засобів автоматизації процесів страхування, формуванні профілю кіберризиків у національній системі кібербезпеки, критичній інформаційній інфраструктурі, дослідженні алгоритмів кіберстрахування з метою їх подальшої автоматизації, обґрунтуванні застосування окремих засобів автоматизації в практичній діяльності.

Робота містить огляд існуючих стандартів та процесів страхування операційних ризиків у кіберпросторі (кіберстрахування), а також аналіз процесів кіберстрахування із застосуванням інформаційних технологій. Стисло проаналізовано стан нормативно-правової бази кіберстрахування в Україні. Детально досліджені процеси кіберстрахування, передбачені Міжнародним стандартом ISO / IEC 27102 Управління інформаційною безпекою – Вказівки щодо кіберстрахування. Також досліджені окремі засоби автоматизації процесів кіберстрахування, запропоновані підходи до оптимізації їх використання в рамках ризик-орієнтованого підходу для профілю ризиків у кіберпросторі (кіберризиків).

Аналіз застосування кіберстрахування, а також інших превентивних методів зменшення ризиків та негативного впливу загроз у кіберпросторі свідчить про незадовільний стан використання таких методів у критичній інформаційній інфраструктурі.

У роботі обґрунтовано та запропоновано систематизацію процесів кіберстрахування для ефективної автоматизації цих процесів та подальшого практичного застосування в задачах проєктування відповідних автоматизованих (інформаційно-комунікаційних) систем.

Отримані результати можна використовувати в алгоритмах кіберстрахування.

Ключові слова: *кіберстрахування; інформаційна безпека; автоматизація; кіберризики.*

https://doi.org/10.32347/2411-4049.2025.2.143-153

Вступ

Питання страхування операційних ризиків у кіберпросторі (кіберстрахування) активно обговорюються у науковій спільноті (див., наприклад, [1-5]). Але на відміну від нормативних, термінологічних та фінансово-економічних аспектів, проблема автоматизації процесів кіберстрахування (як і страхування) тільки починає вирішуватися. Питання управління страховими ризиками досліджувалося К. Вільямсом, С. Волосовичем, Х. Грюндингом, Л. Клапківом та ін., кіберризиками у страхуванні – такими дослідниками: О. Гудзь, Н. Нагайчук, Л. Селіверстова, A. Marotta, R. Böhme, A.G. Schwartz, S. Romanovsky, R.R. Wagner, Р. Пікус, М. Дубина та ін., але, як правило, лише з економічної точки зору.

Гостра потреба у створенні нормативного підґрунтя для страхування кіберризиків призвела до появи низки спеціалізованих стандартів у галузі страхування та інформаційної безпеки [8-17], основним серед яких є International Standard ISO/IEC 27102:2019(E) [8]. Основну увагу ці документи приділяють визначенню, пріоритезації та калькуляції кіберризиків та підвищенню ефективності страхування.

До основних нормативних документів, які діють у сфері страхування та кіберстрахування в Україні, належать Цивільний кодекс України (зі змінами), закони України «Про страхування» (2021), «Про фінансові послуги та фінансові компанії» (2021), Постанови Національного банку України «Про затвердження Положення про встановлення критеріїв, за якими визначається профіль ризику надавачів фінансових послуг, їх суспільна важливість, на підставі яких визначаються наглядові дії Національного банку України» (2023), «Про затвердження Положення про порядок обліку страховиком договорів, пов'язаних зі здійсненням діяльності із страхування, та вимоги до захисту інформації страховика» (2023), «Про затвердження Положення про характеристики та класифікаційні ознаки класів страхування, особливості здійснення діяльності зі страхування та укладання договорів за класами страхування» (2023). Аналіз ринку страхових послуг в Україні, страхових ризиків, інформаційних потоків, бізнес процесів страхування та кіберстрахування наведено в [18-21].

Актуальні питання моніторингу та управління кіберризиками, страхування та кіберстрахування активно обговорюються у світовій науковій та бізнес спільнотах, кількість відповідних публікацій зростає надзвичайно високими темпами (див. огляди [22-24]).

Водночас систематизація, алгоритмізація та автоматизація процесів страхування та кіберстрахування внаслідок їх складності та багатофакторності, що підтверджується численними аналітичними звітами у сфері страхування, залишається складною і одночасно затребуваною науково-практичною задачею, яка потребує розв’язання.

Автоматизація окремих сервісів страхування та кіберстрахування реалізована у інформаційних системах (платформах) управління ризиками, страховими подіями та документами, маркетинговими та статистичними даними великої кількості страхових компаній (що буде проаналізовано нижче).

Стандарти в сфері кіберстрахування

Найпоширеніші визначення або трактування кіберстрахування:

- Кіберстрахування – це механізм захисту бізнесу від фінансових втрат, пов’язаних з кібератаками та витоком даних (Федеральна торгова комісія США / FTC) [25]. 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) [26].
- Кіберстрахування є ключовим елементом стратегії кібербезпеки, який допомагає компенсувати збитки від атак та покращити загальний рівень стійкості компанії (Національний інститут стандартів і технологій США / NIST) [27].

До стандартів (у т.ч. фреймворків) в сфері кіберстрахування, зокрема, належать:

- ISO/IEC 27102:2019 – Information Security, Cybersecurity, and Privacy Protection – Guidelines for Cyber Insurance – стандарт ISO, який пропонує вказівки щодо структурування полісів кіберстрахування, включаючи оцінку ризиків і міркування щодо покриття полісів;
- EU Cybersecurity Certification Framework (Regulation (EU) 2019/881) – встановлює механізми сертифікації кібербезпеки для продуктів, послуг і процесів ІКТ, спрямованих на забезпечення стандартизованих рівнів забезпечення кібербезпеки в ЄС, який має вирішальне значення для оцінки кіберризиків та ризиків кіберстрахування;
- ENISA Cyber Insurance: Recent Advances, Good Practices, and Challenges (November 2016) – описані ключові аспекти кіберстрахування, у т.ч. обізнаність про кіберризики, регуляторний вплив (GDPR, Директива NIS, з подальшою імплементацією до NIS2), найкращі практики;
- NIST Cybersecurity Framework (CSF2) – рекомендації з керування ризиками кібербезпеки та їх зменшення для використання в полісах (договорах) кіберстрахування для оцінки стану безпеки організації;
- Issues Paper on Insurance Sector Operational Resilience (May 2023) – документ Цільової групи IAIS з операційної стійкості (ORTF) містить наглядові практики щодо кібервідмовостійкості (кіберрезильєнтності), аутсорсингу процесів IT та кібербезпеки, управління безперервністю бізнесу (безпосередньо не стосується кіберстрахування, але фактично описує ключові елементи андерайтингу);
- Cyber Essentials Certification та Cyber Liability Insurance [28] – система сертифікації основ кібербезпеки та кіберстрахування від Національного центру кібербезпеки Великої Британії NCSC та його офіційного партнера Міжнародної асоціації безпечного управління підприємствами IASME.

Аналіз стандартів та фреймворків кіберстрахування свідчить про:

- Використання підходів та моделей оцінки ризиків та управління такими ризиками;
- Застосування кіберризиків, операційних ризиків у кіберпросторі, фінансових ризиків, пов’язаних з ймовірністю втрати грошових коштів, неотриманням (недоотриманням) доходів (прибутку), іншими збитками та/або витратами, включаючи можливі збитки (витрати);
- Застосування опису та існуючих класифікацій кіберризиків та кіберінцидентів;
- Важливість кількісної оцінки безпеки та стійкості ланцюгів постачання, залучення постачальників до реагування на надзвичайні події (у т.ч. у кіберпросторі);
- Застосування прийнятих підходів та моделей до формулювань виключень з полісів кіберстрахування, обмеження сум покриття, оцінки ризиків андеррайтингу;
- Необхідність стандартизації процесів збору інформації, оцінка кіберризиків страхувальника, підтримки кіберстрахування за допомогою систем управління інформаційною безпекою, обміну інформацією про ризики та засоби контролю в екосистемі кіберстрахування.

Інформаційно-комунікаційні засоби кіберстрахування

Провідні страхові компанії активно використовують сучасні інформаційно-комунікаційні технології та інструменти для автоматизації процесів страхування та кіберстрахування. Опис окремих рішень наведено у *Таблиці 1*.

Таблиця 1. Інформаційно-комунікаційні засоби страхування та кіберстрахування

Company (resource) title	*Link*	*IC instruments*	*CIM**
Coalition	https://www.coalitioninc.com/	Active Insurance: - Cyber Insurance - Tech Errors & Omissions (EO) - Executive Risks - Miscellaneous Professional Liability Coalition Security: - Coalition Control - Managed Detection & Response (MDR) - Coalition Incident Response (CIR) - Coalition Security Awareness Training	+++
At-Bay	https://www.at-bay.com/	- Cyber risk calculator - Primary & Excess Appetite eForm Guide - Miscellaneous Professional Liability (MPL) Coverage Highlights eForm Guide - Managed Detection and Response (MDR) Service Desk - Broker Platform	+
Cowbell Cyber	https://cowbell.insure/	Adaptive Cyber Insurance (Cowbell Prime 100, 100 PRO, 250, PLUS, ONE) Adaptive Technology Errors & Omissions (Cowbell Prime Tech) Incident Response Plan (IPR) Template	+
Corvus Insurance	https://www.corvusinsurance.com/	Smart Cyber Insurance, Smart Tech EO (Appetite Guide, Application, Request Coverage Form) Expert incident response and claims management (eForm)	++
Beazley	https://www.beazley.com/	Cyber Customer Centre - Risk Management Webinars - Incident Preparation Room - Port scanning and monitoring - Free Phishing Test - IRP Review Broker Centre - API Trading - Cyber Risk Management Tools - Cyber Defences with Managed eXtended Detection and Response (MXDR)	+++

Chubb	https://www.chubb.com/	Individuals & Families Portal Businesses Portal Agents & Brokers Portal Payment Center Chubb Mobile App Chubb Cyber Incident Response Team Report a Claim eForm	++
AIG	https://www.aig.com/	- Cyber Highlight Sheet - AIG's Cyber Coverages - AIG's Cyber Underwriting Application - Sample Client Cyber Maturity Report	+
AXA XL	https://axaxl.com/	- XL GlobalClaim Customer Portal - Design Professional login portal Learning Management System (XLDP LMS)	+
CFC Underwriting	https://www.cfcunderwriting.com/	- Cyber insurance private enterprise application form - Ransomware calculator - CFC mobile app for cyber	++
Liberty Mutual Insurance	https://www.libertymutual.com/	Liberty Mutual app	–
Berkshire Hathaway Specialty Insurance	https://bhspecialty.com/	eAppicitionForms	–
Hiscox	https://www.hiscox.com/	- Hiscox General Liability - Hiscox Professional Liability - Hiscox Cyber Security - Hiscox Business Owner's Policies	+
Lloyd's of London	https://www.lloyds.com/	Member Modeller Software Lloyd’s Investment Platform London Market Introductory Test (LLMIT) Delegated Authority services (DAS) - Delegated Contract and Oversight Manager (DCOM) - Delegated Audit Manager (AiMS) - Coverholder Applications (Atlas) - Lineage Regulatory reporting - Market data collections - Core Market Returns (CMR) - Lloyd’s Direct Reporting (LDR) - SecureShare - Overseas Reporting Service (ORS) - Assisting issuance/print insurance documentation MOCHA/DOPRINT Placing business - Online business insurance Tool (Crystal) - Delegated Data Manager (DA SATS) - Quality Assurance Tool (QA Tool) - Risk Locator Tool (RL Tool) - Italian Web Tender Service - Faster Claims Payment	++++

Munich Re	https://www.munichre.com/	eAppicitionForms	–
Swiss Re	https://www.swissre.com/	Swiss Re Surety Client Portal Property Exposure Management Sustainability Compass Supply Chain Resilience	+
Zurich	https://www.zurich.com/	Cyber Resilience and Insurance Services - Cyber and Data Protection Training - Audit and Compliance - Penetration Testing (Ethical Hacking) - Cyber Toolbox - Crisis and Incident Management - Cyber Quantification My Zurich - Insurance Management Tools - Program Status Tracker - Program Structure Matrix - Policy & Claims - Certificates - Zurich Global Program Support (GPS) Tool - Risk Management Tools - Risk Engineering - Zurich Risk Advisor - Risk Insights - Zurich Risk Room - Zurich Connector API Solution	++++
The Hartford	https://www.thehartford.com/	Hartford Platform for Producers, Brokers, Partners & Providers Hartford Electronic Business Center (EBC) - EBC Agent Portal - Commercial Lines Customer Portal (CLCP)	++
NAS Insurance	https://www.nasinsurance.com/	N/D	N/D
Safe	https://safe.security/	SAFE One Platform - AI - Driven UX - SAFE X - SAFE Mobile App - SAFE Dashboard) - Cyber Singularity Platform - Cyber Risk Quantification - Control Prioritization & Rol - Cyber Insurance Planning - Materiality Risk Reporting - Emerging Risks - Third Party Cyber Risk Management - Open Analytics Engine - MITRE ATT&CS - FAIR - FAIR CAM - FAIR MAM - FAIR TAM	++++

		- Cyber Risk Cloud - First-Party Business Context - Third-Party Business Context - Threat Intel - Enterprise Security Data - Compliance and Questionnaire Data	
International Cybersecurity University	https:/icu-ng.org	Cyber Statistic Indicators - Suspicious Cyber Event Indicators - Network Cybersecurity Indices - Cybersecurity Indicators - Key Cyber Risk and Performance Indicators - ETSI Information Security Indicators - ISO27 Information Security Indicators - NIST Cybersecurity Indicators - Cybersecurity Integration Maturity Model Indicators - Public Cyber Statistics Indicators	

* Cyber Insurance Maturity

Автоматизація процесів кіберстрахування

Аналіз впроваджених у світовій практиці інформаційно-комунікаційних засобів страхування та кіберстрахування та нормативних підстав кіберстрахування дозволяє визначити основні специфічні процеси кіберстрахування (додатково до процесів страхування):

- оцінка кіберризиків (оцінка внутрішнього кіберризику, оцінка засобів контролю інформаційної безпеки, оцінка попередніх та поточних кіберзбитків);
- управління кіберризиками;
- типізація (категоризація) кіберінцидентів;
- управління наслідками кіберінцидентів (мінімізація шкідливого впливу, забезпечення механізмів фінансування для відновлення збитків, сприяння поверненню до нормального функціонування, підвищення стійкості страховика);
- управління інформаційною безпекою під час обміну даними з страховиком;
- управління полісом кіберстрахування, підтвердженнями, витратами на реагування на кіберінциденти та кіберстраховим покриттям;
- андеррайтинг кіберстрахування;
- збір інформації з інформаційних активів (ресурсів, баз даних, систем, систем управління інформаційною безпекою);
- виконання зобов’язань, пов’язаних з інформаційною безпекою (область застосування з СУІБ, політики інформаційної безпеки, оцінка ризиків інформаційної безпеки, декларація про застосування та оцінка ефективності КСЗІ або СУІБ, обробка ризиків інформаційної безпеки, цілі інформаційної безпеки, докази компетентності персоналу, результати оцінки та обробки ризиків інформаційної безпеки, підтвердження результатів моніторингу та вимірювань, докази програм аудиторських перевірок, їх результатів, результатів управлінського аналізу, невідповідностей, подальших вжитих дій, результатів коригувальних дій).

Для оцінки рівня автоматизації зазначених процесів пропонується використовувати показники зрілості кібербезпеки (домен кіберстрахування) та ввести у розгляд індикатор автоматизації процесів кіберстрахування. Цей індикатор залишається на початковому рівні навіть для провідних страхових компаній (див. *Таблицю 1*), в Україні кіберстрахування практичне відсутнє і показники кіберстрахування не враховуються у формуванні профілів кіберризиків.

Висновки

Проаналізовано існуючі стандарти кіберстрахування, характерні бізнес-процеси кіберстрахування, засоби автоматизації процесів страхування, формування профілів кіберризиків для кіберстрахування у критичній інформаційній інфраструктурі.

Детально досліджені процеси кіберстрахування, передбачені Міжнародним стандартом ISO / IEC 27102 Управління інформаційною безпекою – Вказівки щодо кіберстрахування. Також досліджені окремі інформаційно-комунікаційні засоби страхування та кіберстрахування, запропоновані підходи до оптимізації їх використання в рамках ризик-орієнтованого підходу для профілю ризиків у кіберпросторі (кіберризиків).

Запропонована модель кіберстрахування, яка враховує основні вимоги міжнародних нормативних документів та передбачає автоматизацію окремих процесів кіберстрахування.

Аналіз застосування превентивних методів зменшення кіберризиків у критичній інформаційній інфраструктурі свідчить про незадовільний стан використання таких методів.

Запропоновано систематизацію процесів кіберстрахування у відповідності до міжнародних галузевих стандартів з можливістю практичного застосування в задачах проєктування відповідних автоматизованих (інформаційно-комунікаційних) систем.

Отримані результати можна використовувати в алгоритмах страхування та кіберстрахування.

СПИСОК ЛІТЕРАТУРИ / REFERENCES

1. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. Comput. Sci. Rev., 24, 35-61. https://www.semanticscholar.org/paper/Cyber-insurance-survey-Marotta-Martinelli/ad6b9bb3ff08415901a0915ba4f1e5881fa3857e
2. Nebolsina, E. V. (2024). Prospects for the US Cyber Insurance Market in Response to New Challenges. Society: Politics, Economics, Law (in Ukrainian). [Небольсіна, Є. В. (2024). Перспективи ринку кіберстрахування США у відповідь на нові виклики. Общество: политика, экономика, право]. https://www.semanticscholar.org/paper/U.S.-Cyber-Insurance-Market-Outlook-in-Response-to-Nebolsina/3a52eb16d16b93874d80d7617f79c98c65336564
3. Rangu, C.M., Badea, L., Șcheau, M.C., Găbudeanu, L., Panait, I., & Radu, V. (2024). Cyber insurance risk analysis framework considerations. The Journal of Risk Finance. https://www.semanticscholar.org/paper/Cyber-insurance-risk-analysis-framework-Rangu-Badea/3128ad0b22be3684cb5a3aff7da34120475e67df
4. 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://www.semanticscholar.org/paper/Cybersecurity%2C-cyber-insurance-and-enterprises%3A-a-Adriko-Nurse/b0dff05f5f8746d38ade3fe07ca227545e8fcef0#citing-papers

5. Bace, B., Dubois, E., & Tatar, U. (2024). Resilience against Catastrophic Cyber Incidents: A Multistakeholder Analysis of Cyber Insurance. Electronics. https://www.semanticscholar.org/paper/Resilience-against-Catastrophic-Cyber-Incidents%3A-A-Bace-Dubois/9541205d5c607870f89eefd1e42181e6b44bc453
6. 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
7. Koshkin, D. (2023). Cyber risks: Prospective Control Instruments (using the example of Cyber Insurance). Artificial societies. https://www.semanticscholar.org/paper/Cyber-risks%3A-Prospective-Control-Instruments-(using-Koshkin/58bce94470d7ada09338f49f1a154a66d91edfc3
8. International Standard ISO/IEC 27102:2019(E) Information security management – Guidelines for cyber-insurance. First edition 2019-08.
9. European Union Agency for Network and Information Security (ENISA) (2016). Cyber Insurance: Recent Advances, Good Practices and Challenges, November 2016. https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges
10. European Insurance and Occupational Pensions Authority (EIOPA) (2019). Cyber Risk for Insurers–Challenges and Opportunities. https://www.eiopa.europa.eu/document/download/61701869-eab9-49c7-a9ec-14d0b810f755_en?filename=Cyber%20Risk%20for%20Insurers%20-%20Challenges%20and%20Opportunities.pdf
11. International Association of Insurance Supervisors (IAIS) (2020). Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development, December 2020. https://www.iais.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf
12. Privacy + Security Academy. (2021). Cyber liability insurance buying guide 2021. Privacy + Security Academy. https://www.privacysecurityacademy.com/wp-content/uploads/2024/05/Cyber-Liability-Insurance-Buying-Guide-2021.pdf
13. Prudential Regulation Authority (2016). Cyber insurance underwriting risk: Consultation Paper CP39/16 (November), Bank of England, London. https://www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf
14. Organisation for Economic Co-operation and Development (OECD). (2017). Enhancing the role of insurance in cyber risk management. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/12/enhancing-the-role-of-insurance-in-cyber-risk-management_g1g82a47/9789264282148-en.pdf
15. Professional Risk Underwriting Pty Ltd (2021). ProRisk Cyber & Privacy Liability Insurance Policy v04.21. https://www.prorisk.com.au/siteassets/documents/policy-wordings/prorisk-cyber-privacy-liability-insurance-policy-v04.21.pdf
16. Philadelphia Insurance Companies (2021). Cyber security liability policy form (Form 36-8835). https://www.phly.com/files/Cyber%20Security%20Liability%20Policy%20Form36-8835.pdf
17. Royal & Sun Alliance Insurance plc (2018). Cyber Risk Insurance Policy. https://static.rsagroup.com/rsa/commercial-insurance-products/cyber/cyber-risk-insurance-policy-wording.pdf
18. Klapkiv, Yu.M. (2020). Insurance Services Market: Conceptual Principles, Technical Innovations and Development Prospects: Monograph. Ternopil: TNEU (in Ukrainian). [Клапків Ю.М. Ринок страхових послуг: концептуальні засади, технічні інновації та перспективи розвитку: монографія. Тернопіль: ТНЕУ].
19. Lashchyk, I., Kondrat, I., Viblyy, P., & Bilets, V. (2020). Insurance market of Ukraine: current state and development prospects. *Galician Economic Bulletin*, 5 (66), 105–112 (in Ukrainian). [Лащик, І., Кондрат, І., Віблий, П., Білець, В. (2020). Страховий ринок України: сучасний стан та перспективи розвитку. *Галицький економічний вісник*, 5 (66), 105–112].

20. Marina, A.S., Petsenko, M.V. (2023). Insurance market of Ukraine in wartime. *Digital economy and economic security*, 5 (05), 44–51 (in Ukrainian). [Марина, А.С., Пеценко, М.В. (2023). Страховий ринок України в умовах війни. *Цифрова економіка та економічна безпека*, № 5 (05), 44–51]. https://doi.org/10.32782/dees.5-7
21. Korman, I., Semenda, O., & Makushok, O. (2024). Marketing research of the Ukrainian insurance market. *Kyiv Economic Scientific Journal*, (4), 119-126 (in Ukrainian). [Корман, І., Семенда, О., & Макушок, О. (2024). Маркетингове дослідження українського ринку страхових послуг. *Київський економічний науковий журнал*, (4), 119-126]. https://doi.org/10.32782/2786-765X/2024-4-17
22. 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
23. 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
24. Khudintsev, M.M., Zhilin, A.V., Davydyuk, A.V. (2021). World Cybersecurity Indices: Overview and Methods of Formation (Global Report / Catalog). Kyiv: International University of Cybersecurity, Institute of Modeling Problems in Energy named after G.E. Pukhov NAS of Ukraine (in Ukrainian). [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.
25. Federal Trade Commission (FTC) (2024). Cyber insurance. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance
26. 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
27. 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
28. National Cyber Security Centre (2025). *Cyber essentials resources*. https://www.ncsc.gov.uk/cyberessentials/resources#section_3

Стаття надійшла до редакції 12.02.2025 і прийнята до друку після рецензування 02.05.2025

The article was received 12.02.2025 and was accepted after revision 02.05.2025

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