НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

Кваліфікаційна наукова
праця на правах рукопису

Хоменко Олексій Антонович

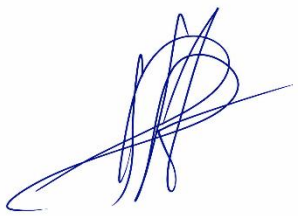
УДК 004.056:004.9

ДИСЕРТАЦІЯ

Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)

122 – «Комп'ютерні науки»
Галузь знань 12 – Інформаційні технології
Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів має посилання на відповідні джерела.



Олексій ХОМЕНКО

Науковий керівник:
Худинцев Микола Миколайович
кандидат фізико-математичних наук, доцент

Київ – 2026

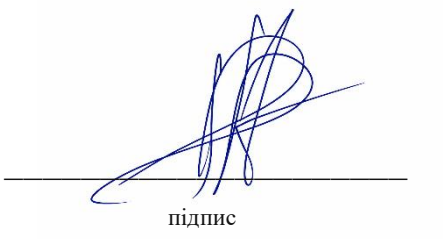
Декларація про використання інструментів ШІ

Під час підготовки рукопису дисертації автор використовував ChatGPT (OpenAI) як допоміжний інструмент для мовно-стилістичного редагування, перевірки логічної послідовності викладу, уніфікації термінології та технічного оформлення роботи

Наукову ідею, концепцію дослідження, методологічні положення, моделі, методи, розрахунки, формули, результати апробації, положення наукової новизни та висновки сформовано автором самостійно на основі проведених досліджень, власних наукових публікацій і професійного досвіду та обговорено з науковим керівником.

Інструменти штучного інтелекту не використовувалися як самостійне джерело наукової інформації, для створення або підміни результатів дослідження, генерування емпіричних даних чи формування неперевірених бібліографічних посилань.

Усі запропоновані за допомогою інструментів штучного інтелекту редакційні зміни перевірялися автором. Наукові положення, фактичні дані, термінологію, розрахунки, посилання на джерела та остаточний текст дисертації автор перевірив особисто і несе повну відповідальність за їх достовірність, обґрунтованість та академічну доброчесність.



підпис

Олексій ХОМЕНКО

АНОТАЦІЯ

Хоменко О. А. Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування). Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, Київ, 2026.

Дисертаційна робота присвячена розробленню комплексу взаємопов'язаних моделей, методів і алгоритмів структуризації, формалізації, інтеграції та оброблення різнорідних показників для оцінювання й індексації операційних ризиків у кіберпросторі. Розроблені моделі, методи й алгоритми формують методологічну та алгоритмічну основу інформаційної технології підтримки прийняття рішень у процесах кіберстрахування.

У вступі обґрунтовано актуальність теми дисертаційного дослідження, визначено його об'єкт і предмет, сформульовано мету та завдання дослідження, розкрито наукову новизну і практичне значення одержаних результатів.

У першому розділі проведено теоретичний аналіз підходів до оцінювання операційних ризиків у кіберпросторі та використання результатів такого оцінювання у процесах кіберстрахування. За результатами аналізу наукових праць, міжнародних стандартів, нормативних документів і сучасних підходів до управління кіберризиками встановлено, що, незважаючи на розвиток методів оцінювання кіберризиків, систем моніторингу інформаційної безпеки та засобів автоматизованого аналізу даних, недостатньо дослідженими залишаються питання формалізованого представлення, інтеграції та оброблення різнорідних показників операційних ризиків у кіберпросторі для підтримки прийняття рішень у процесах кіберстрахування.

Встановлено, що наявні підходи до оцінювання кіберризиків ґрунтуються на використанні різних систем показників, шкал оцінювання, критеріїв і методів

оброблення даних, що ускладнює порівняння одержаних результатів, їх інтеграцію та формування узагальненої оцінки операційних ризиків у кіберпросторі.

Обґрунтовано необхідність структуризації показників операційних ризиків у кіберпросторі, формування системи індикаторів та застосування індексного підходу до їх комплексного оцінювання. Такий підхід забезпечує формалізоване представлення й оброблення різнорідних даних із подальшим використанням одержаних результатів для інформаційної підтримки прийняття рішень у процесах кіберстрахування.

У другому розділі представлено методологічні засади індексного оцінювання стану кібербезпеки та операційних ризиків у кіберпросторі. Вихідним положенням є можливість використання індексів для зіставлення складних сукупностей, елементи яких безпосередньо не підлягають сумуванню. Такий підхід дає змогу формалізувати оброблення різнорідних показників кіберінцидентів, кібератак, кіберзагроз і заходів кіберзахисту шляхом їх структуризації та приведення до зіставного вигляду.

У межах розділу сформовано систему базисних параметрів для статистичного опису стану кібербезпеки та визначено послідовність їх використання під час формування індексних оцінок. Базисні параметри структуровано за групами, що характеризують кіберінциденти, кібератаки, кіберзагрози та заходи кіберзахисту. Запропонована система забезпечує можливість зіставлення показників із різними одиницями вимірювання, а також створює основу для накопичення та систематизації результатів спостережень.

Удосконалено підхід до структуризації показників оцінювання шляхом їх подання у вигляді доменів, піддоменів та індикаторів. Обґрунтовано використання групових індексів (доменних підіндексів) для агрегування споріднених показників і подальшого формування інтегральної оцінки стану об’єкта. Така структура забезпечує перехід від окремих показників до

формалізованого багаторівневого подання результатів оцінювання та створює основу для їх алгоритмічного оброблення.

Окрему увагу приділено базовим індикаторам кібербезпеки та процедурі формування профілю стану кібербезпеки об’єкта оцінювання. Запропонована послідовність передбачає формування структури індикаторів, проведення самооцінювання, визначення поточного і цільового профілів, накопичення результатів та їх подальший аналіз. Застосування запропонованої послідовності забезпечує уніфіковане оцінювання об’єктів та одержання структурованих даних для подальшого формування індексних оцінок.

У третьому розділі проведено аналіз і систематизацію процесів кіберстрахування з урахуванням положень ISO/IEC 27102:2019 та інформаційних технологій, що використовуються для їх підтримки. Визначено, що процеси кіберстрахування охоплюють збирання даних про об’єкт оцінювання, ідентифікацію й оцінювання кіберризиків, оцінювання стану кіберзахисту та формування результатів для інформаційної підтримки прийняття страхових рішень. Це зумовлює необхідність формалізації відповідних інформаційних процесів і визначення процесів, придатних до подальшої алгоритмізації та автоматизації.

На основі аналізу стандартизованих процесів кіберстрахування систематизовано основні етапи оцінювання та управління кіберризиками й визначено процеси, які можуть бути представлені як послідовності операцій із даними. Формалізація таких процесів дає змогу визначити вхідні дані, правила їх перевірки, операції оброблення та вихідні результати, що створює основу для алгоритмізації процесів кіберстрахування.

Систематизовано інформаційні технології та моделі, які застосовуються або можуть застосовуватися у страхуванні та кіберстрахуванні, зокрема технології електронного бізнесу, інтеграції інформаційних ресурсів, аналітики великих даних, штучного інтелекту, машинного навчання, блокчейн-технології та засоби моделювання. Розроблено трикомпонентну п’ятирівневу модель впровадження

інформаційних технологій у процеси кіберстрахування та сформовано підхід до оцінювання зрілості цих процесів.

Запропонований підхід ґрунтується на доменній декомпозиції показників і багаторівневому оцінюванні стану процесів кіберстрахування. Формування доменних оцінок та їх подальше агрегування забезпечують перехід від оцінювання окремих технологічних і організаційних характеристик до формування узагальненого профілю зрілості процесів кіберстрахування. Це створює основу для подальшого поєднання оцінювання кіберризиків і зрілості процесів кіберстрахування в межах єдиної моделі.

У четвертому розділі представлено модель оцінювання ризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model, RA&CIMM), яка поєднує оцінювання ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування. Модель ґрунтується на ризик-орієнтованому підході та охоплює процеси управління кіберризиками й ризиками інформаційної безпеки, заходи із забезпечення інформаційної безпеки та кіберзахисту, а також характеристики зрілості процесів кіберстрахування.

У межах RA&CIMM визначено чотири послідовні етапи оцінювання: самооцінювання, зовнішнє оцінювання, експертна перевірка та повторне оцінювання. Результати оцінювання за експертним і мережевим доменами та доменом зрілості кіберстрахування агрегуються у відповідні доменні підіндекси, на основі яких формується інтегральний індекс. Структуру та початкові вагові характеристики складових моделі сформовано в межах початкового авторського експертного профілю. Для подальшого формалізованого уточнення відносної пріоритетності критеріїв і вагових коефіцієнтів передбачено застосування експертних методів, зокрема методу аналізу ієрархій; наведені початкові ваги методом AHP не визначалися.

Розроблено інструментарій оцінювання у вигляді структурованих опитувальників, призначених для збирання вихідних даних за визначеними критеріями моделі. Одержані результати можуть використовуватися для

визначення поточного стану об’єкта оцінювання, формування профілю ризиків і зрілості, проведення порівняльного аналізу та підготовки інформації для підтримки прийняття рішень у процесах кіберстрахування. RA&CIMM створює основу для подальшої автоматизації процедур збирання, перевірки, структуризації, індексації та інтерпретації результатів оцінювання.

Поєднання індексного підходу, доменної структуризації показників і багаторівневої процедури оцінювання формує методологічну та алгоритмічну основу інформаційної технології оцінювання й індексації операційних ризиків у кіберпросторі та підготовки інформації для підтримки прийняття рішень у процесах кіберстрахування.

У п’ятому розділі проведено вибіркову апробацію окремих положень RA&CIMM, розроблених методів та алгоритмічних процедур оцінювання ризиків і зрілості кіберстрахування на даних страхувальників та учасників страхового ринку України. Для десяти страхувальників опрацьовано результати самооцінювання за структурованим опитувальником. До розрахунку композитного індексу цифрової зрілості (Composite Digital Maturity Index, CDMI) включено 23 оцінювані позиції опитувальника, об’єднані у три домени з ваговими коефіцієнтами 30 %, 40 % і 30 %. Середнє значення CDMI становило 41,41 бала, медіанне — 31,89 бала, а діапазон одержаних оцінок — від 12,62 до 84,84 бала. Для консервативної андеррайтингової інтерпретації результатів сформовано показник CDMI-UW (Composite Digital Maturity Index for Underwriting), у якому пропущені, невизначені та неоцінювані відповіді кодуються нульовим значенням. Критичні контрольні умови перевіряються окремо та використовуються разом із CDMI-UW під час попередньої інтерпретації результатів.

За результатами попередньої інтерпретації одержаних значень у межах пілотного оцінювання шість профілів визначено як такі, що потребують усунення критичних прогалин до подальшого страхового оцінювання; три профілі — як умовно прийнятні для подальшого оцінювання після усунення відповідних

прогалин; один профіль — як прийнятний для подальшого оцінювання з обов'язковою перевіркою підтверджувальних матеріалів.

Для страхових компаній проведено первинне та повторне самооцінювання з інтервалом близько трьох місяців. Кожне оцінювання охоплювало 188 питань, із яких 118 контрольних позицій з однаковими вагами використано для формування індексу за шкалою: «Так» — 100 балів, «Частково» — 50 балів, «Ні» — 0 балів.

Для Страхової компанії 1 значення індексу зросло з 54,66 до 62,29 бала, тобто на 7,63 бала; позитивні зміни зафіксовано за 18 контрольними позиціями. Для Страхової компанії 2 значення індексу зросло з 50,42 до 60,17 бала, тобто на 9,75 бала; позитивні зміни зафіксовано за 23 контрольними позиціями. В обох випадках за результатами повторного самооцінювання зафіксовано перехід від рівня «Встановлений» до рівня «Керований».

Окремі процедури оцінювання автоматизовано із застосуванням електронних опитувальників і структурованих розрахункових таблиць. Вони забезпечують збирання, перевірку, числове кодування, групування, зважування та агрегування відповідей, а також формування доменних оцінок, інтегральних індексів і рекомендацій.

Пілотна апробація продемонструвала можливість кількісного оброблення структурованих анкетних даних, відтворюваність розрахункових процедур і формування інформації для подальшого комплексного оцінювання у процесах кіберстрахування. Водночас одержані оцінки ґрунтуються на даних самооцінювання, тому результати пілотної апробації не можуть розглядатися як результати незалежного аудиту кібербезпеки або як повна валідація RA&CIMM.

Ключові слова: кіберстрахування, операційний ризик, кіберризик, ризик інформаційної безпеки, оцінювання ризиків, оброблення даних, індексація, індекс кібербезпеки, індекс зрілості кіберстрахування, інтегральний індекс, модель оцінювання ризиків та зрілості кіберстрахування, інформаційна технологія, підтримка прийняття рішень.

ANNOTATION

Khomenko O. A. Methodological Foundations for Risk Assessment and Indexing for the Insurance of Operational Risks in Cyberspace (Cyber Insurance). Qualifying scientific work submitted in manuscript form.

Dissertation submitted for the degree of Doctor of Philosophy in Specialty 122 “Computer Science”.

Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2026.

The dissertation is devoted to the development of a set of interrelated models, methods, and algorithms for structuring, formalizing, integrating, and processing heterogeneous indicators used to assess and index operational risks in cyberspace. The developed models, methods, and algorithms constitute the methodological and algorithmic foundation of information technology for decision support in cyber insurance processes.

The Introduction substantiates the relevance of the dissertation topic, defines the object and subject of the research, formulates its purpose and objectives, and presents the scientific novelty and practical significance of the results obtained.

The first chapter presents a theoretical analysis of approaches to assessing operational risks in cyberspace and using the results of such assessments in cyber insurance processes. The analysis of scientific publications, international standards, regulatory documents, and contemporary approaches to cyber risk management has established that, despite the development of cyber risk assessment methods, information security monitoring systems, and automated data analysis tools, the formalized representation, integration, and processing of heterogeneous indicators of operational risks in cyberspace for decision support in cyber insurance processes remain insufficiently studied.

It has been established that existing approaches to cyber risk assessment rely on different systems of indicators, assessment scales, criteria, and data processing methods,

which complicates the comparison and integration of the results obtained and the formation of a generalized assessment of operational risks in cyberspace.

The necessity of structuring indicators of operational risks in cyberspace, developing a system of indicators, and applying an index-based approach to their comprehensive assessment has been substantiated. This approach enables the formalized representation and processing of heterogeneous data, with the results subsequently used to provide information support for decision-making in cyber insurance processes.

The second chapter presents the methodological foundations of the index-based assessment of cybersecurity status and operational risks in cyberspace. The underlying premise is that indices can be used to compare complex sets whose elements cannot be directly added together. This approach makes it possible to formalize the processing of heterogeneous indicators of cyber incidents, cyberattacks, cyber threats, and cybersecurity measures by structuring them and bringing them into a comparable form.

Within the chapter, a system of basic parameters for the statistical description of cybersecurity status has been developed, and the sequence of their use in forming index-based assessments has been determined. The basic parameters are structured into groups characterizing cyber incidents, cyberattacks, cyber threats, and cybersecurity measures. The proposed system enables the comparison of indicators with different units of measurement and provides a basis for accumulating and systematizing observation results.

The approach to structuring assessment indicators has been improved by representing them as domains, subdomains, and indicators. The use of group indices (domain sub-indices) to aggregate related indicators and subsequently form an integral assessment of the object's status has been substantiated. This structure enables the transition from individual indicators to a formalized multilevel representation of assessment results and provides a basis for their algorithmic processing.

Particular attention is given to basic cybersecurity indicators and the procedure for constructing the cybersecurity status profile of the assessment object. The proposed

sequence includes developing the indicator structure, conducting a self-assessment, determining the current and target profiles, accumulating the results, and performing their subsequent analysis. Applying the proposed sequence ensures a consistent assessment of different objects and the production of structured data for the subsequent formation of index-based assessments.

The third chapter analyzes and systematizes cyber insurance processes with due regard to the provisions of ISO/IEC 27102:2019 and the information technologies used to support these processes. It has been determined that cyber insurance processes involve collecting data about the assessment object, identifying and assessing cyber risks, assessing the state of cybersecurity, and generating results to provide information support for insurance decision-making. This necessitates the formalization of the relevant information processes and the identification of processes suitable for subsequent algorithmization and automation.

Based on the analysis of standardized cyber insurance processes, the main stages of cyber risk assessment and management have been systematized, and the processes that can be represented as sequences of data operations have been identified. Formalizing these processes makes it possible to define input data, data validation rules, processing operations, and output results, thereby providing a basis for the algorithmization of cyber insurance processes.

Information technologies and models that are or may be applied in insurance and cyber insurance have been systematized, including e-business technologies, information resource integration, big data analytics, artificial intelligence, machine learning, blockchain technologies, and modelling tools. A three-component, five-level model for implementing information technologies in cyber insurance processes has been developed, and an approach to assessing the maturity of these processes has been formulated.

The proposed approach is based on the domain decomposition of indicators and the multilevel assessment of the state of cyber insurance processes. The formation and subsequent aggregation of domain assessments enable the transition from assessing

individual technological and organizational characteristics to forming a generalized maturity profile of cyber insurance processes. This provides a basis for subsequently combining cyber risk assessment and cyber insurance process maturity assessment within a unified model.

The fourth chapter presents the Risk Assessment & Cyber Insurance Maturity Model (RA&CIMM), which combines the assessment of information security risks, cyber risks, and the maturity of cyber insurance processes. The model is based on a risk-based approach and encompasses cyber risk and information security risk management processes, information security and cybersecurity measures, and the maturity characteristics of cyber insurance processes.

Within RA&CIMM, four sequential assessment stages have been defined: self-assessment, external assessment, expert review, and reassessment. The results obtained within the expert risk assessment domain, the network assessment domain, and the cyber insurance process maturity assessment domain are aggregated into the corresponding domain sub-indices, which are subsequently used to form the integral index. The structure and initial weighting characteristics of the model components were established within the initial author-developed expert profile of RA&CIMM. For their subsequent formalized refinement, the application of expert methods, including the Analytic Hierarchy Process (AHP), is envisaged. Within this dissertation, the initial weighting coefficients presented were not determined using AHP.

An assessment toolkit has been developed in the form of structured questionnaires designed to collect input data according to the defined model criteria. The results obtained can be used to determine the current state of the assessment object, construct its risk and maturity profile, conduct comparative analyses, and prepare information to support decision-making in cyber insurance processes. RA&CIMM provides a basis for the further automation of procedures for collecting, validating, structuring, indexing, and interpreting assessment results.

The combination of the index-based approach, the domain structuring of indicators, and the multilevel assessment procedure constitutes the methodological and

algorithmic foundation of information technology for assessing and indexing operational risks in cyberspace and preparing information to support decision-making in cyber insurance processes.

The fifth chapter presents the pilot testing of selected provisions of RA&CIMM and the developed methods and algorithmic procedures for assessing cyber insurance risks and maturity using data from policyholders and participants in the Ukrainian insurance market. The self-assessment results of ten policyholders were processed using a structured questionnaire. The calculation of the Composite Digital Maturity Index (CDMI) included 23 assessed questionnaire items grouped into three domains with weighting coefficients of 30%, 40%, and 30%. The mean CDMI value was 41.41 points, the median was 31.89 points, and the obtained values ranged from 12.62 to 84.84 points.

The Composite Digital Maturity Index for Underwriting (CDMI-UW) was developed as a conservative variant in which missing, indeterminate, and non-assessable responses are assigned to zero. Critical control conditions are assessed separately and are used together with CDMI-UW for the preliminary interpretation of results.

Based on the preliminary interpretation of the pilot assessment results, six profiles were identified as requiring the elimination of critical gaps before further insurance assessment; three profiles were considered conditionally acceptable for further assessment after the identified gaps had been addressed; and one profile was considered acceptable for further assessment subject to verification of supporting evidence.

Initial and repeat self-assessments were conducted for two insurance companies at an interval of approximately three months. Each assessment comprised 188 questions, of which 118 equally weighted control items were used to calculate the index according to the following scale: “Yes” — 100 points, “Partially” — 50 points, and “No” — 0 points.

For Insurance Company 1, the index increased from 54.66 to 62.29 points, representing an increase of 7.63 points; positive changes were recorded in 18 control items. For Insurance Company 2, the index increased from 50.42 to 60.17 points,

representing an increase of 9.75 points; positive changes were recorded in 23 control items. In both cases, the repeat self-assessment results indicated a transition from the “Established” maturity level to the “Managed” maturity level.

Certain assessment procedures were implemented using electronic questionnaires, structured calculation tables, and a research web application. These tools support the collection, storage, validation, numerical coding, grouping, weighting, and aggregation of responses, the calculation and presentation of domain and aggregated indicators, the generation of recommendations, and the comparison of results across successive assessment cycles. The spreadsheet prototype and the research web application should be regarded as experimental implementations of selected components of a future information system rather than as a completed software system.

The pilot testing demonstrated the feasibility of quantitative processing of structured questionnaire data, the reproducibility of the calculation procedures, and the generation of information for further comprehensive assessment in cyber insurance processes. At the same time, the assessments obtained are based on self-assessment data; therefore, the pilot testing results cannot be regarded as the results of an independent cybersecurity audit or as a full validation of RA&CIMM.

Keywords: cyber insurance; operational risk; cyber risk; information security risk; risk assessment; data processing; indexing; cybersecurity index; cyber insurance maturity index; integral index; cyber insurance risk and maturity assessment model; information technology; decision support.

Список опублікованих праць за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Худинцев М.М., Хоменко О.А. Автоматизація стандартизованих процесів кіберстрахування. Екологічна безпека та природокористування. 2025. Т. 54(2), с. 143–153. DOI: https://doi.org/10.32347/2411-4049.2025.2.143-153

2. Турчинов О.В., Худинцев М.М., Клименков О.А., Хоменко О.А., Палажченко І.Л. Мережева та економічна складова фінансових індексів кібербезпеки. Екологічна безпека та природокористування. 2025. Т. 56(4), с. 102–113. DOI: https://doi.org/10.32347/2411-4049.2025.4.102-113

3. Худинцев М.М., Хоменко О.А. Інформаційні технології кіберстрахування. Електронне моделювання. 2026. Т. 48(1), с. 33–50. DOI: https://doi.org/10.15407/emodel.48.01.033

4. Худинцев М.М., Хоменко О.А., Клименков О.А. Методологічні основи оцінювання ризиків кіберстрахування. Екологічна безпека та природокористування. 2026. Т. 58(2), с. 251–261. DOI: https://doi.org/10.32347/2411-4049.2026.2.251-261

5. Худинцев М.М., Хоменко О.А. Застосування індексів кібербезпеки для оцінки стану інформаційної безпеки об'єктів критичної інфраструктури в умовах військового часу. Актуальні проблеми управління інформаційною безпекою держави : збірник матеріалів XIV Всеукраїнської науково-практичної конференції. Національна академія Служби безпеки України. Інститут модернізації змісту освіти Міністерства освіти і науки України (м. Київ, 30 березня 2023 року). Київ, 2023. с. 341–344. URL: https://nasbu.edu.ua/uploads/p_57_92088934.pdf

6. Худинцев М.М., Хоменко О.А. Статистичний підхід для обробки даних та формування індексів про кіберінциденти, кібератаки, кіберзагрози та заходи протидії. Кібербезпека енергетики : матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ, 31 травня 2023 року). Київ, 2023. с.

100–104. URL: https://ipme.kiev.ua/wp-content/uploads/2023/06/1-Матеріали-КБЕ-2023.pdf

7. Худинцев М.М., Хоменко О.А. Методологічні засади індексу кіберрезильєнтності критичної інфраструктури. Резильєнтність критичної інфраструктури – 2023 : збірник матеріалів науково-практичної конференції. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ, 21 червня 2023 року). Київ, 2023. с. 52–55. URL: https://ipme.kiev.ua/wp-content/uploads/2023/06/Mat-Critical-Infrastructure-Resilience-–-2023.pdf

8. Худинцев М.М., Хоменко О.А. Тренди та інформаційні технології кіберстрахування. Кібербезпека енергетики : матеріали науково-практичної конференції. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ, 29 травня 2024 року). Київ, 2024. с. 56–57. URL: https://ipme.kiev.ua/wp-content/uploads/2024/06/Матеріали-КБЕ-2024.pdf

9. Худинцев М.М., Палажченко І.Л., Хоменко О.А. Оцінка стану кіберзахисту з використанням базових індикаторів кібербезпеки. Інформаційно-комунікаційні технології для перемоги та відновлення : матеріали XXIV Міжнародної науково-практичної конференції Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України (м. Київ, 11–12 листопада 2025 року). Київ, 2025. с. 61–63. URL: https://itgip.org/wp-content/uploads/2025/11/1_zbirka_2025_dlja-sajtu.pdf

10. Хоменко О.А., Худинцев М.М. Інформаційні технології страхування та кіберстрахування. Безпека енергетики в епоху цифрової трансформації : матеріали VII науково-практичної конференції. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ, 20 листопада 2025 року). Київ, 2025. с. 91–92. URL: https://ipme.kiev.ua/wp-content/uploads/2026/01/Матеріали-конференції-БЕЕЦТ-2025.pdf

ЗМІСТ

ВСТУП 21

РОЗДІЛ 1. ОГЛЯД ПРОБЛЕМИ ТА СТАНУ ДОСЛІДЖЕНЬ У СФЕРІ ОЦІНЮВАННЯ ОПЕРАЦІЙНИХ РИЗИКІВ У КІБЕРПРОСТОРІ 38

1.1. Розвиток кіберризиків та їх вплив на операційні процеси 38

1.2. Кіберризик як складова операційного ризику 41

1.3. Методи та моделі оцінювання кіберризиків і стану кібербезпеки 44

1.4. Індексні підходи до оцінювання стану кібербезпеки 50

1.5. Інформаційні технології оцінювання ризиків у процесах кіберстрахування ……. 56

Висновки до розділу 1 63

РОЗДІЛ 2. МОДЕЛІ ТА МЕТОДИ ІНДЕКСНОГО ОЦІНЮВАННЯ ОПЕРАЦІЙНИХ РИЗИКІВ У КІБЕРПРОСТОРІ 66

2.1. Загальні положення та концептуальна постановка задач дослідження 66

2.2. Система базисних параметрів оцінювання кіберінцидентів, кібератак, кіберзагроз та заходів кіберзахисту 71

2.3. Моделі оцінювання стану кіберзахисту з використанням базових індикаторів кібербезпеки 75

2.4. Доменна структура та індексне подання результатів оцінювання 80

2.5. Формування доменних індексів та інтегрального індексу шляхом агрегування показників 84

Висновки до розділу 2 87

РОЗДІЛ 3. МЕТОДИ ТА ІНФОРМАЦІЙНІ ПРОЦЕСИ ОЦІНЮВАННЯ РИЗИКІВ У КІБЕРСТРАХУВАННІ 90

3.1. Стандартизовані процеси кіберстрахування як об’єкти алгоритмізації та автоматизації 90

3.2. Формалізація інформаційних процесів оцінювання кіберризиків 107

3.3. Інформаційні технології страхування та кіберстрахування 114

3.4. Трикомпонентна п’ятирівнева модель впровадження інформаційних технологій у процеси кіберстрахування 126

3.5. Формування індексу зрілості кіберстрахування 138

Висновки до розділу 3 145

РОЗДІЛ 4. МОДЕЛЬ, МЕТОД ТА АЛГОРИТМ ОЦІНЮВАННЯ РИЗИКІВ І ЗРІЛОСТІ КІБЕРСТРАХУВАННЯ 148
4.1. Концептуальні засади та структура моделі RA&CIMM 148
4.2. Доменна структура та початковий експертний профіль RA&CIMM 156
4.3. Метод формування підіндексів та інтегрального індексу RA&CIMM 169
4.4. Алгоритм багаторівневого оцінювання ризиків та зрілості процесів кіберстрахування 175
4.5. Формування інформації для підтримки прийняття рішень у процесах кіберстрахування 182
Висновки до розділу 4 192
РОЗДІЛ 5. ВИБІРКОВЕ ОЦІНЮВАННЯ ЦИФРОВОЇ ЗРІЛОСТІ СТРАХУВАЛЬНИКІВ ТА ЗРІЛОСТІ ПРОЦЕСІВ КІБЕРСТРАХУВАННЯ СТРАХОВИХ КОМПАНІЙ 196
5.1. Вибіркове оцінювання цифрової зрілості страхувальників 197
5.2. Повторне самооцінювання зрілості процесів кіберстрахування страхових компаній 206
5.3. Автоматизація оброблення даних під час оцінювання цифрової зрілості та зрілості процесів кіберстрахування 210
5.4. Висновки та рекомендації щодо практичного використання результатів оцінювання 218
Висновки до розділу 5 225
ВИСНОВКИ 228
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 234
Додаток А. Методика пілотного розрахунку композитного індексу цифрової зрілості CDMI 257
Додаток Б. Акти про впровадження результатів дисертаційного дослідження 261

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AHP — метод аналізу ієрархій (Analytic Hierarchy Process);

AI — штучний інтелект (Artificial Intelligence);

API — інтерфейс прикладного програмування (Application Programming Interface);

C2M2 — модель зрілості спроможностей кібербезпеки (Cybersecurity Capability Maturity Model);

CDMI — композитний індекс цифрової зрілості (Composite Digital Maturity Index);

CDMI-UW — консервативний андеррайтинговий показник композитного індексу цифрової зрілості (Composite Digital Maturity Index for Underwriting);

CRI — індекс кіберрезильєнтності (Cyber Resilience Index);

EDR — система виявлення та реагування на загрози на кінцевих пристроях (Endpoint Detection and Response);

ENISA — Агентство Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity);

ETSI — Європейський інститут телекомунікаційних стандартів (European Telecommunications Standards Institute);

FAIR — факторний аналіз інформаційного ризику (Factor Analysis of Information Risk);

GDPR — Загальний регламент про захист даних (General Data Protection Regulation);

IAIS — Міжнародна асоціація органів страхового нагляду (International Association of Insurance Supervisors);

IEC — Міжнародна електротехнічна комісія (International Electrotechnical Commission);

ISO — Міжнародна організація зі стандартизації (International Organization for Standardization);

LCSI — локальний індекс кібербезпеки (Local Cybersecurity Index);

MDR — кероване виявлення та реагування (Managed Detection and Response);

MITRE ATT&CK — база знань MITRE про тактики й техніки зловмисників (Adversarial Tactics, Techniques, and Common Knowledge);

ML — машинне навчання (Machine Learning);

MXDR — кероване розширене виявлення та реагування (Managed Extended Detection and Response);

NCISS — національна система оцінювання кіберінцидентів (National Cyber Incident Scoring System);

NIST — Національний інститут стандартів і технологій США (National Institute of Standards and Technology);

NIST CSF — рамкова основа кібербезпеки NIST (NIST Cybersecurity Framework);

RA&CIMM — модель оцінювання ризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model);

SGMM — модель зрілості інтелектуальних електричних мереж (Smart Grid Maturity Model);

SIEM — система управління інформацією та подіями безпеки (Security Information and Event Management);

АСУ ТП — автоматизовані системи управління технологічними процесами;

ДІР — державні інформаційні ресурси;

ІБ — інформаційна безпека;

ІТ — інформаційні технології;

КБ — кібербезпека;

КЗ — кіберзахист;

КІ — критична інфраструктура;

КІІ — критична інформаційна інфраструктура;

НДДКР — науково-дослідні та дослідно-конструкторські роботи;

ПЕС КІ — паливно-енергетичний сектор критичної інфраструктури.

ВСТУП

Актуальність теми дисертаційного дослідження. Сучасний етап розвитку інформаційного суспільства характеризується зростанням залежності функціонування держави, суб'єктів господарювання та об'єктів критичної інфраструктури від інформаційно-комунікаційних систем, цифрових сервісів та інформаційних ресурсів. Цифровізація операційних процесів, поряд із розширенням можливостей оброблення та обміну даними, зумовлює збільшення кількості потенційних об'єктів кіберзагроз і посилення впливу кіберінцидентів на безперервність діяльності організацій [1, 2].

Наслідки реалізації кіберзагроз не обмежуються порушенням конфіденційності, цілісності та доступності інформації. Кіберінциденти можуть спричиняти зупинення операційних процесів, порушення функціонування інформаційних систем, втрату інформаційних активів, фінансові збитки та необхідність відновлення цифрової інфраструктури [2, 3]. За таких умов кіберризик набуває ознак операційного ризику, а його оцінювання потребує врахування сукупності технічних, інформаційних, організаційних та управлінських характеристик об'єкта оцінювання.

Особливістю операційних ризиків у кіберпросторі є динамічність середовища їх виникнення та різнорідність даних, що використовуються для оцінювання. Дані про кіберінциденти, кібератаки, кіберзагрози, вразливості та заходи кіберзахисту надходять із різних джерел, мають відмінну структуру, одиниці вимірювання та способи представлення [4, 5]. Безпосереднє зіставлення таких показників є ускладненим, що обмежує можливості формування комплексної оцінки стану кібербезпеки та операційних ризиків у кіберпросторі.

Одним із підходів до оброблення різнорідних показників є використання індексного методу. Застосування індексів дає змогу порівнювати складні сукупності, окремі елементи яких не підлягають безпосередньому сумуванню, та формувати узагальнені оцінки на основі системи показників та індикаторів [6–8]. У попередніх дослідженнях автора розглянуто використання індексів

кібербезпеки для оцінювання стану інформаційної безпеки об’єктів критичної інфраструктури, статистичний підхід до оброблення даних про кіберінциденти, кібератаки, кіберзагрози та заходи протидії, а також методологічні засади формування індексу кіберрезильєнтності критичної інфраструктури [9–11]. Зазначені результати сформували основу для подальшого дослідження методів структуризації, агрегування та індексації показників операційних ризиків у кіберпросторі.

Окремим напрямом управління наслідками реалізації операційних ризиків у кіберпросторі є кіберстрахування. Його використання передбачає збирання та оброблення даних про об’єкт страхування, ідентифікацію й оцінювання кіберризиків, оцінювання стану інформаційної безпеки та кіберзахисту, визначення характеристик ризику, а також формування інформації, необхідної для прийняття страхових рішень [5, 12]. Отже, процеси кіберстрахування безпосередньо пов’язані зі збиранням, представленням, обробленням та аналізом значних обсягів різнорідних даних і потребують застосування методів їх структуризації та формалізації.

Проведений аналіз стандартизованих процесів кіберстрахування показав, що окремі з них можуть бути представлені у вигляді послідовностей операцій зі збирання, перевірки, оброблення та аналізу даних і, відповідно, розглядатися як об’єкти подальшої алгоритмізації та автоматизації. У попередньому дослідженні систематизовано процеси страхування операційних ризиків у кіберпросторі, проаналізовано засоби автоматизації страхових процесів та обґрунтовано можливість використання одержаних результатів під час формування сценаріїв і алгоритмів кіберстрахування [13].

Нормативно-методичною основою формалізації процесів кіберстрахування обрано положення міжнародного стандарту ISO/IEC 27102:2019 «Управління інформаційною безпекою. Настанови щодо кіберстрахування» (Information security management — Guidelines for cyber-insurance), прийнятого в Україні як ДСТУ ISO/IEC 27102:2023 [12, 14]. У межах дослідження здійснено робочий

авторський переклад і змістову адаптацію окремих положень стандарту до термінології, нормативно-правових вимог та особливостей функціонування страхового ринку України. Положення ISO/IEC 27102:2019 використано як рекомендаційну основу для систематизації процесів кіберстрахування; стандарт не визначає вичерпного переліку або обов'язкової послідовності таких процесів.

Розвиток інформаційних технологій створює додаткові можливості для автоматизації окремих процесів страхування та кіберстрахування. До таких технологій належать засоби інтеграції інформаційних ресурсів, аналітики даних, штучного інтелекту, машинного навчання, блокчейн-технології, а також засоби інформаційної та кібербезпеки, які використовуються або можуть бути використані на різних етапах відповідних бізнес-процесів [15–18]. Проведена автором систематизація інформаційних технологій страхування та кіберстрахування дала змогу сформувати трикомпонентну п'ятирівневу модель їх впровадження у процеси кіберстрахування та визначити етапи її реалізації [19].

Водночас розвиток технологічних засобів автоматизації сам по собі не вирішує завдання оцінювання операційних ризиків у кіберпросторі. Наявні підходи ґрунтуються на різних системах показників, критеріях, шкалах і методах інтерпретації результатів [4, 5, 20]. Відсутність узгодженої структури показників ускладнює представлення та зіставлення результатів оцінювання, накопичення зіставних даних, їх інтеграцію та подальше використання для інформаційної підтримки прийняття рішень у процесах кіберстрахування.

Особливої актуальності зазначена проблема набуває в контексті розвитку кіберстрахування в Україні. Обмежене практичне поширення кіберстрахування, недостатність накопичених статистичних даних та відсутність усталених підходів до оцінювання кіберризиків ускладнюють застосування традиційних страхових механізмів оцінювання ризику [21, 22]. Проведений аналіз кіберстрахування та інших інструментів зниження ризиків і мінімізації негативних наслідків реалізації загроз у кіберпросторі свідчить про недостатній рівень їх використання, зокрема у сфері критичної інформаційної інфраструктури [13].

Міжнародні галузеві звіти засвідчують динамічну зміну умов кіберстрахування, вимог до страхувальників, підходів до андеррайтингу та оцінювання ефективності заходів кіберзахисту. Зазначені тенденції підтверджують необхідність використання структурованих і відтворюваних процедур збирання та оброблення даних про кіберризики під час прийняття страхових рішень [23–31].

Дослідження українського страхового ринку характеризують його розвиток в умовах цифрової трансформації, воєнного стану та зміни попиту на страхові послуги [32–34]. Водночас зростання українського ринку кібербезпеки свідчить про підвищення потреби організацій у засобах управління кіберризиками, але саме по собі не означає відповідного поширення кіберстрахування [35]. Це посилює потребу у формалізованих інструментах попереднього оцінювання кіберризиків і готовності потенційних страхувальників.

Додатковим чинником є функціонування інформаційних систем України в умовах воєнного стану. Зростання інтенсивності кіберзагроз, зміна їх характеру та посилення залежності операційних процесів від стійкості інформаційно-комунікаційних систем зумовлюють необхідність розвитку методів оцінювання поточного стану кібербезпеки [1, 2, 36]. Проведені автором дослідження щодо використання індексів кібербезпеки в умовах воєнного часу та формування індексу кіберрезильєнтності критичної інфраструктури підтвердили необхідність переходу від окремих статистичних показників до структурованих систем індикаторів та інтегральних оцінок [9, 11].

Подальший розвиток зазначеного напряму пов’язаний із поєднанням оцінювання ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування. У результаті проведених досліджень розроблено модель оцінювання ризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model, RA&CIMM), визначено її доменну структуру, критерії інтерпретації ризиків і зрілості процесів кіберстрахування, метод формування

доменних підіндексів та інтегрального індексу, а також алгоритм багаторівневого оцінювання [37].

Вибіркову пілотну апробацію окремих положень RA&CIMM, розроблених методів та алгоритмічних процедур проведено на масиві десяти анонімізованих анкет страхувальників і за результатами первинного та повторного самооцінювання страхових компаній, на основі яких сформовано чотири фактичні профілі. Одержані результати мають пілотний характер і ґрунтуються на даних самооцінювання, тому не можуть розглядатися як результати незалежного аудиту кібербезпеки або актуарне обґрунтування страхового тарифу.

Таким чином, аналіз сучасного стану досліджень свідчить про існування суперечності між необхідністю формалізованого представлення, інтеграції та алгоритмічного оброблення різнорідних даних для оцінювання операційних ризиків у кіберпросторі й підтримки прийняття рішень у процесах кіберстрахування та відсутністю цілісного комплексу взаємопов'язаних моделей, методів і алгоритмів, що забезпечують виконання зазначених інформаційних процесів.

Вирішення зазначеної суперечності потребує розроблення комплексу взаємопов'язаних моделей, методів і алгоритмів структуризації, формалізації, інтеграції та оброблення різнорідних показників для оцінювання й індексації операційних ризиків у кіберпросторі та підтримки прийняття рішень у процесах кіберстрахування. Зазначений комплекс має формувати методологічну та алгоритмічну основу відповідної інформаційної технології.

Отже, актуальність теми дисертаційного дослідження визначається необхідністю розроблення комплексу взаємопов'язаних моделей, методів і алгоритмів, що забезпечують структуризацію, формалізацію, інтеграцію та оброблення різнорідних показників для оцінювання й індексації операційних ризиків у кіберпросторі, а також формують методологічну та алгоритмічну основу інформаційної технології підтримки прийняття рішень у процесах кіберстрахування.

Мета і завдання дослідження. Метою дисертаційної роботи є розроблення комплексу взаємопов'язаних моделей, методів і алгоритмів, що забезпечують структуризацію, формалізацію, інтеграцію та оброблення різнорідних показників для підтримки прийняття рішень у процесах оцінювання та індексації операційних ризиків у кіберпросторі з метою їх страхування (кіберстрахування).

Для досягнення поставленої мети необхідно вирішити такі наукові та прикладні завдання:

1) виконати аналітичний огляд сучасних підходів, моделей і методів оцінювання кіберризиків та стану кібербезпеки, дослідити наявні індексні підходи й визначити обмеження їх використання для формалізованого представлення, оброблення та комплексного оцінювання операційних ризиків у кіберпросторі;

2) розвинути методологічні засади індексного оцінювання стану кібербезпеки шляхом формування системи базисних параметрів для формалізованого представлення та статистичного опису даних про кіберінциденти, кібератаки, кіберзагрози й заходи кіберзахисту;

3) розробити модель структуризації різнорідних показників операційних ризиків у кіберпросторі на основі їх доменної декомпозиції та подання у вигляді системи доменів, піддоменів та індикаторів;

4) обґрунтувати підхід до формування піддоменних і доменних індексів та інтегрального індексу, що охоплює кодування і нормування вхідних даних, формування початкового експертного профілю вагових характеристик, можливість їх подальшого формалізованого уточнення та агрегування різнорідних показників операційних ризиків у кіберпросторі;

5) формалізувати стандартизовані процеси кіберстрахування шляхом визначення їхніх вхідних даних, правил перевірки, операцій оброблення та вихідних результатів, виокремити інформаційні процеси, придатні до алгоритмізації й автоматизації, а також систематизувати інформаційні технології страхування та кіберстрахування;

6) розробити модель оцінювання ризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model, RA&CIMM), що поєднує оцінювання ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування;

7) розробити метод формування доменних підіндексів та інтегрального індексу RA&CIMM на основі багаторівневої процедури оцінювання, початкового експертного профілю вагових характеристик і процедури їх подальшого формалізованого уточнення;

8) розробити алгоритм багаторівневого оцінювання ризиків та зрілості процесів кіберстрахування і на його основі сформувати методологічну та алгоритмічну основу інформаційної технології підтримки прийняття рішень;

9) провести пілотну апробацію окремих методичних та алгоритмічних положень RA&CIMM на фактичних даних самооцінювання страхувальників і страхових компаній, оцінити відтворюваність розрахунків, чутливість результатів та можливість формування рекомендацій.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано в межах науково-дослідних робіт, пов'язаних із розробленням концептуальних засад, моделей і методів оцінювання стану кібербезпеки та рівня захищеності інформаційних активів і ресурсів суб'єктів забезпечення кібербезпеки України.

Дослідження виконано в межах науково-дослідної роботи «Розробка концептуальних засад і науково-методичної бази оцінки стану кібербезпеки та рівня захищеності інформаційних активів та ресурсів суб'єктів забезпечення кібербезпеки України» (реєстраційна картка НДДКР № 0121U112396 від 29.07.2021), що виконувалася Громадською організацією «Міжнародний університет кібербезпеки» у 2021–2024 роках [38].

У межах зазначеної науково-дослідної роботи досліджувалися питання формування систем показників та індикаторів, застосування індексного підходу

до оцінювання стану кібербезпеки, а також оцінювання рівня захищеності інформаційних активів і ресурсів.

Окремі результати дисертаційного дослідження пов'язані з виконанням науково-дослідної роботи «Обґрунтування організаційно-правових засад кібероборони України», шифр «Юпітер-КВ» (реєстраційна картка НДДКР № 012U000003Д), що виконувалася у 2024–2025 роках на замовлення Міністерства оборони України, співвиконавцем якої була Громадська організація «Міжнародний університет кібербезпеки».

Тематика дисертації охоплює розроблення моделей, методів та алгоритмів збирання, представлення, оброблення й аналізу даних для підтримки прийняття рішень. У дисертаційній роботі результати зазначених науково-дослідних робіт систематизовано та розвинуто шляхом розроблення комплексу взаємопов'язаних моделей, методів і алгоритмів структуризації, формалізації, інтеграції та оброблення різнорідних показників для оцінювання й індексації операційних ризиків у кіберпросторі. Одержані результати формують методологічну та алгоритмічну основу інформаційної технології підтримки прийняття рішень у процесах кіберстрахування.

Об'єктом дослідження є процеси збирання, представлення, оброблення, зберігання, передавання, аналізу та доступу до даних в інформаційних і комп'ютерних системах під час оцінювання та індексації операційних ризиків у кіберпросторі.

Предметом дослідження є моделі, методи та алгоритми збирання, структуризації, оброблення й аналізу даних в інформаційних і комп'ютерних системах для підтримки прийняття рішень у процесах кіберстрахування.

Методи дослідження. У роботі використано загальнонаукові та спеціалізовані методи дослідження. Методи системного аналізу використано для дослідження процесів оцінювання операційних ризиків у кіберпросторі та визначення взаємозв'язків між показниками кіберризиків, стану кібербезпеки і процесами кіберстрахування. Методи порівняльного аналізу та класифікації

застосовано для дослідження наявних індексів кібербезпеки, моделей оцінювання стану кіберзахисту, стандартизованих процесів та інформаційних технологій кіберстрахування.

Вибір доменного та індексного підходів ґрунтується також на результатах аналізу міжнародних моделей оцінювання зрілості кібербезпеки, зокрема C2M2 Міністерства енергетики США, практичний інструментарій якої забезпечує структуроване самооцінювання, формування профілів зрілості, виявлення прогалин і повторне оцінювання стану організації [39, 40].

Методи статистичного аналізу та індексний метод використано для оброблення і систематизації даних про кіберінциденти, кібератаки, кіберзагрози та заходи кіберзахисту, формування системи базисних параметрів та індексних оцінок. Методи багатокритеріального й експертного оцінювання застосовано для формування структури критеріїв та індикаторів оцінювання ризиків і зрілості процесів кіберстрахування. Метод аналізу ієрархій (Analytic Hierarchy Process, AHP) розглянуто як засіб подальшого формалізованого уточнення відносної пріоритетності критеріїв і вагових коефіцієнтів.

Методи формалізації, структурного моделювання, агрегування даних та алгоритмізації застосовано для розроблення моделей і методів структуризації різнорідних показників, формування доменних підіндексів та інтегрального індексу, а також побудови методологічної й алгоритмічної основи інформаційної технології підтримки прийняття рішень.

Для пілотної апробації окремих положень RA&CIMM використано методи анкетування та структурованого самооцінювання, процедури кодування і нормування відповідей, методи контролю якості даних, зваженого агрегування й описової статистики, аналізу чутливості та рангового кореляційного аналізу з використанням коефіцієнта Спірмена. Метод повторного порівняльного оцінювання застосовано для дослідження змін рівня ризиків і зрілості процесів кіберстрахування страхових компаній за результатами первинного та повторного самооцінювання.

Наукова новизна одержаних результатів. У дисертації розроблено та розвинуто методологічні основи оцінювання й індексації операційних ризиків у кіберпросторі для їх страхування (кіберстрахування), представлені комплексом взаємопов'язаних моделей, методів і алгоритмів структуризації, формалізації, інтеграції та оброблення різнорідних показників для інформаційної підтримки прийняття рішень у процесах кіберстрахування.

Вперше:

- розроблено модель оцінювання ризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model, RA&CIMM), яка, на відміну від підходів, що передбачають відокремлене оцінювання кіберризиків, стану інформаційної безпеки або зрілості відповідних процесів, поєднує їх у єдиній доменній структурі на основі ризик-орієнтованого підходу та багаторівневої процедури оцінювання, що забезпечує інтегроване представлення результатів оцінювання ризиків і зрілості процесів кіберстрахування для інформаційної підтримки прийняття страхових рішень;
- розроблено метод формування доменних підіндексів та інтегрального індексу оцінювання ризиків і зрілості кіберстрахування, який ґрунтується на структуруванні показників за доменами й піддоменами, нормуванні одержаних оцінок, застосуванні початкового експертного профілю вагових характеристик, можливості їх подальшого формалізованого уточнення та зваженому агрегуванні результатів, що забезпечує формування кількісного профілю ризиків і зрілості об'єкта оцінювання;
- розроблено алгоритм багаторівневого оцінювання ризиків та зрілості кіберстрахування, який встановлює послідовність збирання і перевірки вхідних даних, самооцінювання, зовнішнього оцінювання, експертної перевірки, збирання й оброблення технічних показників мережевого домену, формування доменних підіндексів та інтегрального індексу, інтерпретації результатів, формування рекомендацій і повторного оцінювання, що забезпечує

простежуваність перетворення первинних даних на інформацію для підтримки прийняття страхових рішень.

Удосконалено:

- методологічні засади індексного оцінювання стану кібербезпеки та операційних ризиків у кіберпросторі, які відрізняються систематизацією різнорідних показників кіберінцидентів, кібератак, кіберзагроз і заходів кіберзахисту, формуванням системи базисних параметрів для їх формалізованого представлення та статистичного опису, а також подальшим групуванням і агрегуванням показників для побудови індексних оцінок;
- підхід до структуризації показників оцінювання кіберризиків, який відрізняється формалізованим поданням множини різнорідних показників у вигляді ієрархічної системи доменів, піддоменів та індикаторів із формуванням відповідних доменних оцінок, що забезпечує алгоритмічне оброблення, агрегування та інтегроване представлення результатів оцінювання.

Набули подальшого розвитку:

- підходи до формалізації та автоматизації процесів кіберстрахування на основі положень ISO/IEC 27102:2019 шляхом їх систематизації, представлення як послідовностей операцій зі збирання, перевірки, структуризації, оброблення й аналізу даних, визначення інформаційних входів і вихідних результатів, а також формування сценаріїв та алгоритмів оцінювання ризиків і зрілості процесів кіберстрахування;
- підходи до оцінювання зрілості процесів кіберстрахування шляхом урахування рівня розвитку та впровадження процесів управління кіберризиками й ризиками інформаційної безпеки, заходів інформаційної безпеки та кіберзахисту, а також рівня використання інформаційних технологій у процесах кіберстрахування, що створило основу для інтеграції оцінювання зрілості процесів кіберстрахування з процедурою оцінювання ризиків у межах RA&CIMM.

Практичне значення одержаних результатів. Практичне значення розроблених моделей, методів та алгоритмів полягає в можливості їх використання для збирання, представлення, структуризації, оброблення й аналізу даних під час оцінювання та індексації операційних ризиків у кіберпросторі, а також для інформаційної підтримки прийняття рішень у процесах кіберстрахування.

Розроблена RA&CIMM забезпечує структуризацію процесу оцінювання за визначеними доменами, піддоменами та індикаторами, формування профілю ризиків і зрілості об'єкта оцінювання та використання одержаних результатів для порівняльного аналізу, моніторингу й інформаційної підтримки прийняття рішень.

Практичну перевірку окремих методичних та алгоритмічних положень RA&CIMM здійснено шляхом їх реалізації у формі структурованих опитувальників, словників кодування, контрольних процедур, алгоритмів формування індексних оцінок, структурованих розрахункових таблиць і дослідного вебзастосунку. Під час інтерпретації результатів ураховано, що дані самооцінювання потребують подальшого підтвердження результатами експертного оцінювання і технічної верифікації.

Робочий авторський переклад та адаптовані положення ISO/IEC 27102:2019 використано в діяльності Громадської організації «Міжнародний університет кібербезпеки» під час виконання науково-дослідної роботи № 0121U112396. Адаптовані положення стандарту застосовано як нормативно-методичну основу для систематизації процесів кіберстрахування, формування критеріїв оцінювання ризиків і зрілості та розроблення відповідного інструментарію.

Для пілотної апробації окремих положень RA&CIMM розроблено структуровані електронні опитувальники, словники кодування, контрольні правила, розрахункові таблиці та дослідний вебзастосунок для автоматизованого збирання, оброблення, узагальнення і представлення результатів оцінювання. На масиві десяти анонімізованих анкет страхувальників апробовано 23-показникову

тридоменну процедуру формування композитного індексу цифрової зрілості (Composite Digital Maturity Index, CDMI) та його консервативного андеррайтингового показника (Composite Digital Maturity Index for Underwriting, CDMI-UW), а також перевірено процедури оброблення пропущених і неоцінюваних відповідей, множинних відповідей та критичних контрольних умов.

Поєднання інтегрального показника з критичними контрольними умовами дало змогу сформувати попередні рекомендації щодо страхової прийнятності. Для шести профілів страхувальників рекомендовано відкласти страхове рішення до впровадження мінімально необхідних заходів кіберзахисту, для трьох — продовжити оцінювання після усунення критичних прогалин, один профіль визначено прийнятним у межах пілотного оцінювання.

На чотирьох фактичних профілях, сформованих за результатами первинного та повторного самооцінювання страхових компаній, перевірено можливість зіставлення результатів послідовних циклів оцінювання та відстеження впливу змін за окремими контрольними позиціями на інтегральний результат.

Розроблені табличний прототип і дослідний вебзастосунок реалізують процедури збирання, перевірки, числового кодування, групування, зважування й агрегування даних, аналізу чутливості, перевірки критичних умов та формування рекомендацій. Вони забезпечують обчислення доменних і узагальнених показників, представлення індивідуальних і зведених результатів та порівняння результатів послідовних циклів оцінювання. Розроблені засоби доцільно розглядати як дослідні реалізації окремих складових майбутньої інформаційної системи, а не як завершену програмну систему. Одержані результати можуть бути використані під час подальшого розвитку та практичної апробації інформаційної технології підтримки прийняття рішень у процесах кіберстрахування.

Особистий внесок здобувача. Усі наукові результати, що виносяться на захист, одержані здобувачем особисто або за його безпосередньої участі. У

наукових працях, опублікованих у співавторстві, здобувачеві належать результати, пов'язані з постановкою завдань оцінювання операційних ризиків у кіберпросторі в предметній області кіберстрахування, дослідженням можливостей застосування індексного підходу, систематизацією показників та індикаторів кіберризиків, аналізом інформаційних технологій страхування і кіберстрахування, а також розробленням підходів до формалізації й автоматизації стандартизованих процесів кіберстрахування.

Особисто здобувачем розвинуто методологічні засади індексного оцінювання стану кібербезпеки та операційних ризиків у кіберпросторі, удосконалено підхід до структуризації різнорідних показників оцінювання, сформовано вимоги до їх використання у процесах кіберстрахування, розроблено концептуальні положення та доменну структуру RA&CIMM, метод формування доменних підіндексів та інтегрального індексу, алгоритм багаторівневого оцінювання, а також критерії інтерпретації ризиків і зрілості процесів кіберстрахування.

Здобувачем розроблено структуру опитувальників, словники кодування, процедури перевірки, контролю якості та агрегування даних, виконано розрахунки CDMI та CDMI-UW за даними десяти анонімізованих анкет страхувальників, проведено аналіз чутливості й інтерпретацію одержаних результатів. Для перевірки повторного циклу оцінювання здобувачем опрацьовано результати первинного та повторного самооцінювання страхових компаній, сформовано фактичні профілі, виконано відповідні розрахунки та підготовлено рекомендації за результатами оцінювання.

Апробація результатів дисертації. Основні положення та результати дисертаційного дослідження доповідалися й обговорювалися на міжнародних і всеукраїнських наукових та науково-практичних конференціях, зокрема: XIV Всеукраїнській науково-практичній конференції «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 30 березня 2023 р.); науково-практичній конференції «Кібербезпека енергетики» Інституту проблем

моделювання в енергетиці ім. Г. Є. Пухова НАН України (Київ, 31 травня 2023 р.); науково-практичній конференції «Резильєнтність критичної інфраструктури — 2023» (Київ, 21 червня 2023 р.); науково-практичній конференції «Кібербезпека енергетики» Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України (Київ, 29 травня 2024 р.); XXIV Міжнародній науково-практичній конференції «Інформаційно-комунікаційні технології для перемоги та відновлення» Інституту телекомунікацій і глобального інформаційного простору НАН України (Київ, 11–12 листопада 2025 р.); VII науково-практичній конференції «Безпека енергетики в епоху цифрової трансформації» Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України (Київ, 20 листопада 2025 р.). Окремі результати дисертаційного дослідження, одержані у співавторстві, було представлено на міжнародному науковому заході Центру передового досвіду НАТО з кібероборони (NATO Cooperative Cyber Defence Centre of Excellence, NATO CCDCOE) у березні 2026 року.

На зазначених наукових заходах апробовано результати досліджень, присвячених:

- застосуванню індексів кібербезпеки для оцінювання стану інформаційної безпеки об’єктів критичної інфраструктури;
- статистичному підходу до оброблення даних про кіберінциденти, кібератаки, кіберзагрози та заходи протидії;
- методологічним засадам формування індексу кіберрезильєнтності критичної інфраструктури;
- тенденціям розвитку та застосуванню інформаційних технологій кіберстрахування;
- оцінюванню стану кіберзахисту з використанням базових індикаторів кібербезпеки;
- систематизації інформаційних технологій страхування та кіберстрахування.

Публікації. За темою дисертації опубліковано 10 наукових праць, у яких висвітлено основні положення та результати дисертаційного дослідження. Із них чотири статті опубліковано в наукових фахових виданнях, шість праць — у матеріалах міжнародних і всеукраїнських наукових та науково-практичних конференцій.

В опублікованих працях представлено результати досліджень щодо:

- застосування індексів кібербезпеки для оцінювання стану інформаційної безпеки та статистичного оброблення даних про кіберінциденти, кібератаки, кіберзагрози й заходи протидії;
- формування індексу кіберрезильєнтності критичної інфраструктури;
- формалізації та автоматизації стандартизованих процесів кіберстрахування;
- систематизації інформаційних технологій страхування і кіберстрахування;
- оцінювання стану кіберзахисту з використанням базових індикаторів кібербезпеки;
- дослідження складових індексів кібербезпеки;
- розроблення методологічних основ оцінювання ризиків і зрілості процесів кіберстрахування та моделі RA&CIMM.

Структура дисертації. Дисертаційна робота складається з анотації, вступу, п’яти розділів, загальних висновків, списку використаних джерел та додатків. У першому розділі проаналізовано проблему та стан досліджень у сфері оцінювання операційних ризиків у кіберпросторі. У другому розділі розроблено моделі та методи індексного оцінювання й доменної структуризації показників. У третьому розділі формалізовано процеси кіберстрахування та систематизовано інформаційні технології їх автоматизації. У четвертому розділі розроблено RA&CIMM, метод формування доменних підіндексів та інтегрального індексу, алгоритм багаторівневого оцінювання, а також сформовано методологічну й алгоритмічну основу інформаційної технології підтримки прийняття рішень. У

п’ятому розділі проведено пілотну апробацію окремих методичних та алгоритмічних положень RA&CIMM на анонімізованих даних самооцінювання страхувальників і фактичних даних первинного та повторного самооцінювання страхових компаній.

РОЗДІЛ 1. ОГЛЯД ПРОБЛЕМИ ТА СТАНУ ДОСЛІДЖЕНЬ У СФЕРІ ОЦІНЮВАННЯ ОПЕРАЦІЙНИХ РИЗИКІВ У КІБЕРПРОСТОРІ

1.1. Розвиток кіберризиків та їх вплив на операційні процеси

Стрімкий розвиток інформаційно-комунікаційних технологій та цифровізація основних процесів діяльності державних установ, підприємств і організацій зумовили посилення залежності функціонування цих суб'єктів від інформаційних систем, цифрових сервісів та інформаційних ресурсів [1, 3, 41]. Історичним етапом формування державної політики у цій сфері була Стратегія кібербезпеки України 2016 року [42], положення якої надалі були розвинені й актуалізовані чинною Стратегією кібербезпеки України та планом її реалізації [1, 41].

Інформаційні технології стали невід'ємною складовою управлінських, виробничих, фінансових та інших операційних процесів. За таких умов порушення функціонування інформаційних систем може безпосередньо впливати на здатність організації виконувати основні функції та забезпечувати безперервність діяльності.

Одночасно з розвитком цифрових технологій відбувається трансформація характеру ризиків, пов'язаних із використанням інформаційних систем і мереж. Кіберзагрози дедалі частіше розглядаються не лише як технологічні загрози інформаційній безпеці, а й як чинники, здатні спричиняти істотні порушення операційної діяльності. Реалізація кіберзагроз може призводити до порушення конфіденційності, цілісності та доступності інформації, зупинення окремих процесів, втрати доступу до інформаційних ресурсів, порушення взаємодії між структурними підрозділами та контрагентами, необхідності відновлення інформаційної інфраструктури й виникнення фінансових втрат [2, 4].

Зазначені зміни зумовлюють необхідність розгляду кіберризику в контексті його впливу на операційні процеси організації. У такому разі оцінювання не може обмежуватися визначенням імовірності реалізації окремої кіберзагрози або встановленням наявності певної вразливості, а має охоплювати сукупність чинників, що визначають можливість виникнення негативних наслідків для функціонування організації [4, 43].

Особливого значення зазначена проблема набуває для об'єктів критичної інфраструктури, функціонування яких безпосередньо залежить від стійкості інформаційних та інформаційно-комунікаційних систем. Порушення роботи таких систем може мати наслідки, що виходять за межі окремої організації та впливають на функціонування галузей, надання суспільно важливих послуг і забезпечення життєдіяльності населення [44, 45].

Організація кіберзахисту таких об'єктів потребує поєднання нормативних, організаційних, управлінських та технічних складових у межах цілісної організаційно-технічної моделі. Концептуальні засади побудови та впровадження такої моделі на національному рівні розглянуто в працях українських дослідників [46, 47]. Для цього дослідження відповідний підхід є важливим як основа структуризації різнорідних показників, що характеризують стан кіберзахисту та можуть ураховуватися під час оцінювання операційного кіберризику.

В умовах воєнного стану вплив кіберризиків на операційну діяльність додатково посилюється. Кіберпростір використовується як середовище цілеспрямованого впливу на інформаційні ресурси, інформаційні системи та об'єкти критичної інфраструктури. Зміна інтенсивності, характеру та спрямованості кіберзагроз потребує постійного оновлення даних про стан кібербезпеки й чинники, що впливають на рівень кіберризику [1, 36].

Особливо критичними є кіберризики в енергетичному секторі, у якому порушення функціонування інформаційних і автоматизованих систем керування може впливати на безперервність надання життєво важливих послуг [48]. Наукові та практичні дослідження у цій сфері охоплюють питання кіберстійкості

енергетичної інфраструктури, організації галузевої системи кібербезпеки, енергетичної безпеки та відновлення відповідної інфраструктури [36, 49–55].

У попередніх дослідженнях автора оцінювання стану інформаційної безпеки об'єктів критичної інфраструктури розглянуто на основі застосування індексів кібербезпеки [9]. Надалі цей напрям розвинуто шляхом застосування статистичного підходу до оброблення даних про кіберінциденти, кібератаки, кіберзагрози та заходи протидії [10], а також обґрунтування методологічних засад формування індексу кіберрезильєнтності критичної інфраструктури [11].

Аналіз зазначених категорій даних свідчить про їх суттєву різнорідність. Відомості про кіберінциденти можуть бути представлені абсолютними та відносними показниками; характеристики кібератак — розподілами за типами, джерелами та об'єктами впливу; кіберзагрози — категоріями й рівнями небезпеки; заходи протидії — показниками впровадження організаційних і технічних засобів кіберзахисту [56–58]. Тому безпосереднє агрегування таких даних потребує їх попередньої структуризації, нормування та приведення до формалізованого подання. Відповідний статистичний підхід до оброблення даних про кіберінциденти, кібератаки, кіберзагрози та заходи протидії розглянуто в попередньому дослідженні автора [10].

Для оцінювання впливу кіберризиків на операційні процеси недостатньо використання одного показника або окремої статистичної характеристики. Зокрема, кількість зареєстрованих кіберінцидентів не відображає повною мірою ймовірність їх виникнення та масштаби потенційних наслідків. Так само наявність технічних засобів кіберзахисту сама по собі не визначає рівень операційного ризику без урахування критичності інформаційних активів, організації управління ризиками та здатності організації запобігати кіберінцидентам, реагувати на них і відновлюватися після їх виникнення [3, 43, 59].

Отже, розвиток кіберризиків і посилення їх впливу на операційні процеси зумовлюють необхідність переходу від аналізу окремих характеристик

кіберзагроз і засобів кіберзахисту до комплексного оцінювання сукупності взаємопов'язаних показників. Таке оцінювання має передбачати структуризацію, формалізоване представлення, нормування, оброблення та агрегування різнорідних даних для формування узагальненої оцінки операційних ризиків у кіберпросторі.

З огляду на це подальше розроблення методів оцінювання операційних ризиків у кіберпросторі потребує уточнення співвідношення кіберризику та операційного ризику, аналізу наявних моделей і методів оцінювання кіберризиків, індексних підходів до оцінювання стану кібербезпеки та інформаційних технологій, що застосовуються у процесах кіберстрахування. Зазначені питання розглянуто в наступних підрозділах дисертаційної роботи.

1.2. Кіберризик як складова операційного ризику

Ризик характеризує вплив невизначеності на досягнення визначених цілей. Його оцінювання передбачає ідентифікацію джерел і чинників ризику, аналіз можливості виникнення небажаних подій та визначення характеру й масштабу їх потенційних наслідків [60]. Залежно від предметної області змінюються джерела ризику, характеристики відповідних подій і способи подання їх наслідків, однак спільною залишається необхідність формалізованого опису чинників, що впливають на стан об'єкта оцінювання.

Операційний ризик характеризує можливість виникнення негативних наслідків у процесі функціонування організації внаслідок недоліків внутрішніх процесів, порушення функціонування систем, дій персоналу або впливу зовнішніх подій [61]. В умовах цифровізації значна частина операційних процесів реалізується з використанням інформаційних і комп'ютерних систем та інформаційно-комунікаційних технологій. Тому порушення функціонування

цифрової інфраструктури може безпосередньо спричинити порушення операційної діяльності організації.

Ризик інформаційної безпеки пов’язаний із можливістю виникнення негативних наслідків унаслідок порушення конфіденційності, цілісності або доступності інформації та інформаційних систем. Його оцінювання передбачає визначення інформаційних активів, загроз, вразливостей, наявних заходів захисту та можливих наслідків реалізації відповідних загроз [3, 58]. Такий підхід дає змогу оцінити захищеність інформаційних ресурсів, однак не завжди безпосередньо відображає вплив кіберінциденту на операційні процеси організації.

Кіберризик пов’язаний із можливістю реалізації кіберзагроз щодо інформаційних ресурсів та інформаційної інфраструктури, використанням вразливостей інформаційних і комп’ютерних систем та виникненням негативних наслідків для інформаційних активів, технологічних процесів і діяльності організації [3, 44]. Його оцінювання потребує врахування взаємозв’язків між джерелами кіберзагроз, станом об’єкта оцінювання, наявними заходами кіберзахисту, ймовірністю виникнення кіберінцидентів та масштабами їх можливих наслідків [43, 59].

У межах дисертаційного дослідження прийнято концептуальне співвідношення, за якого операційний ризик розглядається як ширша категорія, ризик інформаційної безпеки — як ризик, пов’язаний із порушенням властивостей інформації та функціонування інформаційних систем, а кіберризик — як ризик, зумовлений реалізацією кіберзагроз у кіберпросторі. Якщо реалізація кіберзагрози призводить до порушення операційних процесів організації, відповідний кіберризик розглядається як складова операційного ризику.

З огляду на зазначене в дисертаційному дослідженні під операційним ризиком у кіберпросторі розуміється ризик виникнення негативних наслідків для операційних процесів організації унаслідок реалізації кіберзагроз, порушення функціонування інформаційних і комп’ютерних систем або недостатньої

результативності організаційних і технічних заходів інформаційної безпеки та кіберзахисту. Таке трактування дає змогу пов'язати показники кіберзагроз, вразливостей і стану кіберзахисту з характеристиками операційних наслідків та визначити склад даних, необхідних для подальшого оцінювання.

Взаємозв'язок розглянутих категорій можна подати у вигляді такої причинно-наслідкової послідовності:

джерело кіберзагрози → реалізація кіберзагрози з використанням вразливості → кіберінцидент → порушення властивостей інформації або функціонування інформаційної або комп'ютерної системи → порушення операційного процесу → операційні наслідки.

У наведеній послідовності кіберризик характеризує невизначеність, пов'язану з можливістю реалізації кіберзагрози та її впливом на відповідний об'єкт, тоді як операційний аспект ризику визначається характером можливих наслідків для процесів діяльності організації. Тому віднесення кіберризику до операційних ризиків визначається не лише джерелом його виникнення, а насамперед здатністю реалізованої кіберзагрози порушувати виконання операційних функцій.

Для задач оцінювання така постановка має принципове значення. Якщо об'єктом аналізу є окрема кіберзагроза, оцінювання може охоплювати характеристики загрози, наявні вразливості та технічний стан засобів захисту. Якщо оцінюється операційний ризик у кіберпросторі, система показників має додатково враховувати критичність інформаційних активів і операційних процесів, стан управління ризиками, впроваджені заходи кіберзахисту, а також здатність організації реагувати на кіберінциденти та відновлювати функціонування систем [3, 43, 59].

Таким чином, операційний ризик у кіберпросторі є багатофакторною категорією, оцінювання якої потребує оброблення різнорідних показників, що характеризують джерела кіберзагроз, вразливості, стан інформаційних і комп'ютерних систем, процеси управління ризиками, заходи інформаційної

безпеки та кіберзахисту, а також можливі операційні наслідки. Різнорідність і взаємозалежність зазначених показників обмежують можливість визначення рівня ризику на основі одного показника.

Зазначену проблему можна формалізувати як задачу структуризації, представлення та оброблення множини різнорідних вхідних даних для формування узагальненої оцінки операційного ризику в кіберпросторі. Така постановка створює основу для визначення структури показників, способів їх формалізованого подання, правил оброблення та процедур агрегування одержаних результатів.

Отже, розгляд кіберризику як складової операційного ризику у випадках, коли його реалізація впливає на операційні процеси, визначає необхідність переходу від аналізу окремих технічних характеристик кіберзагроз до комплексного оцінювання сукупності показників. Такі показники мають характеризувати стан об’єкта оцінювання, його інформаційні активи, наявні вразливості, процеси управління ризиками та можливі наслідки для операційної діяльності. Це зумовлює необхідність аналізу наявних моделей і методів оцінювання кіберризиків та стану кібербезпеки, який проведено в наступному підрозділі.

1.3. Методи та моделі оцінювання кіберризиків і стану кібербезпеки

Оцінювання кіберризиків і стану кібербезпеки пов’язане з обробленням значної кількості різнорідних даних, що характеризують кіберінциденти, кібератаки, кіберзагрози, вразливості, стан інформаційних і комп’ютерних систем та впроваджені заходи кіберзахисту [56–58, 62, 63]. Залежно від об’єкта й мети оцінювання відповідні характеристики можуть бути представлені кількісними, якісними або категоріальними показниками, зокрема сформованими експертним

шляхом. Така різнорідність зумовлює необхідність побудови структурованої системи показників, придатних для формалізованого представлення, оброблення та агрегування.

У попередніх дослідженнях автора оцінювання стану інформаційної безпеки та кібербезпеки розглянуто з позицій формування кількісних показників та індексів на національному, секторальному й організаційному рівнях [6, 9–11, 64]. Встановлено, що суб'єктами індексування залежно від призначення відповідного індексу можуть бути держави, галузі або сектори економіки, підприємства та організації. Об'єктами індексування можуть бути процеси діяльності відповідних суб'єктів, стан їх кібербезпеки й рівень захищеності від кіберзагроз, а також окремі показники безпеки та захищеності.

Зазначений підхід має принципове значення для визначення об'єкта оцінювання. Стан кібербезпеки не може бути охарактеризований лише кількістю зафіксованих кіберінцидентів або наявністю окремого засобу кіберзахисту. Об'єкт оцінювання характеризується сукупністю взаємопов'язаних процесів, станів і показників [3, 57, 58, 62, 63]. Тому розв'язання задачі оцінювання потребує визначення множини характеристик досліджуваного об'єкта, інформаційних зв'язків між ними та способу їх представлення в межах єдиної системи.

Одним із підходів до розв'язання зазначеної задачі є застосування методів статистичного дослідження. У попередньому дослідженні автора, присвяченому обробленню даних про кіберінциденти, кібератаки, кіберзагрози та заходи протидії, розглянуто методи статистичного спостереження, зведення і групування даних, формування узагальнювальних статистичних показників, а також аналізу й інтерпретації одержаних результатів [10]. До узагальнювальних статистичних показників належать середні та відносні величини, показники варіації й динаміки, статистичні індекси та рейтинги [7].

З позицій системного аналізу одним із ключових етапів статистичного дослідження є формування системи базисних параметрів. Такі параметри

виконують системоутворювальну функцію та визначають склад даних, що підлягають збиранню, накопиченню, обробленню й аналізу. У попередньому дослідженні автора запропоновано модель статистичної системи індексів для опису кіберінцидентів, кібератак, кіберзагроз і заходів протидії [10]. У межах цієї моделі до базисних параметрів віднесено індикатори кіберінцидентів, кібератак і кіберзагроз, а також показники заходів кіберзахисту.

Формування системи базисних параметрів є початковим етапом статистичного спостереження процесів і подій у кіберпросторі. Наступні етапи передбачають збирання, перевірку, накопичення, групування, оброблення та аналіз відповідних даних. У межах задач оцінювання кіберризиків цю послідовність інформаційних процесів можна подати таким чином:

формування системи параметрів → збирання та перевірка даних → накопичення даних → групування й оброблення → аналіз → формування узагальненої оцінки.

Наведена послідовність відображає перехід від множини різнорідних відомостей про процеси та події у кіберпросторі до їх структурованого представлення й формалізованого оброблення. З позицій комп'ютерних наук система параметрів визначає структуру вхідних даних, а послідовність операцій над ними створює основу для алгоритмізації процедур оцінювання.

Під час формування набору базисних параметрів ураховано положення нормативних і методичних документів та моделей, у яких застосовуються системи показників та індикаторів, зокрема Національної системи оцінювання кіберінцидентів (National Cyber Incident Scoring System, NCISS), класифікації кіберінцидентів Організації з безпеки і співробітництва в Європі, системи оцінювання кіберризиків NIST, показників кіберстійкості MITRE, індикаторів інформаційної безпеки ETSI та положень ISO/IEC 27004 щодо моніторингу, вимірювання, аналізу й оцінювання інформаційної безпеки [56–58, 62, 63, 65].

Аналіз зазначених підходів показує, що оцінювання окремих складових кібербезпеки здійснюється із застосуванням наборів показників та індикаторів,

сформованих відповідно до визначених об’єкта й мети оцінювання [56–58, 62, 63, 65]. Відмінності у складі параметрів не виключають можливості їх систематизації за функціональним призначенням. Цей підхід використано для формування чотирьох груп базисних параметрів, що характеризують кіберінциденти, кібератаки, кіберзагрози та заходи кіберзахисту.

Подальший розвиток зазначеного напряму пов’язаний із застосуванням моделей, побудованих на системах базових індикаторів кібербезпеки. У попередньому дослідженні автора проаналізовано модель зрілості спроможностей у сфері кібербезпеки (Cybersecurity Capability Maturity Model, C2M2), модель зрілості інтелектуальних електричних мереж (Smart Grid Maturity Model, SGMM), локальний індекс кібербезпеки (Local Cybersecurity Index, LCSI), а також системи показників та індикаторів, визначені нормативно-методичними документами України [39, 66, 67]. Відповідні документи регламентують проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, підвищення рівня її кіберзахисту, забезпечення кіберзахисту автоматизованих систем керування технологічними процесами та кібербезпеки паливно-енергетичного сектору критичної інфраструктури.

У проаналізованих моделях і нормативно-методичних документах оцінювання здійснюється за сукупністю доменів — логічно виокремлених областей оцінювання — та відповідних показників, параметрів або індикаторів, а в окремих випадках також за піддоменами й рівнями зрілості [39, 66, 67]. Спільним для цих підходів є структурне представлення складного об’єкта оцінювання у вигляді ієрархічної системи взаємопов’язаних елементів.

Застосування доменної структури дає змогу декомпозувати складний об’єкт оцінювання на логічно пов’язані області, кожна з яких характеризується визначеним набором індикаторів. За такого підходу окремий показник розглядається як елемент відповідного домену або піддомену. Це створює можливість формування доменних оцінок та їх подальшого агрегування для одержання узагальненої оцінки стану об’єкта [39, 66, 67].

Окремим напрямом є дослідження моделей кіберрезильєнтності. Кіберрезильєнтність характеризує здатність організації передбачати несприятливі кіберподії, протистояти їм, відновлюватися після них та адаптуватися до змінених умов, забезпечуючи виконання критичних функцій [8, 63]. У попередньому дослідженні автора обґрунтовано методологічні засади індексу кіберрезильєнтності (Cyber Resilience Index, CRI), у структурі якого виокремлено дві взаємопов'язані складові: систему практик кіберрезильєнтності та індексне оцінювання її фактичного стану [11].

Важливим результатом аналізу моделей кіберрезильєнтності є розмежування процесу визначення необхідних практик і процесу оцінювання фактичного стану об'єкта. Така логіка відповідає загальній послідовності оцінювання: спочатку визначаються структура характеристик об'єкта, відповідні показники та критерії їх оцінювання, після чого здійснюються збирання, перевірка, оброблення й агрегування одержаних значень.

У подальших дослідженнях зазначений структурний принцип використано під час аналізу моделей оцінювання у сфері кіберстрахування. У праці «Інформаційні технології кіберстрахування» розглянуто факторний аналіз інформаційного ризику (Factor Analysis of Information Risk, FAIR), байєсівські мережі та інші підходи до моделювання кіберризиків [19]. FAIR забезпечує кількісне оцінювання частоти виникнення подій і величини можливих втрат, що дає змогу представляти ризик у фінансовому вираженні, однак його застосування потребує достатнього обсягу якісних вихідних даних [43, 59].

Байєсівські мережі дають змогу представляти причинно-наслідкові зв'язки між факторами кіберризику та здійснювати їх імовірнісний аналіз. Водночас застосування таких моделей потребує визначення структури взаємозв'язків, налаштування параметрів і накопичення даних, достатніх для одержання обґрунтованих оцінок [19]. Тому вибір моделі має враховувати мету оцінювання, склад і якість доступних даних, а також можливість формалізації взаємозв'язків між факторами ризику.

Проведений аналіз засвідчив актуальність автоматизації оцінювання кіберризиків, моделювання частоти виникнення кіберінцидентів і величини можливих втрат, накопичення та оброблення даних про системні ризики, адаптації наявних методів до аналізу кіберподій, а також обґрунтованого вибору моделей відповідно до завдань кіберстрахування [19, 68, 69].

Отже, аналіз моделей і методів дає змогу виокремити такі взаємопов'язані підходи до оцінювання кіберризиків і стану кібербезпеки: статистичне спостереження та оброблення даних про кіберподії; формування систем базисних параметрів та індикаторів; застосування моделей оцінювання стану кіберзахисту; доменну декомпозицію об'єкта оцінювання; визначення рівнів зрілості; формування індексних оцінок; кількісне та ймовірнісне моделювання інформаційних і кіберризиків [19, 39, 56–59, 62, 63, 65–67, 70].

Кожен із зазначених підходів забезпечує розв'язання окремої складової задачі оцінювання. Статистичні методи застосовуються для збирання, групування, оброблення й аналізу даних; система базисних параметрів визначає їх структуру; моделі, побудовані на системах індикаторів, характеризують стан окремих складових кіберзахисту; доменна декомпозиція забезпечує структуризацію складного об'єкта; моделі зрілості дають змогу визначати рівень розвитку відповідних процесів; індексні методи забезпечують нормування та агрегування різнорідних показників; кількісні й імовірнісні моделі використовуються для оцінювання частоти подій і величини можливих втрат.

Водночас оцінювання операційних ризиків у кіберпросторі для потреб кіберстрахування потребує поєднання зазначених підходів у межах єдиної методологічної основи. Об'єкт оцінювання має бути представлений системою параметрів та індикаторів, структурованих за логічними областями оцінювання, а різнорідні вхідні дані — приведені до форми, придатної для перевірки, нормування, групування, оброблення й агрегування з подальшим формуванням узагальненої оцінки.

Таким чином, проведений аналіз підтверджує доцільність застосування індексного підходу для формалізованого представлення, нормування й агрегування різнорідних показників стану кібербезпеки та операційних ризиків у кіберпросторі. Наявні індексні підходи та можливості їх використання для розв'язання задач дисертаційного дослідження проаналізовано в наступному підрозділі.

1.4. Індексні підходи до оцінювання стану кібербезпеки

Кількісне оцінювання стану інформаційної безпеки та кібербезпеки потребує формування узагальнених показників, які характеризують складні об'єкти й процеси на основі сукупності окремих параметрів. Одним із підходів до розв'язання цієї задачі є застосування індексного методу, який дає змогу систематизувати, зіставляти та агрегувати показники, що характеризують різні складові стану об'єкта оцінювання [7].

У попередніх дослідженнях автора встановлено, що залежно від призначення індексу суб'єктами індексування можуть бути держави, галузі або сектори економіки, підприємства й організації. Об'єктами індексування можуть виступати процеси діяльності відповідних суб'єктів, стан їх інформаційної безпеки та кібербезпеки, рівень захищеності від кіберзагроз, а також окремі показники безпеки й захищеності [6, 9, 64].

Індексування у сфері кібербезпеки може здійснюватися на національному, секторальному та організаційному рівнях. На національному рівні індекс характеризує сукупність показників розвитку кібербезпеки, кіберстійкості або кіберпотужності держави. На секторальному рівні об'єктом оцінювання є стан кібербезпеки відповідної галузі або сектору економіки. На організаційному рівні

індексування спрямоване на оцінювання стану окремого підприємства або організації, їх інформаційних ресурсів, процесів і рівня захищеності [6, 9, 64].

У попередній праці автора, присвяченій застосуванню індексів кібербезпеки для оцінювання стану інформаційної безпеки об'єктів критичної інфраструктури, проаналізовано глобальні та національні індекси, а також мережеві індекси й рейтингові платформи кібербезпеки [9]. До досліджуваної сукупності включено Panorays, Black Kite Cyber Risk Ratings Platform, BitSight Security Ratings Platform, Cyber Exposure Index, CyberGreen, National Cyber Power Index, Prevalent Vendor Threat Monitor, RiskRecon Cybersecurity Ratings, SecurityScorecard Ratings Platform та UpGuard Ratings Platform.

Проведений аналіз засвідчив відмінності у визначенні предмета й об'єкта індексування. Відповідні системи можуть бути орієнтовані на оцінювання зовнішньої поверхні атаки, стану мережевої безпеки, характеристик кіберризику, кібербезпеки постачальників або інших складових цифрової екосистеми [9]. Отже, поняття «індекс кібербезпеки» не визначає єдиного складу показників або універсальної процедури оцінювання: структура індексу залежить від його призначення, рівня оцінювання та доступних джерел даних.

Окрему групу становлять фондові й тематичні індекси, що використовуються для формування інвестиційних продуктів і відображають динаміку вартості акцій компаній сектору кібербезпеки [71–78]. Такі індекси характеризують визначений сегмент ринку капіталу, а не стан кібербезпеки, рівень кіберризику або зрілість процесів конкретної організації. Тому вони не можуть безпосередньо використовуватися для оцінювання страхового кіберризику, але демонструють різноманітність цілей, об'єктів і методик індексування у сфері кібербезпеки.

У страховій практиці індексний підхід також застосовується в індексному страхуванні, за якого виплата пов'язується з досягненням заздалегідь визначеним параметром установленого порогового значення, а не з індивідуальним оцінюванням фактичного збитку [79]. Таке розуміння індексного страхування

необхідно відрізняти від індексного оцінювання кіберризиків, яке в цьому дослідженні використовується для нормування, агрегування та узагальненого представлення різнорідних показників об’єкта оцінювання.

У попередній публікації за участю автора також розглянуто можливість застосування ресурсних кооперативних теоретико-ігрових моделей для прогнозування поведінки окремих фінансових індексів кібербезпеки [64, 80, 81]. У межах цього дослідження зазначений підхід використано для окреслення можливого напряму подальшого моделювання та не застосовано під час формування або апробації RA&CIMM.

Особливе значення для індексування має формування системи показників. Індекс не є первинною характеристикою об’єкта, а утворюється внаслідок оброблення та агрегування множини вхідних даних за визначеною процедурою [7]. Тому обґрунтованість та інформативність індексної оцінки залежать від повноти опису об’єкта, структури показників, якості вхідних даних і правил їх оброблення.

У попередній праці автора, присвяченій статистичному підходу до оброблення даних про кіберінциденти, кібератаки, кіберзагрози та заходи протидії, запропоновано модель статистичної системи індексів [10]. Базисними параметрами цієї моделі визначено індикатори кіберінцидентів, кібератак і кіберзагроз, а також показники заходів кіберзахисту.

Формування системи базисних параметрів забезпечує перехід від аналізу окремих подій і характеристик до структурованої множини даних. Індикатори кіберінцидентів характеризують події, які відбулися та мають ознаки порушення стану кібербезпеки; індикатори кібератак — способи й характеристики здійснення негативного впливу; індикатори кіберзагроз — потенційні джерела, умови та чинники такого впливу; показники заходів кіберзахисту — стан впровадження засобів і процедур протидії відповідним загрозам та кібератакам [10].

З позицій оброблення даних формування індексу передбачає виконання послідовності взаємопов'язаних операцій. Первинні дані збираються з визначених джерел, перевіряються, структуруються відповідно до системи параметрів, приводяться до зіставного вигляду, групуються за встановленими ознаками та агрегуються за визначеною процедурою формування індексної оцінки [10]. Таким чином, індексування є не лише способом представлення кінцевого результату, а й упорядкованою послідовністю операцій над даними.

У подальших дослідженнях індексний підхід застосовано до оцінювання кіберрезильєнтності критичної інформаційної інфраструктури. У попередній праці автора обґрунтовано модель, що поєднує систему практик кіберрезильєнтності (Cyber Resilience Framework, CRF) та індекс оцінювання стану кіберрезильєнтності (Cyber Resilience Index, CRI) [11]. CRI призначений для формування узагальненої оцінки рівня кіберрезильєнтності організації на основі показників, структурованих відповідно до визначених практик.

Зазначена структура відображає важливий для дисертаційного дослідження принцип: модель представлення об'єкта оцінювання та метод оцінювання його стану є взаємопов'язаними, але не тотожними складовими. Модель визначає структуру областей, характеристик і зв'язків об'єкта, тоді як метод встановлює послідовність збирання, перевірки, нормування, оброблення й агрегування значень відповідних показників.

Аналогічний принцип застосовано під час розроблення проєкту «Методика оцінки зрілості кібербезпеки та кіберстрахування електричних мереж». У межах цього проєкту індекс кібербезпеки визначено як інтегральне значення сукупності індикаторів кібербезпеки, сформоване за встановленою процедурою. Залежно від способу формування та представлення результатів розрізнено автоматичний, синтетичний і аналітичний індекси кібербезпеки, а також індекс зрілості кібербезпеки [64].

Автоматичний індекс кібербезпеки передбачає формування безрозмірного інтегрального значення із застосуванням формалізованих методів та алгоритмів

автоматичного індексування. Синтетичний індекс є інтегральним значенням сукупності індикаторів кібербезпеки, сформованим за визначеною процедурою. Індекс зрілості утворюється шляхом агрегування індикаторів, що характеризують рівень розвитку й впровадження відповідних процесів. Аналітичний індекс представлено інформаційними матеріалами, що містять експертні, аналітичні та статистичні відомості про стан безпеки, рівень захищеності й окремі наслідки реалізації загроз [64].

Таке розмежування відображає різні способи представлення й оброблення даних. Аналітичний індекс передбачає змістове узагальнення та інтерпретацію різнорідних даних, статистичних відомостей і експертних оцінок без їх обов'язкового агрегування в єдине числове значення. Синтетичний індекс передбачає агрегування визначеної множини індикаторів. Автоматичний індекс додатково потребує формалізованого опису процедур збирання, перевірки, оброблення та агрегування даних у вигляді методів і алгоритмів, придатних для програмної реалізації.

З позицій комп'ютерних наук автоматизоване формування індексної оцінки потребує формального визначення структури вхідних даних, правил їх перевірки та перетворення, процедур нормування й агрегування, а також алгоритму формування вихідного значення. Отже, перехід від аналітичного опису стану кібербезпеки до автоматизованого індексування передбачає формалізацію всього інформаційного процесу оцінювання.

Окремим прикладом розвитку індексного підходу є локальний індекс кібербезпеки (Local Cybersecurity Index, LCSI), розглянутий у попередніх дослідженнях автора [64, 67]. LCSI визначено як комбінований індекс організаційного рівня. Об'єктом індексування може бути об'єкт критичної інформаційної інфраструктури, орган державної влади, підприємство, установа або організація, а на секторальному рівні — сукупність відповідних об'єктів, інформаційних, комунікаційних і мережевих ресурсів.

Застосування LCSI дає змогу перейти від глобальних і національних оцінок до індексування стану конкретного об’єкта або групи об’єктів. Такий перехід має принципове значення для кіберстрахування, оскільки оцінюванню підлягає конкретна організація з властивими їй інформаційними активами, операційними процесами, кіберзагрозами, вразливостями та впровадженими заходами кіберзахисту.

Проведений аналіз дає змогу визначити загальну послідовність індексного оцінювання стану кібербезпеки:

об’єкт оцінювання → система показників та індикаторів → збирання і перевірка даних → структурування та групування → нормування і приведення значень до зіставного вигляду → агрегування → індексна оцінка → інтерпретація результату.

Зазначена послідовність узагальнює результати попередніх досліджень індексів кібербезпеки, статистичної системи базисних параметрів, індексу кіберрезильєнтності та методичних підходів до оцінювання зрілості [6, 9–11, 64, 67]. Вона не визначає конкретного математичного методу формування інтегрального індексу, але створює структурну основу для подальшої формалізації відповідної задачі.

Водночас можливість безпосереднього застосування наявних індексів кібербезпеки у процесах кіберстрахування обмежується їх цільовим призначенням. Національні індекси характеризують держави або національні системи кібербезпеки; мережеві рейтинги — окремі зовнішні характеристики цифрової інфраструктури; індекси кіберрезильєнтності — здатність організації підтримувати та відновлювати виконання критичних функцій в умовах негативного кібернетичного впливу [6, 8, 9, 11]. Для потреб кіберстрахування необхідно одночасно враховувати характеристики кіберризику, стан інформаційної безпеки й кіберзахисту, а також рівень зрілості відповідних процесів.

Таким чином, індексний підхід створює методологічну основу для структуризації, нормування та агрегування різнорідних показників, однак потребує адаптації до інформаційних процесів конкретної предметної області. Для кіберстрахування така адаптація передбачає визначення джерел і складу вхідних даних, процедур їх збирання, перевірки, оброблення й аналізу, а також способів використання одержаних результатів під час прийняття рішень.

Це зумовлює необхідність аналізу інформаційних технологій, які застосовуються для оцінювання ризиків і підтримки прийняття рішень у процесах кіберстрахування.

1.5. Інформаційні технології оцінювання ризиків у процесах кіберстрахування

Розвиток кіберстрахування пов’язаний із необхідністю оброблення значних обсягів інформації про об’єкти страхування, інформаційні активи, кіберзагрози, кіберінциденти, стан інформаційної безпеки та кіберзахисту. Оцінювання операційних ризиків у кіберпросторі передбачає послідовне збирання, представлення, перевірку, оброблення, аналіз та інтерпретацію різнорідних даних. За таких умов інформаційні технології є не лише засобом автоматизації окремих страхових операцій, а й інструментальною основою оцінювання кіберризиків та інформаційної підтримки прийняття рішень [19, 68, 69].

Окремим напрямом наукових досліджень є персональне кіберстрахування, у межах якого систематизуються характерні кіберризики, види страхового покриття та чинники розвитку відповідних страхових продуктів [82]. Водночас у цій дисертації предмет дослідження обмежено інформаційними процесами оцінювання операційних кіберризиків і зрілості процесів кіберстрахування на рівні організацій.

У наукових дослідженнях і документах міжнародних організацій до основних проблем розвитку кіберстрахування віднесено обмеженість і неоднорідність даних про кіберінциденти та збитки, інформаційну асиметрію між страхувальником і страховиком, взаємозалежність кіберризиків, складність їх кількісного оцінювання та необхідність удосконалення процедур андеррайтингу [83–90].

У попередньому дослідженні автора процеси кіберстрахування розглянуто відповідно до положень міжнародних стандартів і наявних практик страхування операційних ризиків у кіберпросторі. Зокрема, досліджено положення ISO/IEC 27102:2019 «Information security management — Guidelines for cyber-insurance» та систематизовано процеси кіберстрахування, придатні до подальшої формалізації, алгоритмізації й автоматизації [12, 13].

На основі положень ISO/IEC 27102:2019 та аналізу практик кіберстрахування систематизовано дев’ять специфічних процесів: оцінювання кіберризиків, зокрема внутрішнього кіберризику, засобів контролю інформаційної безпеки та збитків від кіберінцидентів; управління кіберризиками; типізація кіберінцидентів; управління наслідками кіберінцидентів; управління інформаційною безпекою під час обміну даними зі страховиком; управління полісом кіберстрахування, підтвердними матеріалами, витратами на реагування на кіберінциденти та страховим покриттям; андеррайтинг кіберстрахування; збирання інформації про інформаційні активи; виконання зобов’язань, пов’язаних з інформаційною безпекою [12, 13].

Аналіз зазначених процесів показує, що значна їх частина безпосередньо пов’язана з операціями над даними. Збирання інформації про інформаційні активи формує множину вхідних даних про об’єкт оцінювання. Оцінювання кіберризиків передбачає оброблення характеристик загроз, вразливостей, заходів кіберзахисту та можливих наслідків. Типізація кіберінцидентів потребує класифікації подій за визначеними ознаками. Під час андеррайтингу результати

оцінювання використовуються для формування інформації, необхідної для прийняття страхового рішення.

Таким чином, окремі процеси кіберстрахування можуть бути представлені як послідовності операцій над даними:

джерела інформації → збирання даних → перевірка і структуризація → попереднє оброблення → оцінювання показників → агрегування результатів → інтерпретація → формування інформації для підтримки прийняття рішень.

Таке подання відповідає результатам авторського дослідження стандартизованих процесів кіберстрахування, у якому обґрунтовано можливість використання їх систематизованої сукупності для подальшої формалізації, алгоритмізації та автоматизації [13]. Одержані результати можуть бути використані під час розроблення сценаріїв і алгоритмів кіберстрахування, а також проєктування відповідних інформаційних систем.

З позицій комп'ютерних наук представлення процесів як послідовностей операцій над даними є передумовою їх формалізації та алгоритмізації. Для кожного такого процесу можуть бути визначені джерела та множина вхідних даних, правила їх перевірки й оброблення, послідовність виконуваних операцій і структура вихідних даних. Це створює основу для переходу від змістового опису бізнес-процесу кіберстрахування до його формалізованого представлення як інформаційного процесу.

Окремі процеси кіберстрахування є спільними з процесами традиційного страхування та можуть автоматизуватися із застосуванням аналогічних підходів і алгоритмів. Водночас процеси кіберстрахування характеризуються високим рівнем використання інформаційних технологій, застосуванням спеціалізованих засобів комунікації для збирання даних про кіберризики, а також наявністю напівавтоматизованого зворотного зв'язку, призначеного для інформаційної підтримки та оптимізації бізнес-рішень [19, 68, 69].

Зазначені особливості зумовлюють необхідність системного розгляду інформаційних технологій, які можуть застосовуватися у процесах страхування та кіберстрахування. У попередніх дослідженнях автора систематизовано технології електронного бізнесу, інтеграції інформаційних ресурсів, аналітики великих даних, штучного інтелекту, машинного навчання, оброблення природної мови, блокчейн-технології та смартконтракти, мобільні системи підтримки, а також засоби математичного, імітаційного і статистичного моделювання [19, 68, 69].

Вибір відповідної технології визначається особливостями інформаційного процесу та задачами, які підлягають розв'язанню. Технології інтеграції інформаційних ресурсів можуть застосовуватися для збирання й об'єднання даних із різних джерел. Методи статистичного моделювання та аналітики даних використовуються для оброблення накопичених відомостей і дослідження характеристик ризику. Технології штучного інтелекту й машинного навчання можуть забезпечувати класифікацію даних, виявлення закономірностей і підтримку аналітичних процедур. Блокчейн-технології та смартконтракти можуть застосовуватися для реалізації окремих операцій обміну, зберігання й оброблення даних у страхових процесах [19].

Водночас застосування окремої інформаційної технології саме по собі не забезпечує розв'язання задачі оцінювання кіберризику. Для програмної реалізації відповідного процесу необхідно визначити структуру вхідних даних, систему показників і критеріїв, правила перевірки, перетворення й агрегування значень, а також спосіб формування та інтерпретації результату оцінювання. Отже, технологічні засоби мають застосовуватися в межах формалізованої моделі відповідного інформаційного процесу.

Окремим напрямом автоматизації є застосування спеціалізованих систем оцінювання кіберризиків. Прикладом є система CyberMatics, яку компанія AIG використовувала для автоматизованого збирання та аналізу технічних даних про кіберризики. Такий підхід передбачає використання даних про стан об'єкта

страхування для інформаційної підтримки оцінювання ризику й андеррайтингу [91].

Іншим напрямом є застосування методів машинного навчання та геоінформаційних технологій для оцінювання ризиків. У матеріалах Allianz зазначено, що поєднання внутрішніх даних страховика, даних третіх сторін і показників, які надходять у режимі реального часу від сенсорних пристроїв, дає змогу формувати повніші профілі ризику. Методи машинного навчання і штучного інтелекту можуть застосовуватися для виявлення закономірностей у накопичених даних, підтримки прийняття рішень та прогнозування несприятливих подій. Як окремий приклад наведено використання геопросторових даних для визначення ризику повеней. Отже, поєднання методів машинного навчання, геоінформаційних технологій і даних моніторингу створює можливості для автоматизованого оброблення значних масивів різнорідної інформації, уточнення характеристик ризику та інформаційної підтримки страхових рішень [92].

Розглянуті практичні приклади підтверджують можливість застосування спеціалізованих платформ, машинного навчання, штучного інтелекту, геоінформаційних технологій і засобів моніторингу для збирання та оброблення даних у страхових процесах [91, 92]. Водночас використання окремих технологічних рішень не забезпечує системного представлення взаємозв'язків між технологіями, процесами оцінювання кіберризиків і процесами кіберстрахування.

У попередньому дослідженні автора запропоновано трикомпонентну п'ятирівневу модель впровадження інформаційних технологій у кіберстрахуванні в Україні [19, 69]. Структура моделі охоплює три взаємопов'язані компоненти, або домени: інформаційні технології та технічні рішення страхування; оцінювання страхових кіберризиків; інформаційні технології та технічні рішення кіберстрахування.

П’ятирівневе представлення моделі охоплює початковий, або хаотичний, повторюваний, встановлений, керований та оптимізований рівні зрілості застосування інформаційних технологій у процесах кіберстрахування. Така структура дає змогу перейти від фіксації факту використання окремих технологій до оцінювання послідовності їх впровадження та рівня розвитку відповідних процесів [19].

Для характеристики рівня розвитку та впровадження процесів кіберстрахування у попередньому дослідженні автора запропоновано концепцію індексу зрілості кіберстрахування [19, 69]. До його можливих показників віднесено кількість або частку впроваджених процесів кіберстрахування; рівень зрілості та результативності цих процесів; рівень інтеграції інформаційних технологій у процеси кіберстрахування; а також зміни результатів діяльності після впровадження відповідних технологій.

На цьому етапі індекс зрілості кіберстрахування розглядався як концептуальний багатодоменний показник високого рівня. Деталізацію його структури, складу показників і процедур оцінювання було визначено напрямом подальших досліджень [19]. Це сформувало передумови для розроблення моделі оцінювання ризиків і зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model, RA&CIMM).

Запропонований підхід розвиває індексні методи, розглянуті у підрозділі 1.4. Якщо індекси кібербезпеки характеризують стан безпеки або захищеності об’єкта, то індекс зрілості кіберстрахування характеризує рівень розвитку та впровадження відповідних процесів. Тому комплексне оцінювання у предметній області кіберстрахування потребує врахування двох взаємопов’язаних груп характеристик: характеристик кіберризику й стану кіберзахисту та характеристик зрілості процесів кіберстрахування [37].

Результати попередніх досліджень автора відображають послідовний розвиток наукової задачі. На першому етапі досліджено можливості застосування індексів кібербезпеки та формування системи базисних параметрів [9, 10]. Надалі

обґрунтовано методологічні засади індексу кіберрезильєнтності та розглянуто оцінювання стану кіберзахисту з використанням базових індикаторів [11, 67]. Наступним етапом стала систематизація стандартизованих процесів кіберстрахування, придатних до формалізації й алгоритмізації, та дослідження інформаційних технологій, що можуть застосовуватися у відповідних процесах [13, 19, 68, 69].

Проведений аналіз показує, що в попередніх дослідженнях сформовано окремі методичні підходи до оцінювання стану кібербезпеки, системи показників та індикаторів, індексні методи агрегування даних, систематизовану сукупність процесів кіберстрахування та перелік інформаційних технологій для їх підтримки [13, 19, 37, 64]. Водночас залишається нерозв'язаною задача узгодженого поєднання цих складових у межах єдиного процесу оцінювання та інформаційної підтримки прийняття рішень у кіберстрахуванні.

Розв'язання зазначеної задачі потребує формалізації структури вхідних даних і взаємозв'язків між показниками, визначення процедур їх збирання, перевірки, нормування, групування й агрегування, а також розроблення взаємопов'язаних моделей, методів та алгоритмів, придатних до подальшої програмної реалізації. Така постановка відповідає головній науковій ідеї дисертації — формуванню методологічної та алгоритмічної основи інформаційної технології оцінювання й індексації операційних ризиків у кіберпросторі для підтримки прийняття рішень у процесах кіберстрахування.

Таким чином, аналіз інформаційних технологій і процесів кіберстрахування підтверджує необхідність переходу від розрізненого використання окремих показників, індексів і технологічних засобів до формалізованої системи оцінювання операційних ризиків у кіберпросторі. Така система має забезпечувати збирання, представлення, перевірку й оброблення різнорідних даних, групування показників за визначеними областями оцінювання, формування доменних оцінок та інтегральної оцінки, а також підготовку структурованої інформації для підтримки прийняття рішень у процесах кіберстрахування.

Висновки до розділу 1

За результатами аналізу проблеми та сучасного стану досліджень у сфері оцінювання операційних ризиків у кіберпросторі сформульовано такі висновки.

1. Встановлено, що цифровізація операційних процесів посилює залежність функціонування організацій від стану інформаційних і комп'ютерних систем, цифрових сервісів та інформаційних ресурсів. Реалізація кіберзагроз може призводити не лише до порушення конфіденційності, цілісності й доступності інформації, а й до порушення або припинення операційних процесів, втрати доступу до інформаційних ресурсів, необхідності проведення відновлювальних заходів і виникнення фінансових втрат. Це зумовлює необхідність розгляду кіберризику з урахуванням його можливого впливу на операційну діяльність організації.

2. Обґрунтовано доцільність розгляду кіберризику як складової операційного ризику у випадках, коли реалізація кіберзагрози спричиняє негативні наслідки для операційних процесів організації. У межах дисертаційного дослідження операційний ризик у кіберпросторі визначено як ризик виникнення негативних наслідків для операційних процесів організації унаслідок реалізації кіберзагроз, порушення функціонування інформаційних і комп'ютерних систем або недостатньої результативності організаційних і технічних заходів інформаційної безпеки та кіберзахисту. Встановлено, що оцінювання такого ризику потребує врахування взаємопов'язаної сукупності характеристик кіберзагроз, кіберінцидентів, інформаційних активів, стану кіберзахисту, процесів управління ризиками та можливих операційних наслідків.

3. Встановлено, що для оцінювання кіберризиків і стану кібербезпеки застосовуються методи статистичного спостереження й оброблення даних про кіберподії, системи базисних параметрів та індикаторів, моделі оцінювання стану кіберзахисту, доменна декомпозиція об'єкта оцінювання, моделі зрілості,

індексні, кількісні та ймовірнісні методи. У попередніх дослідженнях автора сформовано систему базисних параметрів, що охоплює індикатори кіберінцидентів, кібератак і кіберзагроз, а також показники заходів кіберзахисту. Різнорідність відповідних показників ускладнює їх безпосереднє зіставлення й агрегування та потребує формалізованого представлення структури вхідних даних.

4. Встановлено, що індексний підхід дає змогу структурувати, нормувати, групувати й агрегувати множину різнорідних показників. За результатами узагальнення попередніх досліджень визначено таку послідовність індексного оцінювання:

об'єкт оцінювання → система показників та індикаторів → збирання і перевірка даних → структурування та групування → нормування і приведення значень до зіставного вигляду → агрегування → індексна оцінка → інтерпретація результату.

Автоматизація зазначеної послідовності потребує формального визначення структури вхідних даних, правил їх перевірки й оброблення, а також процедур формування доменних оцінок та інтегральної оцінки.

5. На основі положень ISO/IEC 27102:2019 та аналізу практик кіберстрахування систематизовано дев'ять специфічних процесів кіберстрахування. Встановлено, що процеси оцінювання кіберризиків, збирання інформації про інформаційні активи, типізації кіберінцидентів та андеррайтингу можуть бути представлені як послідовності операцій зі збирання, перевірки, структуризації, оброблення, агрегування та інтерпретації даних. Систематизовано інформаційні технології, які застосовуються або можуть застосовуватися для підтримки відповідних процесів. Аналіз трикомпонентної п'ятирівневої моделі впровадження інформаційних технологій у кіберстрахуванні створив передумови для подальшого формування підходу до оцінювання зрілості процесів кіберстрахування.

6. Встановлено, що наявні підходи окремо забезпечують оцінювання стану кібербезпеки, аналіз кіберризиків, визначення рівня зрілості процесів або формування окремих індексних оцінок. Водночас для підтримки прийняття рішень у процесах кіберстрахування необхідне узгоджене використання різнорідних показників у межах єдиної формалізованої структури оцінювання. Це зумовлює необхідність розроблення взаємопов'язаних моделей, методів та алгоритмів, що забезпечують структуризацію показників за логічними областями оцінювання, оброблення різнорідних даних, а також формування доменних оцінок та інтегральної оцінки.

7. За результатами розділу сформульовано наукову задачу формалізації процесу оцінювання операційних ризиків у кіберпросторі шляхом структуризації, представлення та оброблення різнорідних даних, а також розроблення методів їх індексного агрегування для інформаційної підтримки прийняття рішень у процесах кіберстрахування. Для розв'язання цієї задачі в наступному розділі необхідно сформувати систему базисних параметрів, розробити модель доменної структуризації показників та індикаторів і обґрунтувати принципи формування піддоменних і доменних індексів та інтегрального індексу.

РОЗДІЛ 2. МОДЕЛІ ТА МЕТОДИ ІНДЕКСНОГО ОЦІНЮВАННЯ ОПЕРАЦІЙНИХ РИЗИКІВ У КІБЕРПРОСТОРІ

2.1. Загальні положення та концептуальна постановка задач дослідження

За результатами аналізу, проведеного в першому розділі, встановлено, що оцінювання операційних ризиків у кіберпросторі потребує оброблення значної кількості різнорідних показників. Вони характеризують кіберінциденти, кібератаки, кіберзагрози, вразливості, інформаційні активи, заходи інформаційної безпеки та кіберзахисту, процеси управління ризиками й можливі наслідки для операційної діяльності організації. Використання окремих показників не забезпечує комплексного представлення стану об’єкта оцінювання, оскільки кожен із них характеризує лише окрему складову операційного ризику в кіберпросторі.

Вхідні дані можуть мати кількісну, якісну, категоріальну або текстову форму, надходити з різних джерел, використовувати різні одиниці вимірювання та характеризувати різні часові періоди. Частина даних збирається за результатами статистичного спостереження, частина формується під час самооцінювання або експертного оцінювання, а окремі технічні дані можуть надходити від засобів моніторингу інформаційної безпеки. Різнорідність таких даних ускладнює їх безпосереднє зіставлення, спільне оброблення та використання для формування узагальненої оцінки.

У межах дисертаційного дослідження індексне оцінювання розглядається як упорядкований інформаційний процес, що охоплює визначення структури вхідних даних, формування системи параметрів та індикаторів, перевірку і приведення їх значень до зіставного вигляду, групування, нормування, зважування, агрегування та інтерпретацію одержаних результатів. Таке

представлення забезпечує перехід від множини окремих відомостей про стан об’єкта до формалізованих доменних оцінок та інтегральної оцінки.

Методологічну основу індексного оцінювання операційних ризиків у кіберпросторі становить поєднання системного, статистичного та індексного підходів. Системний підхід використовується для визначення структури об’єкта оцінювання, взаємозв’язків між його характеристиками та ієрархії показників. Статистичний підхід забезпечує організацію спостереження, збирання, накопичення, групування, оброблення й аналізу даних. Індексний підхід застосовується для приведення різнорідних показників до зіставного вигляду та формування піддоменних і доменних індексів та інтегрального індексу.

Статистичне дослідження передбачає послідовне проведення статистичного спостереження, зведення і групування одержаних даних, формування узагальнювальних показників, а також аналіз та інтерпретацію результатів. До таких показників належать середні й відносні величини, показники варіації та динаміки, статистичні індекси й рейтинги [7]. Їх застосування дає змогу досліджувати структуру, співвідношення та зміни сукупностей даних про процеси й події у кіберпросторі.

Початковим етапом організації статистичного та індексного оцінювання є формування системи базисних параметрів. Базисні параметри визначають склад і структуру даних, що підлягають збиранню та подальшому обробленню. У попередньому дослідженні автора запропоновано модель статистичної системи індексів, базисними параметрами якої визначено індикатори кіберінцидентів, кібератак і кіберзагроз, а також показники заходів кіберзахисту [10]. Зазначені групи утворюють початкову систему параметрів для опису стану кібербезпеки та подальшої структуризації показників операційних ризиків у кіберпросторі.

Формування системи базисних параметрів забезпечує перехід від неструктурованої множини відомостей до визначеної структури даних. Після встановлення складу параметрів здійснюються збирання та перевірка даних, їх накопичення, групування, оброблення й аналіз. З позицій комп’ютерних наук така

послідовність визначає структуру вхідних даних і створює передумови для формалізації та алгоритмізації процедур оцінювання.

Індексний підхід застосовується для дослідження складних сукупностей, елементи яких не підлягають безпосередньому підсумовуванню. Індекс у цьому разі є узагальненим результатом оброблення визначеної множини показників відповідно до встановленої процедури. Застосування індексного підходу дає змогу зіставляти стан об'єктів у просторі й часі, визначати відмінності між окремими складовими, оцінювати ступінь наближення до цільового або нормативного стану та формувати узагальнене представлення результатів оцінювання [7].

Практичні аспекти застосування індексів кібербезпеки для оцінювання стану інформаційної безпеки об'єктів критичної інфраструктури та формування індексу кіберрезильєнтності розглянуто в попередніх працях автора [9, 11].

У статистичній теорії за ступенем охоплення елементів сукупності розрізняють індивідуальні та загальні індекси. Індивідуальний індекс характеризує зміну окремого елемента сукупності. Загальний індекс характеризує зміну складної сукупності в цілому або її окремої групи. Однією з форм загального індексу є агрегатний індекс, у якому різнорідні елементи приводяться до зіставного вигляду із застосуванням визначених співвимірників або вагових характеристик [7]. У межах дисертаційного дослідження для груп показників, об'єднаних відповідним доменом або піддоменом, використовуються підіндекси, а для узагальненого представлення результатів оцінювання — інтегральний індекс.

Можливість формування індексної оцінки залежить від способу представлення первинних даних, показників та індикаторів. Кількісні дані можуть використовуватися після перевірки, за потреби — перетворення та приведення до встановленої шкали. Для якісних, категоріальних і текстових даних необхідно визначити правила числового кодування. Після цього значення відповідних показників можуть бути нормовані, згруповані й агреговані згідно зі

структурою моделі оцінювання. Правила оброблення даних мають також визначати порядок роботи з пропущеними, невизначеними, множинними та непридатними для оцінювання значеннями.

Для структуризації різнорідних показників застосовується доменна декомпозиція об’єкта оцінювання. Домен визначає логічно виокремлену область оцінювання, у межах якої об’єднуються функціонально пов’язані показники та індикатори. За необхідності домен поділяється на піддомени, що забезпечують додаткову деталізацію відповідної області. Таким чином, структурна модель показників може бути представлена як ієрархічна система, що охоплює об’єкт оцінювання, домени, піддомени, показники та індикатори [39, 66, 67].

Доменна структура створює основу для формування оцінок окремих областей і відповідних доменних індексів. Сукупність доменних оцінок утворює профіль стану об’єкта, який дає змогу виявляти відмінності між окремими складовими, визначати проблемні області та порівнювати поточний і цільовий стани. Подальше агрегування доменних індексів забезпечує формування інтегрального індексу об’єкта оцінювання.

Інтегральна оцінка не замінює аналізу окремих доменів, піддоменів, показників та індикаторів. Для обґрунтованої інтерпретації результатів необхідно забезпечити простежуваність усіх етапів перетворення — від первинних даних до піддоменних і доменних індексів та інтегрального індексу. Отже, модель оцінювання має одночасно забезпечувати узагальнення результатів і можливість їх подальшої деталізації.

Концептуальна постановка задачі індексного оцінювання операційних ризиків у кіберпросторі охоплює три взаємопов’язані рівні:

1) Вхідний рівень, на якому формується структурована множина даних про кіберінциденти, кібератаки, кіберзагрози, вразливості, інформаційні активи, заходи інформаційної безпеки та кіберзахисту, процеси управління ризиками й можливі операційні наслідки.

2) Рівень оброблення, що охоплює перевірку даних, числове кодування, нормування, групування показників за доменами й піддоменами, визначення вагових коефіцієнтів та агрегування.

3) Рівень формування результатів, на якому обчислюються піддоменні й доменні індекси, формується профіль стану об’єкта та визначається інтегральний індекс із подальшою інтерпретацією одержаних результатів.

До основних вимог до процесу індексного оцінювання належать структурованість і повнота вхідних даних, зіставність показників, відтворюваність обчислень, простежуваність перетворення даних, збереження ієрархії результатів та можливість повторного оцінювання. Дотримання цих вимог створює передумови для алгоритмізації процедур збирання, перевірки, кодування, нормування, групування, зважування й агрегування даних.

У предметній області кіберстрахування результати індексного оцінювання можуть використовуватися для формування структурованої інформації про стан об’єкта оцінювання, рівень операційних ризиків у кіберпросторі, стан інформаційної безпеки й кіберзахисту та зрілість відповідних процесів. Така інформація може застосовуватися для попереднього визначення страхової прийнятності, обґрунтування подальших процедур оцінювання, визначення пріоритетних заходів кіберзахисту та напрямів удосконалення процесів кіберстрахування. Остаточне страхове рішення має прийматися уповноваженими особами з урахуванням результатів оцінювання, підтверджених даних та інших страхових, правових, фінансових і актуарних чинників.

Відповідно до концептуальної постановки в межах розділу необхідно розв’язати такі взаємопов’язані задачі: сформувати систему базисних параметрів оцінювання кіберінцидентів, кібератак, кіберзагроз і заходів кіберзахисту; провести порівняльний аналіз моделей оцінювання стану кіберзахисту з використанням базових індикаторів кібербезпеки; сформувати модель доменної структуризації показників та індикаторів; обґрунтувати принципи формування

піддоменних, доменних та інтегрального індексів. Послідовність розв'язання зазначених задач визначає структуру наступних підрозділів.

Результати, одержані в розділі 2, формують методологічну основу для подальшої формалізації інформаційних процесів кіберстрахування у третьому розділі, розроблення RA&CIMM, методу формування підіндексів та інтегрального індексу й алгоритму багаторівневого оцінювання у четвертому розділі, а також пілотної апробації окремих методичних та алгоритмічних положень у п'ятому розділі.

2.2. Система базисних параметрів оцінювання кіберінцидентів, кібератак, кіберзагроз та заходів кіберзахисту

Визначення системи показників є одним із основних етапів підготовки даних для статистичного та індексного оцінювання. Під час дослідження процесів і подій у кіберпросторі ця задача ускладнюється значною кількістю характеристик, які описують кіберінциденти, кіберзагрози, способи реалізації негативного впливу та заходи протидії [10, 93]. Відповідні характеристики можуть мати різне походження, зміст, формат і одиниці вимірювання, що потребує їх попередньої систематизації та формалізованого представлення.

У попередньому дослідженні автора базисні параметри визначено як основу підготовки даних у межах статистичного підходу [10]. Вони встановлюють склад і структуру характеристик досліджуваної сукупності та виконують системоутворювальну функцію для відповідної статистичної системи. Формування системи базисних параметрів дає змогу структурувати різнорідні показники та створює основу для їх подальшого приведення до зіставного вигляду, оброблення й індексного агрегування.

Для оброблення даних про процеси та події у кіберпросторі в попередньому дослідженні автора запропоновано модель статистичної системи індексів, яка охоплює відомості про кіберінциденти, кібератаки, кіберзагрози та заходи протидії [10, 94]. У межах цієї моделі визначено чотири групи базисних параметрів:

1) індикатори кіберінцидентів;
2) індикатори кібератак;
3) індикатори кіберзагроз;
4) показники заходів кіберзахисту.

Зазначені групи утворюють початкову систему базисних параметрів для структурованого представлення та подальшого оброблення різнорідних даних.

Формування системи базисних параметрів здійснювалося з урахуванням положень Національної системи оцінювання кіберінцидентів Агентства з кібербезпеки та захисту інфраструктури США (CISA National Cyber Incident Scoring System, NCISS) [65], класифікації кіберінцидентів Організації з безпеки і співробітництва в Європі [56], підходу NIST Cyber Risk Scoring [62], показників кіберрезильєнтності MITRE [63], індикаторів інформаційної безпеки ETSI [57], положень ISO/IEC 27004:2016 щодо моніторингу, вимірювання, аналізу й оцінювання інформаційної безпеки [58], а також Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури [95].

Першу групу базисних параметрів утворюють індикатори кіберінцидентів. У межах статистичного дослідження кіберінцидент розглядається як подія, відомості про яку можуть бути зафіксовані, класифіковані та включені до статистичної сукупності. Відповідні індикатори призначені для структурованого опису характеристик зафіксованих кіберінцидентів і забезпечують можливість їх подальшого групування, оброблення та аналізу [56, 65].

Використання індикаторів кіберінцидентів забезпечує перехід від опису окремої події до формування структурованої сукупності даних про кіберінциденти. У межах статистичного підходу це дає змогу застосовувати

методи статистичного спостереження, зведення і групування даних, формування узагальнювальних показників, а також аналізу та інтерпретації одержаних результатів [7, 10].

Другу групу базисних параметрів утворюють індикатори кібератак. На відміну від індикаторів кіберінцидентів, які характеризують зафіксовані події та їх наслідки, індикатори кібератак описують способи, етапи й характеристики здійснення негативного впливу. Використання цієї групи дає змогу систематизувати дані за способами реалізації такого впливу та сформувати структуровану сукупність відомостей про кібератаки [10].

У базовому дослідженні для ілюстрації цієї групи розглянуто збирання відомостей про хости, служби й облікові записи, перехоплення та аналіз мережевого трафіку, а також застосування методів соціальної інженерії [10]. Зазначені дії можуть характеризувати розвідувальні або підготовчі етапи кібератаки та способи одержання інформації, необхідної для подальшої реалізації негативного впливу. Виокремлення відповідної групи індикаторів забезпечує можливість групування даних і дослідження структури та динаміки кібератак.

Третю групу базисних параметрів становлять індикатори кіберзагроз. Їх виокремлення зумовлене необхідністю врахування потенційних чинників негативного впливу на інформаційні ресурси, інформаційні і комп'ютерні системи. Представлення кіберзагроз як окремої групи параметрів дає змогу відмежувати відомості про потенційні джерела та умови негативного впливу від даних про зафіксовані кіберінциденти і способи здійснення кібератак [3, 10, 44].

Розмежування індикаторів кіберінцидентів, кібератак і кіберзагроз у межах системи базисних параметрів запобігає змішуванню різних за змістом категорій даних. Це забезпечує формування окремих структурованих сукупностей даних для їх подальшого групування, оброблення, аналізу та використання під час оцінювання операційних ризиків у кіберпросторі.

Четверту групу базисних параметрів становлять показники заходів кіберзахисту. Їх включення до статистичної системи індексів забезпечує

врахування не лише відомостей про кіберінциденти, кібератаки та кіберзагрози, а й даних про організаційні й технічні заходи, спрямовані на запобігання негативному впливу, реагування на нього та відновлення після його реалізації. Таким чином забезпечується формалізоване представлення як чинників операційного ризику в кіберпросторі, так і засобів його зменшення [3, 10, 95].

Таким чином, запропонована система базисних параметрів охоплює чотири взаємопов'язані, але різні за функціональним призначенням групи даних. Індикатори кіберінцидентів характеризують зафіксовані події; індикатори кібератак — способи та характеристики здійснення негативного впливу; індикатори кіберзагроз — потенційні чинники такого впливу; показники заходів кіберзахисту — засоби та дії, спрямовані на запобігання негативному впливу, реагування на нього та відновлення після його реалізації [10].

Формування системи базисних параметрів для статистичного та індексного оцінювання кіберінцидентів, кібератак, кіберзагроз і заходів кіберзахисту є передумовою організації статистичного спостереження за відповідними процесами. Подальше оброблення даних передбачає їх збирання, перевірку, систематизацію, зберігання, групування та аналіз із формуванням структурованих наборів даних, придатних для обчислення статистичних та індексних показників [7, 10].

Узагальнену структуру системи базисних параметрів статистичного та індексного оцінювання наведено в табл. 2.1.

Таблиця 2.1 — Система базисних параметрів статистичного та індексного оцінювання

Група базисних параметрів	**Об'єкт характеристики**	**Призначення в системі оцінювання**
Індикатори кіберінцидентів	Зафіксовані кіберінциденти	Структуроване представлення, групування та аналіз даних про кіберінциденти
Індикатори кібератак	Способи та характеристики здійснення негативного впливу	Систематизація, групування та аналіз даних про кібератаки

Індикатори кіберзагроз	Потенційні чинники негативного впливу	Формування та аналіз структурованої сукупності даних про кіберзагрози
Показники заходів кіберзахисту	Організаційні й технічні заходи та засоби кіберзахисту	Урахування заходів, спрямованих на запобігання негативному впливу, реагування на нього та відновлення після його реалізації

Джерело: розроблено автором.

2.3. Моделі оцінювання стану кіберзахисту з використанням базових індикаторів кібербезпеки

Подальший розвиток системи базисних параметрів пов'язаний із визначенням способів організації показників та індикаторів у моделях оцінювання стану кіберзахисту. Для цього в попередніх дослідженнях автора проведено порівняльний аналіз моделей, а також нормативних і методичних документів, що містять структуровані набори вимог, показників та індикаторів кібербезпеки [39, 66, 67, 95–99].

У межах аналізу розглянуто модель зрілості спроможностей у сфері кібербезпеки Cybersecurity Capability Maturity Model (C2M2), модель зрілості інтелектуальних електричних мереж Smart Grid Maturity Model (SGMM), нормативні й методичні документи України, умовно позначені за номерами відповідних актів як «1176», «601», «463», «417» і «375», а також модель оцінювання зрілості кібербезпеки електричних мереж «908» та узагальнювальну модель локального індексу кібербезпеки (Local Cybersecurity Index, LCSI) [39, 66, 67, 95–99]. Розгляд SGMM у національному контексті також узгоджується з Концепцією впровадження «розумних мереж» в Україні до 2035 року, якою визначено основні напрями технологічного розвитку відповідної енергетичної інфраструктури [100]. Досвід застосування системного аналізу, індикативного оцінювання та інтегральних показників до складних характеристик енергетичної безпеки представлено також у працях українських дослідників [101, 102].

Відповідні підходи підтверджують доцільність багаторівневої структуризації показників, однак їхні конкретні індикатори й вагові значення безпосередньо до RA&CIMM не переносяться.

Практичне застосування такого підходу реалізовано Міністерством енергетики США в межах Cybersecurity Capability Maturity Model (C2M2). Офіційний інструмент самооцінювання C2M2 забезпечує структуроване оцінювання 356 практик кібербезпеки, об'єднаних у десять доменів, визначення рівнів зрілості за кожним доменом та автоматизоване формування звіту з профілем досягнутих рівнів, виявленими прогалинами і напрямами подальшого вдосконалення. У сформованому інструментом звіті результати самооцінювання використовуються для визначення поточного стану, порівняння його з цільовим профілем, пріоритизації заходів і проведення повторного оцінювання [39, 40]. Це підтверджує практичну придатність доменного структурування показників, їх формалізованого оцінювання та подання результатів у вигляді профілю зрілості. У цьому дисертаційному дослідженні зазначену загальну логіку розвинено для задач кіберстрахування шляхом поєднання оцінювання кіберризиків, технічного стану інформаційно-комунікаційної системи та зрілості процесів кіберстрахування в межах RA&CIMM.

Структура досліджених моделей і нормативно-методичних підходів може бути представлена через N_D доменів, що визначають логічні області оцінювання, та N_I показників, параметрів або індикаторів, які оцінюються за N_L рівнями зрілості. В окремих підходах додатково передбачено N_{sD} піддоменів або цілей оцінювання. Кількісні характеристики наборів параметрів, досліджених у попередній роботі автора, наведено в табл. 2.2 [67].

Таблиця 2.2 — Кількісні характеристики наборів параметрів моделей і нормативно-методичних підходів до оцінювання стану кіберзахисту

Модель або нормативно-методичний підхід	**Умовне позначення**	**N_D**	**N_{sD}**	**N_I**	**N_L**
Cybersecurity Capability Maturity Model, version 2.1	C2M2	10	43	356	4
Smart Grid Maturity Model, version 1.2	SGMM	8	40	178	6
Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом	«1176»	6	–	29	2
Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури	«601»	5	23	108	4
Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами	«463»	2	23	107	5
Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури	«417»	5	23	102	4
Порядок огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури	«375»	13	–	–	2
Модель оцінювання зрілості кібербезпеки електричних мереж	«908»	10	43	356	4
Модель локального індексу кібербезпеки	LCSI	3	82	503	2

Примітка. N_D — кількість доменів; N_{sD} — кількість піддоменів або цілей оцінювання; N_I — кількість показників, параметрів або індикаторів; N_L — кількість рівнів оцінювання.

Порівняння кількісних характеристик моделей і нормативно-методичних підходів свідчить про істотні відмінності в кількості доменів, піддоменів, індикаторів та рівнів оцінювання. Кількість доменів у досліджених підходах становить від 2 до 13, а кількість індикаторів у тих із них, для яких цей показник визначено, — від 29 до 503.

Застосування розгорнутих моделей, що містять значну кількість показників та індикаторів, ускладнює оперативне оцінювання стану кіберзахисту великої

кількості об’єктів. Для зменшення обсягу даних, необхідних для такого оцінювання, запропоновано використовувати скорочений набір базових індикаторів кібербезпеки, відібраних експертним шляхом із загального переліку індикаторів відповідної моделі. Це дає змогу знизити трудомісткість збирання й оброблення даних та збільшити кількість об’єктів спостереження [67].

Основним результативним показником розглянутих моделей є рівень захищеності або зрілості кібербезпеки об’єкта оцінювання. Індикатор моделі являє собою формалізовану характеристику визначеного показника або параметра, встановленого в межах відповідної моделі. Індикатори можуть бути подані числовими значеннями або у формі тверджень, позначених текстовими або умовними ідентифікаторами [67].

Для індикаторів, поданих у формі тверджень, може застосовуватися процедура чисельної індикації. Під чисельною індикацією розуміється встановлення відповідності між індикатором, що має форму твердження, та його числовим значенням або балом. Правила встановлення такої відповідності визначаються в межах відповідної моделі оцінювання. Зазначене положення відповідає опублікованому авторському підходу до оброблення базових індикаторів кібербезпеки [67].

Індекс моделі формується шляхом агрегування числових значень індикаторів за визначеною процедурою. Залежно від структури моделі можуть обчислюватися індекси окремих доменів, піддоменів або інтегральний індекс моделі. Отже, необхідною передумовою індексного оцінювання є приведення первинних індикаторів до числової та зіставної форми.

Наявність індикаторів у формі тверджень зумовлює необхідність попереднього визначення шкали та правил їх оцінювання. Без чисельного подання таких індикаторів неможливо виконати їх математичне агрегування та сформувати індексну оцінку. Результати оцінювання можуть бути представлені у вигляді профілю захищеності або зрілості, що відображає значення індикаторів і рівні, досягнуті об’єктом оцінювання.

У проєкті «Методика оцінювання зрілості кібербезпеки та кіберстрахування електричних мереж» оцінювання передбачено здійснювати з використанням моделей зрілості кібербезпеки, моделей заходів кіберзахисту та моделей індексного оцінювання. Його метою є визначення поточного стану та вимірювання змін рівня кібербезпеки або кіберзахисту об'єкта оцінювання. До основних завдань віднесено оцінювання зрілості кібербезпеки, порівняння стану кіберзахисту різних організацій або однієї організації в різні періоди, оцінювання результативності обміну знаннями і практиками, а також визначення пріоритетності заходів та інвестицій [38, 67].

Оцінювання може здійснюватися із застосуванням моделей C2M2, SGMM і LCSI, а також підходів, сформованих на основі нормативних і методичних документів «1176», «601», «463», «417» та «375». Вибір конкретної моделі або підходу здійснюється суб'єктом оцінювання з урахуванням його мети, особливостей об'єкта, складу доступних даних і необхідного рівня деталізації [39, 66, 95–99].

Незважаючи на відмінності в цільовому призначенні та кількісній структурі, досліджені моделі й нормативно-методичні підходи ґрунтуються на спільному принципі: стан об'єкта оцінювання описується множиною показників або індикаторів, упорядкованих за логічними областями оцінювання. Залежно від структури відповідної моделі такі області можуть бути поділені на піддомени або цілі, а результати оцінювання — співвіднесені зі встановленими рівнями захищеності або зрілості.

Оцінювання стану кіберзахисту з використанням базових індикаторів запропоновано здійснювати за такою послідовністю:

1) формування структури оцінювання та визначення набору базових індикаторів кібербезпеки;

2) проведення самооцінювання суб'єктом оцінювання та формування поточного профілю захищеності або зрілості;

3) визначення цільового профілю та формування переліку політик і заходів, необхідних для його досягнення;

4) накопичення, систематизація й аналіз емпіричних даних;

5) проведення повторного оцінювання та визначення змін стану об’єкта оцінювання [67].

З погляду оброблення даних формування структури індикаторів визначає склад і спосіб подання вхідних параметрів; самооцінювання забезпечує збирання первинних даних та формування поточного профілю; визначення цільового профілю дає змогу встановити напрями вдосконалення; накопичення й аналіз емпіричних даних створюють інформаційну основу для повторного оцінювання. Порівняння результатів первинного і повторного оцінювання дає змогу визначити зміни стану кіберзахисту об’єкта.

Розглянуті моделі та підходи до використання базових індикаторів можуть застосовуватися, зокрема, для оцінювання стану кіберзахисту суб’єктів страхових відносин — страховиків і страхувальників. Використання скороченого набору базових індикаторів зменшує обсяг даних, необхідних для оцінювання, а їх доменна організація забезпечує структуризацію за логічними областями. Результатом оцінювання є профіль захищеності або зрілості, а за умови чисельного подання індикаторів — доменні індекси та інтегральний індекс.

2.4. Доменна структура та індексне подання результатів оцінювання

Результати аналізу моделей оцінювання стану кіберзахисту свідчать, що одним зі спільних принципів їх побудови є структуризація об’єкта оцінювання за логічно відокремленими областями — доменами. Кожен домен охоплює визначену сукупність взаємопов’язаних процесів, заходів, показників або

індикаторів, які характеризують окрему складову стану кібербезпеки або кіберзахисту [39, 66, 67].

Залежно від рівня деталізації моделі домени можуть поділятися на піддомени, цілі оцінювання або групи практик. Наступний рівень структури утворюють показники та відповідні їм індикатори, за значеннями яких визначається фактичний стан об'єкта оцінювання. У моделях зрілості додатково застосовуються рівні, що характеризують послідовні стани розвитку та керованості процесів кібербезпеки або кіберзахисту.

Узагальнену структуру моделі оцінювання можна представити так:

об'єкт оцінювання → домени → піддомени або цілі оцінювання → показники → індикатори → числові оцінки → піддоменні й доменні індекси → інтегральний індекс.

Одержані результати можуть бути представлені у вигляді профілю, який зберігає структуру значень за окремими індикаторами, піддоменами та доменами.

Домен визначає логічно відокремлену область оцінювання, яка об'єднує споріднені характеристики об'єкта. Піддомен деталізує відповідну область; показник характеризує певну властивість, процес або стан; індикатор містить значення, на підставі якого здійснюється оцінювання відповідного показника. Профіль відображає сукупність одержаних результатів за окремими складовими, а індексна оцінка формується шляхом агрегування числових значень індикаторів за встановленою процедурою.

Доменна організація показників забезпечує декомпозицію складного об'єкта оцінювання на взаємопов'язані складові. Це дає змогу оцінювати не лише стан об'єкта загалом, а й стан окремих областей його кібербезпеки або кіберзахисту, виявляти проблемні складові та формувати структурований профіль поточного стану.

У моделях, що охоплюють значну кількість показників та індикаторів, доменна структура виконує також функцію систематизації даних. Показники та індикатори об'єднуються відповідно до їх функціонального призначення і

належності до певних процесів, практик або заходів кіберзахисту. За результатами оцінювання можуть формуватися окремі доменні оцінки, сукупність яких відображає структуру стану об’єкта та може використовуватися для подальшого інтегрального оцінювання [67].

Необхідною умовою формування індексних оцінок є приведення результатів оцінювання індикаторів до порівнянної форми. Первинні індикатори можуть мати числове подання або бути сформульовані як твердження, відповідність яким визначається під час самооцінювання, експертного оцінювання або зовнішньої перевірки. Для подальшого математичного оброблення й агрегування значення таких індикаторів мають бути закодовані, нормовані та подані в межах встановленої шкали.

У проєкті «Методика оцінювання зрілості кібербезпеки та кіберстрахування електричних мереж» залежно від способу формування та подання результатів розрізнено автоматичний, синтетичний і аналітичний індекси кібербезпеки, а також індекс зрілості кібербезпеки [67].

Автоматичний індекс кібербезпеки формується шляхом алгоритмічного оброблення даних із застосуванням формалізованих процедур їх збирання, перевірки, нормування та агрегування. Результат подається у вигляді безрозмірного числового значення, що характеризує узагальнений стан кібербезпеки об’єкта оцінювання.

Синтетичний індекс кібербезпеки є інтегральним числовим значенням, сформованим шляхом агрегування сукупності індикаторів кібербезпеки відповідно до встановленої процедури. На відміну від автоматичного індексу, його формування не обов’язково передбачає автоматизоване отримання та оброблення всіх первинних даних.

Аналітичний індекс кібербезпеки являє собою комплексне інформаційно-аналітичне подання результатів оцінювання, що охоплює експертні, статистичні та інші відомості про стан кібербезпеки, рівень захищеності й можливі наслідки реалізації кіберзагроз. Індекс зрілості кібербезпеки, своєю чергою, є інтегральним

числовим значенням індикаторів, що характеризують рівень розвитку, впровадження та керованості процесів, практик і заходів кібербезпеки.

Розмежування зазначених типів індексів визначається способом отримання, оброблення та подання результатів. Аналітичний індекс забезпечує змістову інтерпретацію стану об’єкта на основі сукупності експертних, статистичних та інших відомостей. Синтетичний індекс передбачає формування узагальненого числового значення на основі встановленої системи індикаторів. Автоматичний індекс додатково потребує формалізованих процедур збирання, перевірки, нормування, оброблення й агрегування даних, придатних для алгоритмічної реалізації.

Доменна структура створює основу для формування доменних індексів. Доменний індекс характеризує стан окремої логічної області оцінювання та обчислюється на основі сукупності пов’язаних із нею числових значень індикаторів. Сукупність доменних індексів дає змогу сформувати профіль стану об’єкта, у якому відображаються відмінності між окремими складовими кібербезпеки або кіберзахисту.

Профіль оцінювання може використовуватися для представлення поточного та цільового станів об’єкта. Поточний профіль відображає фактичні результати оцінювання, тоді як цільовий профіль визначає значення показників і рівні, яких необхідно досягти внаслідок впровадження відповідних організаційних і технічних заходів. Порівняння поточного та цільового профілів забезпечує виявлення невідповідностей, визначення пріоритетних напрямів удосконалення та планування подальших дій.

Інтегральне індексне подання результатів не замінює аналізу окремих доменів, піддоменів та індикаторів. Інтегральний індекс характеризує загальний стан об’єкта оцінювання, однак не відображає повною мірою відмінностей між його складовими. Тому модель індексування має забезпечувати як узагальнення результатів, так і можливість їх послідовної деталізації до рівня доменів, піддоменів та окремих індикаторів.

Під час оцінювання операційних ризиків у кіберпросторі доменна структура дає змогу систематизувати різнорідні показники за функціональними областями та сформувати взаємопов'язану систему індикаторів. До її складу можуть входити індикатори кіберінцидентів, кібератак і кіберзагроз, показники заходів кіберзахисту, а також показники стану та зрілості відповідних процесів [10, 67].

Таким чином, доменна структура забезпечує ієрархічне подання об'єкта оцінювання, систематизацію різнорідних показників та індикаторів, формування профілів захищеності або зрілості й обчислення доменних індексів. Подальше узагальнення результатів потребує формування інтегрального індексу та визначення вагових коефіцієнтів, що забезпечують урахування відносної значущості окремих складових.

2.5. Формування доменних індексів та інтегрального індексу шляхом агрегування показників

Застосування індексного підходу до оцінювання складних об'єктів передбачає узагальнення сукупності різнорідних показників та індикаторів, що характеризують окремі складові досліджуваного явища. Для цього можуть використовуватися доменні й агрегатні індекси, які забезпечують подання результатів на різних рівнях узагальнення [7].

Доменний індекс охоплює сукупність функціонально пов'язаних показників та індикаторів, об'єднаних у межах окремої логічної області оцінювання. Його застосування дає змогу сформувати узагальнену числову оцінку відповідного домену або піддомену та порівняти стан окремих складових об'єкта оцінювання.

Агрегатний індекс призначений для узагальнення значень показників або доменних індексів, які можуть відрізнятися за змістом, шкалами та одиницями вимірювання. Для забезпечення їх порівнянності первинні значення мають бути попередньо нормовані. Під час агрегування можуть застосовуватися вагові коефіцієнти, що відображають відносну значущість окремих складових у формуванні загального результату.

Використання доменних та агрегатного індексів відповідає ієрархічній структурі моделі оцінювання. Спочатку на основі значень індикаторів формуються оцінки піддоменів або доменів, після чого доменні індекси можуть бути агреговані в інтегральний індекс моделі. Одночасне подання доменних індексів та інтегрального індексу забезпечує як узагальнену характеристику стану об'єкта, так і можливість визначення внеску його окремих складових.

Якщо первинні індикатори мають числове подання, на їх основі можуть формуватися доменні індекси та інтегральний індекс. Якщо індикатори не приведено до числової форми, результати можуть бути представлені у вигляді категоріального профілю, однак їх математичне агрегування та формування індексної оцінки неможливі без попереднього числового кодування.

Отже, можливість математичного агрегування визначається способом формалізації первинних даних.

У разі застосування двобальної шкали індикатор набуває значення 1, якщо фактичний стан об'єкта відповідає встановленому твердженню, та значення 0, якщо не відповідає йому. Для індикаторів, які потребують більшої деталізації, можуть застосовуватися багатобальні, порядкові або нормовані шкали. Правила присвоєння числових значень і критерії переходу між рівнями мають бути визначені в межах відповідної моделі [67].

За способом урахування відносної значущості індикаторів оцінка може бути простою або зваженою. Проста оцінка передбачає однаковий внесок усіх індикаторів у результат агрегування. Зважена оцінка формується із застосуванням

вагових коефіцієнтів, значення яких відображають відносну значущість окремих індикаторів, показників або доменів.

Використання вагових коефіцієнтів дає змогу врахувати, що окремі індикатори можуть характеризувати різні за значущістю процеси, заходи або чинники операційного ризику в кіберпросторі. Тому їхній внесок у доменну або інтегральну оцінку може відрізнятися. Спосіб визначення ваг, умови їх нормування та процедура застосування мають бути встановлені в межах відповідного методу індексного оцінювання.

Для кожного піддомену та домену формується відповідна індексна оцінка, а сукупність одержаних оцінок утворює профіль стану об’єкта. Інтегральний індекс відображає узагальнений результат оцінювання об’єкта загалом. Таке подання забезпечує одночасне отримання деталізованих та узагальнених результатів.

Групування індикаторів за доменами й піддоменами створює основу для формування піддоменних і доменних індексів. Кожен із цих індексів характеризує визначену складову об’єкта та дає змогу виявити відмінності між окремими областями оцінювання. Сукупність піддоменних і доменних індексів утворює профіль стану об’єкта та дає змогу визначити складові, які потребують додаткового аналізу або вдосконалення.

Агрегування часткових оцінок забезпечує формування інтегрального індексу, що характеризує стан об’єкта оцінювання загалом. Водночас інтегральний індекс має використовуватися разом із результатами оцінювання окремих доменів. Збереження ієрархічної структури результатів забезпечує можливість переходу від узагальненого значення до доменних оцінок і значень окремих індикаторів.

У задачах оцінювання операційних ризиків у кіберпросторі доменні індекси забезпечують узагальнення показників за окремими логічними областями, а інтегральний індекс — формування узагальненої оцінки об’єкта на основі різнорідних складових. Вагові коефіцієнти використовуються для врахування

відносної значущості окремих індикаторів і доменів у загальному результаті оцінювання.

Таким чином, формування доменних індексів та інтегрального індексу забезпечує послідовний перехід від значень окремих індикаторів до оцінок піддоменів і доменів та узагальненої оцінки об’єкта. Чисельна індикація дає змогу включати до процесу індексування показники, подані у формі тверджень, а застосування вагових коефіцієнтів — ураховувати відносну значущість окремих індикаторів і доменів у загальному результаті [67].

Поєднання системи базисних параметрів, доменної структури показників, процедур чисельної індикації, нормування та агрегування формує методологічну основу індексного оцінювання операційних ризиків у кіберпросторі. Одержані результати надалі використовуються для розроблення моделей, методів і алгоритмів оброблення різнорідних даних та інформаційної підтримки прийняття рішень у процесах кіберстрахування [10, 37, 67].

Висновки до розділу 2

У розділі розроблено методологічні положення індексного оцінювання операційних ризиків у кіберпросторі на основі поєднання системного, статистичного та індексного підходів. За результатами проведеного дослідження сформульовано такі висновки.

1. Сформовано концептуальну постановку задачі індексного оцінювання операційних ризиків у кіберпросторі. Визначено послідовність переходу від різнорідних вхідних даних до формалізованих результатів оцінювання, що охоплює структуризацію і перевірку даних, їх числове кодування, нормування, групування, визначення вагових коефіцієнтів та агрегування. Виокремлено три взаємопов’язані рівні цього процесу: рівень

вхідних даних, рівень їх оброблення та рівень формування результатів. Встановлено вимоги до структурованості й порівнянності вхідних даних, відтворюваності обчислень, простежуваності перетворень та збереження ієрархічної структури результатів оцінювання.

2. Сформовано систему базисних параметрів статистичного та індексного оцінювання процесів у кіберпросторі, що охоплює індикатори кіберінцидентів, кібератак і кіберзагроз, а також показники заходів кіберзахисту. Запропонована систематизація забезпечує розмежування даних про зафіксовані події, способи здійснення негативного впливу, потенційні чинники такого впливу та заходи, спрямовані на запобігання йому, реагування на нього і відновлення після його реалізації. Це створює основу для формування структурованих сукупностей даних, їх накопичення, оброблення, аналізу та подальшого індексного оцінювання.

3. За результатами порівняльного аналізу моделей і нормативно-методичних підходів до оцінювання стану кіберзахисту визначено спільні принципи організації показників та індикаторів. Досліджено моделі C2M2, SGMM і LCSI, модель оцінювання зрілості кібербезпеки електричних мереж «908», а також підходи, сформовані на основі нормативних і методичних документів «1176», «601», «463», «417» та «375». Встановлено, що вони відрізняються кількістю доменів, піддоменів, індикаторів і рівнів оцінювання, проте ґрунтуються на структуризації об’єкта за логічними областями. Обґрунтовано використання скороченого набору базових індикаторів кібербезпеки для зменшення обсягу вхідних даних і трудомісткості процедур оцінювання стану кіберзахисту.

4. Сформовано узагальнену доменну структуру подання результатів оцінювання, яка забезпечує перехід від об’єкта оцінювання через домени, піддомени або цілі оцінювання, показники та індикатори до профілю захищеності або зрілості, доменних індексів та інтегральної оцінки. Визначено особливості автоматичного, синтетичного й аналітичного подання індексів кібербезпеки, а

також індексу зрілості кібербезпеки. Показано, що доменна декомпозиція забезпечує формування поточного і цільового профілів об’єкта, а ієрархічна структура результатів дає змогу здійснювати перехід від інтегральної оцінки до оцінок окремих доменів, піддоменів та індикаторів.

5. Розроблено підхід до формування доменних індексів та інтегрального індексу на основі різнорідних показників операційних ризиків у кіберпросторі. Групування індикаторів за доменами й піддоменами створює основу для формування піддоменних і доменних індексів, а їх подальше агрегування — для одержання інтегрального індексу об’єкта оцінювання. Для врахування відносної значущості окремих складових передбачено використання вагових коефіцієнтів, спосіб визначення та застосування яких конкретизовано в межах методу, розробленого в четвертому розділі. Поєднання системи базисних параметрів, доменної структури, чисельної індикації, нормування та агрегування формує методологічну основу подальшої формалізації та алгоритмізації оцінювання операційних ризиків у кіберпросторі та зрілості процесів кіберстрахування.

Одержані результати формують методологічну основу для подальшої формалізації інформаційних процесів кіберстрахування та розроблення моделей, методів і алгоритмів збирання, оброблення й аналізу даних для підтримки прийняття рішень у процесах кіберстрахування, що розглядаються в наступних розділах дисертації.

РОЗДІЛ 3. МЕТОДИ ТА ІНФОРМАЦІЙНІ ПРОЦЕСИ ОЦІНЮВАННЯ РИЗИКІВ У КІБЕРСТРАХУВАННІ

3.1. Стандартизовані процеси кіберстрахування як об’єкти алгоритмізації та автоматизації

У другому розділі сформовано методологічні засади структуризації, формалізованого представлення та індексного оброблення різнорідних показників стану кібербезпеки й операційних ризиків у кіберпросторі. Подальше застосування цих засад у кіберстрахуванні потребує систематизації відповідних процесів, визначення джерел і структури вхідних даних, правил їх перевірки, операцій збирання, передавання, оброблення й аналізу, а також способів формування вихідних результатів. Тому в цьому розділі процеси кіберстрахування розглядаються як взаємопов’язані інформаційні процеси та об’єкти подальшої формалізації, алгоритмізації й автоматизації.

Питання страхування операційних ризиків у кіберпросторі, тобто кіберстрахування, є предметом досліджень вітчизняних і зарубіжних науковців. Теоретичні та методологічні засади управління страховими ризиками розглядали C. A. Williams, R. M. Heins, С. В. Волосович і Ю. М. Клапків [103–105]. Проблематику кіберризиків та їх страхування досліджували A. Marotta зі співавторами, S. Romanosky зі співавторами, R. Böhme і G. Schwartz, Р. В. Пікус і Ю. Л. Бабенко, L. A. Odell, J. C. Fauntleroy та R. R. Wagner [106–110]. У відповідних працях розглянуто теоретичні засади дослідження кіберризиків, особливості функціонування кіберстрахування, підходи до моделювання кіберризику, формування страхового покриття, а також збирання, оброблення та

використання даних про стан кібербезпеки для підтримки прийняття страхових рішень.

Окремий напрям досліджень становлять міжнародні стандарти, рекомендації та практики у сфері кіберстрахування й управління кіберризиками. Їх положення визначають підходи до оцінювання кіберризиків, інформаційної взаємодії між учасниками кіберстрахування, управління станом кібербезпеки та використання результатів оцінювання для підтримки прийняття страхових рішень [3, 5, 12, 16, 17, 20, 111, 112].

Водночас результати аналізу наукових праць, нормативних документів і практик застосування кіберстрахування свідчать, що основну увагу в них зосереджено на економічних, фінансових, організаційних і нормативних аспектах кіберстрахування, а також на застосуванні окремих технологічних засобів оцінювання кіберризиків [5, 12, 17, 20, 106]. У межах опрацьованого масиву джерел недостатньо дослідженими залишаються системне подання кіберстрахування як сукупності взаємопов'язаних інформаційних процесів, визначення їхніх вхідних і вихідних даних та операцій оброблення інформації, а також виокремлення процесів, придатних до формалізації, алгоритмізації й автоматизації. Необхідність розв'язання зазначеного науково-прикладного завдання стала підставою для систематизації стандартизованих процесів кіберстрахування та дослідження можливостей їх подальшої формалізації й автоматизації [13].

Автоматизація страхування та кіберстрахування реалізується із застосуванням інформаційних систем і спеціалізованих платформ, призначених для управління ризиками, опрацювання страхових подій і документів, аналізу статистичних даних та інформаційної підтримки прийняття рішень [19, 113]. Водночас автоматизація ізольованих сервісів не забезпечує системного подання кіберстрахування як сукупності взаємопов'язаних інформаційних процесів і не визначає структуру інформаційних зв'язків між ними. Тому необхідною передумовою розроблення відповідних моделей, методів і алгоритмів є

систематизація процесів кіберстрахування, визначення для кожного з них джерел і структури вхідних даних, правил їх перевірки, операцій оброблення та формування вихідних результатів [13].

Необхідність нормативного врегулювання страхування кіберризиків зумовила розроблення спеціалізованих стандартів у сфері страхування та інформаційної безпеки. У відповідних документах основну увагу приділено ідентифікації, визначенню пріоритетності й оцінюванню кіберризиків, а також інформаційній взаємодії учасників процесу страхування. Одним зі спеціалізованих міжнародних стандартів у досліджуваній предметній області є ISO/IEC 27102:2019 «Інформаційна безпека, кібербезпека та захист приватності. Настанови щодо кіберстрахування» (Information security, cybersecurity and privacy protection — Guidelines for cyber-insurance). Стандарт містить настанови щодо обміну інформацією між страховиком і страхувальником, оцінювання ризиків та врахування питань страхового покриття у процесах кіберстрахування [12].

В Україні нормативне регулювання страхової діяльності здійснюється відповідно до Цивільного кодексу України [114], законів України «Про страхування» [115], «Про фінансові послуги та фінансові компанії» [116], а також нормативно-правових актів Національного банку України [114–117]. У межах державного регулювання ринків небанківських фінансових послуг Національний банк України також уповноважений застосовувати коригувальні заходи, заходи раннього втручання та заходи впливу відповідно до встановленого нормативного порядку [118]. Для досліджуваної предметної області мають значення нормативні положення, якими визначено критерії встановлення профілю ризику надавачів фінансових послуг [119], характеристики та класифікаційні ознаки класів страхування й особливості укладання договорів за відповідними класами [120], порядок обліку страховиками договорів і вимоги до захисту інформації страховика [121]. Результати аналізу нормативної бази свідчать про врегулювання загальних процесів страхової діяльності, управління ризиками та захисту інформації страховика. Водночас спеціалізоване нормативне

забезпечення формалізації, алгоритмізації та автоматизації процесів кіберстрахування залишається недостатньо сформованим.

У міжнародних нормативно-методичних документах і матеріалах спеціалізованих організацій кіберстрахування розглядається з різних позицій. Федеральна торгова комісія США (Federal Trade Commission, FTC) визначає кіберстрахування як один із механізмів захисту суб'єктів господарювання від фінансових втрат, пов'язаних із кібератаками та порушеннями конфіденційності даних. Страхове покриття може включати витрати на юридичний захист, відновлення даних, інформування постраждалих осіб, компенсацію завданих збитків та інші витрати, пов'язані з наслідками кіберінцидентів [122].

Агентство Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity, ENISA) розглядає кіберстрахування як інструмент передавання та розподілу фінансових наслідків кіберризиків, пов'язаних із кібератаками, кіберінцидентами й порушеннями безпеки даних. Водночас значення кіберстрахування не обмежується компенсацією збитків: процедури оцінювання ризику, андеррайтингу та визначення умов страхового покриття можуть сприяти підвищенню обізнаності організацій щодо кіберризиків і впровадженню заходів їх зниження [20, 112].

Національний інститут стандартів і технологій США (National Institute of Standards and Technology, NIST) визначає функціональну основу управління кіберризиками, що охоплює керування, ідентифікацію, захист, виявлення, реагування та відновлення [3]. Отже, у міжнародних підходах кіберстрахування пов'язується з передаванням фінансових наслідків кіберризиків, управлінням ними та підвищенням кіберстійкості об'єкта страхування.

Відмінності у трактуванні кіберстрахування підтверджують комплексний характер цієї предметної області. Для завдань формалізації та автоматизації це має принципове значення, оскільки процеси кіберстрахування доцільно розглядати як сукупність взаємопов'язаних інформаційних процесів оцінювання й управління кіберризиками, обміну даними, андеррайтингу, управління

страховим покриттям та реагування на наслідки кіберінцидентів. Подання таких процесів має передбачати визначення джерел і структури вхідних даних, правил їх перевірки, операцій оброблення й аналізу, інформаційних зв'язків між процесами та способів формування вихідних результатів.

До нормативних і методичних документів, положення яких можуть використовуватися у процесах кіберстрахування, належать ISO/IEC 27102:2019 [12], Європейська рамка сертифікації кібербезпеки, визначена Регламентом (ЄС) 2019/881 [123], матеріали ENISA щодо розвитку, практик, моделей і проблем кіберстрахування [17, 20, 112], Рамкова основа кібербезпеки NIST (NIST Cybersecurity Framework, NIST CSF) [3], рекомендації IAIS щодо андеррайтингу кіберризиків [5], а також система Cyber Essentials Національного центру кібербезпеки Великої Британії та пов'язані з нею можливості отримання кіберстрахового покриття [111]. Перелік і характеристики відповідних документів та підходів систематизовано в попередньому дослідженні автора [13].

Базовим спеціалізованим стандартом у сфері кіберстрахування є ISO/IEC 27102:2019, який містить настанови щодо оцінювання кіберризиків, обміну інформацією між страховиком і страхувальником та врахування питань страхового покриття. Його положення передбачають використання даних про кіберризики, інформаційні активи, наявні засоби контролю та стан інформаційної безпеки у процесах взаємодії між учасниками кіберстрахування [12].

Європейська рамка сертифікації кібербезпеки, установлена Регламентом (ЄС) 2019/881, визначає механізми сертифікації кібербезпеки продуктів, послуг і процесів інформаційно-комунікаційних технологій та передбачає використання стандартизованих рівнів забезпечення довіри [123]. Відомості про наявність сертифікатів і встановлені рівні забезпечення довіри можуть використовуватися як структуровані вхідні дані під час оцінювання стану кібербезпеки об'єкта, пов'язаних із ним кіберризиків і прийняття андеррайтингових рішень.

У матеріалах ENISA проаналізовано сучасний стан ринку кіберстрахування, належні практики, проблеми оцінювання кіберризиків,

динаміку попиту, а також моделі й методи кіберстрахування та можливості застосування штучного інтелекту [17, 20, 112]. Результати цих досліджень підтверджують взаємозв'язок між розвитком кіберстрахування, удосконаленням методів оцінювання кіберризиків, використанням нових технологій оброблення даних і змінами нормативного середовища.

Рамкова основа кібербезпеки NIST версії 2.0 (NIST Cybersecurity Framework 2.0, NIST CSF 2.0) визначає шість взаємопов'язаних функцій управління кіберризиками: керування (Govern), ідентифікацію (Identify), захист (Protect), виявлення (Detect), реагування (Respond) та відновлення (Recover) [3]. Результати оцінювання за відповідними функціями можуть використовуватися для формування структурованого профілю стану кібербезпеки організації та як інформаційна основа для оцінювання кіберризиків і прийняття рішень у процесах кіберстрахування.

Документ IAIS «Issues Paper on Insurance Sector Operational Resilience» містить огляд наглядових практик у сферах операційної та кіберстійкості, залучення зовнішніх постачальників інформаційно-технологічних послуг, обміну інформацією та управління безперервністю діяльності [124]. Хоча цей документ безпосередньо не визначає процеси кіберстрахування, розглянуті в ньому складові можуть використовуватися для оцінювання операційної та кіберстійкості об'єкта страхування, формування відповідних вхідних даних і забезпечення прийняття андеррайтингових рішень.

Система Cyber Essentials поєднує перевірку впровадження базових технічних заходів кібербезпеки з можливістю отримання кіберстрахового покриття. Організації, зареєстровані у Великій Британії або на територіях Коронних володінь, із річним оборотом до 20 млн фунтів стерлінгів, які отримали сертифікат Cyber Essentials для всієї організації та погодилися на участь у програмі, мають право на відповідне страхове покриття. Такий підхід демонструє практичний зв'язок між перевіркою стану кібербезпеки, формуванням

структурованих відомостей про впроваджені засоби контролю та використанням результатів оцінювання у процесах кіберстрахування [111].

Порівняльний аналіз розглянутих стандартів, рамкових і методичних документів дав змогу визначити спільні положення, що мають значення для формалізації інформаційних процесів кіберстрахування.

По-перше, у досліджених документах оцінювання ризиків розглядається як основа для вибору способів їх подальшого оброблення. У процесах кіберстрахування результати оцінювання використовуються для визначення профілю кіберризику, обґрунтування потреби та обсягу страхового покриття, прийняття андеррайтингових рішень і формування заходів управління ризиком.

По-друге, у розглянутих документах кіберризики пов'язуються з операційними та фінансовими наслідками реалізації кіберзагроз. Для їх оцінювання необхідне спільне використання технічних характеристик об'єкта, відомостей про кіберзагрози, вразливості та засоби контролю, а також даних про можливі перерви в діяльності, витрати, збитки й інші фінансові наслідки. Це зумовлює потребу в інтегрованому обробленні різнорідних технічних, організаційних і фінансово-економічних даних.

По-третє, у стандартах і методичних документах застосовуються описи та класифікації кіберризиків, кіберзагроз і кіберінцидентів. Використання узгоджених класифікацій забезпечує структуроване представлення даних про джерела загроз, події, вразливості, засоби контролю та наслідки реалізації ризиків, а також створює передумови для їх кодування, порівняння й подальшого автоматизованого оброблення. Прикладом формалізованого зіставлення відомостей про кібератаки є рекомендації CISA щодо відображення спостережуваної поведінки атакувальників через тактики й техніки бази знань MITRE ATT&CK [125].

По-четверте, оцінювання кіберризиків має враховувати залежності від постачальників інформаційно-технологічних послуг, учасників ланцюгів постачання та інших суб'єктів інформаційної взаємодії. Відомості про такі

залежності, застосовувані засоби контролю, порушення функціонування та участь зовнішніх постачальників у реагуванні на кіберінциденти мають включатися до складу вхідних даних. Отже, межі об'єкта оцінювання можуть виходити за межі окремої організації та охоплювати пов'язані з нею інформаційні системи, процеси й зовнішніх учасників.

По-п'яте, у практиках кіберстрахування результати оцінювання кіберризиків використовуються для визначення умов страхового покриття, лімітів відповідальності, виключень із договору страхування та прийняття андеррайтингових рішень. Формування таких рішень потребує оброблення даних про об'єкт страхування, кіберзагрози, вразливості, наявні засоби контролю, можливі сценарії кіберінцидентів та очікувані наслідки їх реалізації.

По-шосте, процеси збирання, перевірки, передавання та оброблення даних про кіберризики потребують уніфікованих вимог до складу, структури, повноти й достовірності відповідної інформації. Інформаційна взаємодія між страхувальником, страховиком, брокерами, постачальниками послуг кібербезпеки та іншими учасниками кіберстрахування має забезпечувати узгоджене представлення даних про інформаційні активи, кіберризики, засоби контролю та наслідки кіберінцидентів. Це створює передумови для формалізації, алгоритмізації й автоматизації відповідних інформаційних процесів.

Таким чином, результати порівняльного аналізу нормативних і методичних документів дають змогу визначити ключову для подальшого дослідження особливість: процеси кіберстрахування ґрунтуються на збиранні, передаванні, перевірці, структурованому представленні, обробленні й аналізі різнорідних даних про об'єкт страхування, інформаційні активи, кіберризики, кіберінциденти, засоби контролю та наслідки реалізації загроз. Результати виконання відповідних операцій використовуються для формування профілю кіберризику, визначення умов страхового покриття, прийняття андеррайтингових та управлінських рішень. Це дає підстави розглядати процеси кіберстрахування

як взаємопов’язані інформаційні процеси та об’єкти подальшої формалізації, алгоритмізації й автоматизації.

Страхові компанії та спеціалізовані учасники ринку кіберстрахування застосовують інформаційно-комунікаційні технології й програмні засоби для автоматизації окремих процесів страхування та кіберстрахування. У попередньому дослідженні автора проаналізовано засоби, призначені для електронної взаємодії з клієнтами й брокерами, збирання та оброблення даних про кіберризики, підтримки андеррайтингу, моніторингу стану кібербезпеки та реагування на кіберінциденти [13]. Результати проведеного аналізу систематизовано в таблиці 3.1.

Таблиця 3.1 — Окремі інформаційно-комунікаційні засоби страхування та кіберстрахування

Компанія	**Інформаційно-комунікаційні засоби**	**Умовна оцінка CIM**
Coalition	Active Insurance: cyber-insurance; Tech Errors & Omissions; Executive Risks; Miscellaneous Professional Liability. Coalition Security: Coalition Control; Managed Detection & Response (MDR); Coalition Incident Response (CIR); Coalition Security Awareness Training	+++
At-Bay	cyber-risk Calculator; Primary & Excess Appetite eForm Guide; Miscellaneous Professional Liability Coverage Highlights eForm Guide; Managed Detection and Response Service Desk; Broker Platform	+
Cowbell Cyber	Adaptive cyber-insurance: Cowbell Prime 100, 100 PRO, 250, PLUS, ONE; Adaptive Technology Errors & Omissions; Incident Response Plan Template	+

Corvus Insurance	Smart cyber-insurance; Smart Tech EO; Appetite Guide; Application; Request Coverage Form; expert incident response and claims management	++
Beazley	Cyber Customer Centre; Risk Management Webinars; Incident Preparation Room; port scanning and monitoring; phishing testing; IRP Review; Broker Centre; API Trading; cyber-risk Management Tools; Managed eXtended Detection and Response (MXDR)	+++
Chubb	Individuals & Families Portal; Businesses Portal; Agents & Brokers Portal; Payment Center; Chubb Mobile App; Chubb Cyber Incident Response Team; Report a Claim eForm	++
AIG	Cyber Highlight Sheet; AIG Cyber Coverages; AIG Cyber Underwriting Application; Sample Client Cyber Maturity Report	+
AXA XL	XL GlobalClaim Customer Portal; Design Professional login portal; Learning Management System	+
CFC Underwriting	Cyber-insurance private enterprise application form; Ransomware Calculator; CFC mobile application for cyber	++
Liberty Mutual Insurance	Liberty Mutual application	–
Berkshire Hathaway Specialty Insurance	Electronic application forms	–

Примітка. CIM (Cyber Insurance Maturity) — умовна порівняльна оцінка зрілості кіберстрахування, використана в попередньому дослідженні автора. Більша кількість знаків «+» позначає відносно вищу функціональну насиченість виявленого комплексу інформаційно-комунікаційних засобів; знак «–» означає, що в межах проведеного аналізу спеціалізованих засобів кіберстрахування не виявлено. Наведена оцінка не є розрахованим інтегральним індексом зрілості кіберстрахування.

Джерело: адаптовано автором за [13].

Наведені в таблиці 3.1 дані свідчать про відмінності у функціональному призначенні та складі інформаційно-комунікаційних засобів, які застосовуються учасниками ринку кіберстрахування. Частина цих засобів призначена переважно для електронної взаємодії з клієнтами, брокерами та іншими учасниками страхового процесу. До них належать електронні форми, особисті кабінети й портали, мобільні застосунки, засоби подання заяв і повідомлень, а також інформаційні ресурси для супроводження договорів страхування.

Інша група засобів безпосередньо пов'язана зі збиранням та обробленням даних для оцінювання кіберризиків і підтримки андеррайтингу. До неї належать калькулятори кіберризику, електронні анкети й форми андеррайтингу, звіти про стан і зрілість кібербезпеки, а також інструменти аналізу та управління кіберризиками. Застосування таких засобів свідчить про перехід від автоматизації традиційних страхових операцій до автоматизації процесів отримання, перевірки, структурованого представлення та оброблення даних про кіберризики.

Комплексні рішення поєднують страхові сервіси з технічними засобами кібербезпеки. До них належать кероване виявлення та реагування (Managed Detection and Response, MDR), розширене кероване виявлення та реагування (Managed Extended Detection and Response, MXDR), засоби моніторингу й реагування на кіберінциденти, сканування інформаційних ресурсів, тестування стійкості до фішингових атак, аналіз планів реагування на інциденти та навчання з питань кібербезпеки. У такому разі дані про стан кібербезпеки можуть формуватися не лише за результатами анкетування або самооцінювання, а й у процесі автоматизованого моніторингу, виявлення подій та реагування на них.

Проведений аналіз засвідчив, що інформаційно-комунікаційні засоби кіберстрахування відрізняються за функціональним призначенням, складом операцій з даними та рівнем інтеграції з процесами кібербезпеки. Для їх порівняльної характеристики в попередньому дослідженні автора використано умовну оцінку CIM [13]. Вищі значення цієї оцінки отримали комплекси, що

охоплюють не лише електронне оформлення страхових операцій, а й збирання та аналіз даних про кіберризики, моніторинг стану кібербезпеки, реагування на кіберінциденти й інформаційну підтримку управління ризиками. Водночас CIM у таблиці 3.1 має порівняльний характер і не є розрахованим інтегральним індексом зрілості кіберстрахування.

Окремий напрям автоматизації становлять спеціалізовані технологічні рішення для оцінювання кіберризиків. Прикладом є CyberMatics — запатентований технологічний процес компанії AIG, призначений для оцінювання рівня кіберризику організації, формування оцінок ризику, визначення пріоритетних заходів контролю та прогнозування результатів їх упровадження. У межах цього процесу дані страхувальника передаються залученим партнерам із кібербезпеки, попередньо обробляються та використовуються в андеррайтинговій моделі AIG. На основі одержаних даних оновлюється профіль кіберзрілості, формуються оцінки ризику, результати порівняльного аналізу та рекомендації щодо його зниження. Одержана інформація використовується для підтримки управління кіберризиками та прийняття андеррайтингових рішень [91].

Перспективним напрямом розвитку засобів автоматизації є застосування методів машинного навчання, геоінформаційних технологій та даних моніторингу. Одним із джерел таких даних можуть бути пристрої та сенсорні системи Інтернету речей, що забезпечують мережеву взаємодію фізичних об’єктів і передавання показників їхнього стану [126]. У матеріалах Allianz зазначено, що спільне використання внутрішніх даних страховика, даних третіх сторін і показників, які надходять у режимі реального часу від сенсорних пристроїв, дає змогу формувати повніші й точніші профілі ризику. Методи машинного навчання та штучного інтелекту можуть застосовуватися для виявлення закономірностей у накопичених даних, прогнозування несприятливих подій та інформаційної підтримки прийняття страхових рішень. Одним із наведених прикладів є використання геопросторових даних для оцінювання

ризику повеней. Поєднання зазначених технологій створює можливості для автоматизованого оброблення значних масивів різнорідних даних та уточнення характеристик ризику [92, 126].

Водночас результати проведеного аналізу засвідчили недостатній рівень використання кіберстрахування та інших інструментів зниження ризиків і мінімізації негативних наслідків реалізації загроз у кіберпросторі, зокрема на об'єктах критичної інформаційної інфраструктури. Дані, що формуються у процесах кіберстрахування, не мають усталеного інтегрованого представлення у профілях кіберризику, а автоматизація відповідних процесів залишається фрагментарною [13]. Це зумовлює необхідність систематизації стандартизованих процесів кіберстрахування, визначення структури їхніх вхідних і вихідних даних та представлення таких процесів як об'єктів подальшої формалізації, алгоритмізації й автоматизації.

За результатами аналізу, систематизації та змістової адаптації положень ISO/IEC 27102:2019 до завдань дослідження визначено сукупність основних процесів кіберстрахування [12, 13]. Їх виокремлення ґрунтується на функціональному призначенні відповідних процесів, складі даних, що в них використовуються, виконуваних операціях оброблення інформації та результатах, необхідних для підтримки прийняття страхових і управлінських рішень.

До систематизованої сукупності основних процесів кіберстрахування віднесено:

1) оцінювання кіберризиків, кіберзбитків і засобів їх контролю;

2) управління кіберризиками;

3) типізацію та категоризацію кіберінцидентів;

4) управління наслідками кіберінцидентів;

5) управління інформаційною безпекою під час обміну даними зі страховиком;

6) управління договором (полісом) кіберстрахування, підтвердженнями, витратами на реагування на кіберінциденти та страховим покриттям;

7) андеррайтинг кіберстрахування;

8) збирання даних з інформаційних активів;

9) виконання зобов'язань, пов'язаних з інформаційною безпекою [12, 13].

Оцінювання кіберризиків, кіберзбитків і засобів їх контролю є початковим процесом формування інформації про ризик. Він охоплює збирання та перевірку даних про об'єкт оцінювання, ідентифікацію кіберризиків, визначення можливих наслідків їх реалізації та врахування наявних засобів контролю. Результатом процесу є структуровані дані про кіберризики та їх характеристики, які використовуються у процесах управління кіберризиками й андеррайтингу.

Управління кіберризиками передбачає оброблення та використання результатів оцінювання для прийняття рішень щодо способів поводження з ризиком. З позицій ризик-орієнтованого підходу цей процес охоплює формування профілю кіберризиків, визначення їх пріоритетності, вибір заходів контролю та подальший моніторинг зміни відповідних характеристик.

Типізація та категоризація кіберінцидентів забезпечують структуроване представлення даних про події в кіберпросторі. Віднесення кіберінцидентів до визначених типів і категорій створює можливість їх уніфікованого кодування, накопичення, пошуку, порівняння та подальшого автоматизованого оброблення. Результатом процесу є структурований набір відомостей про кіберінциденти, який може використовуватися для аналізу повторюваності подій, їх наслідків і пов'язаних із ними кіберризиків.

Управління наслідками кіберінцидентів передбачає збирання, перевірку та оброблення даних про реалізовані кіберризики. До складу відповідної інформації належать відомості про характеристики кіберінциденту, порушені інформаційні активи й операційні процеси, завдані збитки, виконані заходи реагування та витрати, пов'язані з ліквідацією наслідків і відновленням діяльності. Результати

оброблення цих даних використовуються для врегулювання страхових вимог, уточнення профілю кіберризику та подальшого оцінювання ризиків.

Управління інформаційною безпекою під час обміну даними зі страховиком є окремим процесом, оскільки оцінювання кіберризиків передбачає передавання відомостей про інформаційні активи, стан кібербезпеки, вразливості, кіберінциденти та засоби контролю. Відповідний інформаційний обмін має забезпечувати конфіденційність, цілісність, доступність і контрольованість доступу до даних, а також можливість перевірки їх походження та повноти.

Управління договором (полісом) кіберстрахування, підтвердженнями, витратами на реагування на кіберінциденти та страховим покриттям охоплює оброблення даних про умови страхування й наслідки реалізації кіберризиків. У межах цього процесу використовуються відомості про об’єкт страхування, страхові ризики та випадки, обсяг покриття, ліміти відповідальності, виключення, підтвердні документи, витрати на реагування та результати врегулювання страхових випадків. Результатом процесу є актуалізована інформація про виконання умов договору та використання страхового покриття.

Андеррайтинг кіберстрахування передбачає комплексне оброблення й аналіз даних для прийняття рішення щодо можливості та умов страхування кіберризиків. Вхідними даними є відомості про об’єкт страхування, інформаційні активи, стан кібербезпеки, наявні засоби контролю, попередні кіберінциденти, можливі збитки та результати оцінювання кіберризиків. На основі цих даних формуються андеррайтинговий висновок, умови страхового покриття, обмеження та інші параметри, необхідні для прийняття страхового рішення.

Практичні документи страховиків, регуляторні матеріали та наукові дослідження підтверджують використання під час андеррайтингу структурованих анкет, відомостей про впроваджені заходи кібербезпеки, характеристики інформаційних активів, залежності між ризиками та можливі сценарії збитків [127–135]. Водночас склад питань, критерії оцінювання та правила інтерпретації відповідей істотно відрізняються, що ускладнює

зіставлення результатів і підтверджує доцільність їх формалізованого представлення та оброблення.

Збирання даних з інформаційних активів є процесом формування вхідних даних для подальшого оцінювання. Джерелами можуть бути інформаційні системи, реєстри, бази даних, засоби моніторингу, системи управління інформаційною безпекою, технічна документація, анкети та результати самооцінювання. Зібрані дані підлягають перевірці, структуруванню й перетворенню у форму, придатну для оцінювання кіберризиків та аналізу стану кібербезпеки.

Виконання зобов'язань, пов'язаних з інформаційною безпекою, передбачає збирання та використання документованої інформації про функціонування системи управління інформаційною безпекою, застосовувані політики й засоби контролю, результати оцінювання та оброблення ризиків, моніторингу, вимірювань і аудиторських перевірок. До відповідних даних також належать результати управлінського аналізу, відомості про виявлені невідповідності, вжиті коригувальні заходи та підтвердження їх результативності. Ця інформація використовується для перевірки виконання страхувальником установлених вимог і зобов'язань у сфері інформаційної безпеки.

Систематизація наведених процесів дала змогу визначити спільну для них інформаційну складову. Кожний процес передбачає виконання однієї або декількох операцій над даними: збирання, перевірку, передавання, накопичення, класифікацію, структурування, перетворення, оцінювання й аналіз. Результати виконання цих операцій використовуються для формування профілів ризику, страхових і андеррайтингових рішень, визначення умов покриття та подальшого управління кіберризиками.

Узагальнену послідовність оброблення даних у процесах кіберстрахування подано таким чином:

збирання даних про інформаційні активи та стан об'єкта → перевірка і структуроване представлення даних → ідентифікація й оцінювання

кіберризиків та засобів контролю → формування профілю кіберризиків → використання результатів в андеррайтингу та управлінні страховим покриттям → накопичення й аналіз даних про кіберінциденти та наслідки їх реалізації → уточнення вхідних даних для наступного циклу оцінювання.

Відповідна послідовність відображає циклічний характер інформаційної взаємодії у процесах кіберстрахування. Дані, одержані на етапі оцінювання, використовуються для інформаційної підтримки прийняття страхових рішень. Відомості про реалізовані кіберризики, кіберінциденти та їх наслідки накопичуються, аналізуються і можуть використовуватися для уточнення вхідних даних під час наступного циклу оцінювання.

З позицій автоматизації систематизована сукупність процесів дає змогу визначити функціональні вимоги до автоматизації відповідних інформаційних процесів кіберстрахування. Для кожного процесу можуть бути визначені джерела вхідних даних, способи їх представлення, операції оброблення й аналізу, вихідні результати та інформаційні зв'язки з іншими процесами.

Формалізація зазначених інформаційних зв'язків є необхідною умовою переходу від змістового опису предметної області до розроблення відповідних моделей, методів і алгоритмів. Систематизація процесів кіберстрахування визначає структуру інформаційних процесів, які підлягають подальшому формальному поданню й алгоритмізації та можуть ураховуватися під час проєктування автоматизованих інформаційно-комунікаційних систем.

За результатами аналізу наукових праць, міжнародних стандартів, рекомендацій і практик автоматизації страхових операцій систематизовано процеси кіберстрахування з урахуванням положень ISO/IEC 27102:2019. Дослідження положень ISO/IEC 27102:2019 і практик застосування інформаційно-комунікаційних засобів дало змогу визначити процеси, придатні до подальшої формалізації, алгоритмізації й автоматизації [12, 13].

Одержані результати створюють основу для формального подання процесів збирання, представлення, оброблення й аналізу даних про кіберризики та

розроблення алгоритмів їх реалізації в інформаційних і комп'ютерних системах кіберстрахування. Формалізацію відповідних інформаційних процесів розглянуто в наступному підрозділі.

3.2. Формалізація інформаційних процесів оцінювання кіберризиків

Систематизація стандартизованих процесів кіберстрахування, проведена в підрозділі 3.1, показала, що значна частина цих процесів пов'язана зі збиранням, передаванням, накопиченням, структуруванням, обробленням, аналізом і використанням даних про об'єкт оцінювання, інформаційні активи, ризики інформаційної безпеки, кіберризики, кіберінциденти, засоби контролю та наслідки реалізації загроз. Об'єкти й процеси кіберстрахування, придатні до подальшої формалізації, алгоритмізації та автоматизації, досліджено в попередніх працях автора [13, 37].

Процеси оцінювання ризиків інформаційної безпеки та кіберризиків характеризуються використанням різнорідних показників, нормативних вимог, результатів самооцінювання, експертних оцінок і технічних даних. Це зумовлює необхідність формалізації операцій збирання, представлення, перевірки, оброблення й аналізу відповідних даних як передумови автоматизації процедур оцінювання та використання одержаних результатів для підтримки прийняття рішень у процесах кіберстрахування.

Методологічні засади формалізації процесів оцінювання та управління ризиками визначено в міжнародних стандартах, рекомендаціях спеціалізованих організацій і наукових працях. ISO 31000:2018 встановлює принципи, рамкову основу та процес управління ризиками, що охоплює визначення сфери застосування, середовища і критеріїв ризику, його ідентифікацію, аналіз, оцінювання та оброблення, а також моніторинг, перегляд, документування і

звітування [136]. У стандартах і рекомендаціях ISO/IEC, NIST та ENISA відповідні положення конкретизовано для інформаційної безпеки й кібербезпеки [3, 12, 17, 20, 112]. Проведений у першому та другому розділах аналіз показав, що ці підходи створюють основу для кількісного представлення окремих характеристик кіберризику. Водночас у межах опрацьованого масиву джерел не виявлено цілісного формального подання наскрізного інформаційного процесу використання різнорідних даних для підтримки прийняття рішень у кіберстрахуванні.

У попередніх працях автора обґрунтовано застосування статистичних та індексних підходів до оброблення даних про операційні ризики в кіберпросторі, визначено базові індикатори кібербезпеки, а також досліджено процеси автоматизації кіберстрахування й використання інформаційних технологій для їх реалізації [10, 13, 37, 67, 69]. Сукупність одержаних результатів дає змогу перейти від визначення окремих показників і процесів до формалізації послідовності збирання, представлення, оброблення й аналізу даних у процесах кіберстрахування.

Основою формалізації процесу оцінювання є ризик-орієнтований підхід. Його застосування передбачає визначення об’єкта оцінювання, ідентифікацію джерел і чинників ризику, формування системи показників, збирання відповідних даних, їх перевірку, чисельне представлення й оброблення, а також формування результатів оцінювання для підтримки прийняття рішень [136].

Проведений у другому розділі аналіз показав, що вихідні дані для оцінювання операційних ризиків у кіберпросторі є різнорідними за походженням, формою подання та способом отримання. Вони можуть характеризувати кіберінциденти, кібератаки, кіберзагрози, вразливості, стан інформаційних і комп’ютерних систем, організаційні й технічні заходи кіберзахисту, рівень виконання нормативних вимог, стан управління ризиками та інші характеристики об’єкта оцінювання [10, 37, 67].

Для використання різнорідних даних у процесах кіберстрахування необхідне їх структуроване та формалізоване представлення. Формалізація інформаційного процесу оцінювання передбачає визначення послідовності операцій, за допомогою яких вихідні дані перевіряються, структуруються, перетворюються на показники та індикатори, а їх чисельні значення використовуються для формування групових, доменних та інтегральної індексних оцінок.

У загальному вигляді інформаційний процес оцінювання операційних ризиків у кіберпросторі подано такою послідовністю [37]:

визначення об'єкта оцінювання → збирання вихідних даних → перевірка та структуризація даних → визначення показників та індикаторів → чисельне представлення їх значень → групування показників → формування групових і доменних оцінок → агрегування результатів → формування профілю операційних ризиків → підготовка інформації для підтримки прийняття рішень.

Наведена послідовність визначає загальну структуру оброблення даних незалежно від конкретного набору показників, джерел інформації або програмних засобів, які використовуються для її реалізації.

Структурне подання інформаційного процесу оцінювання операційних ризиків у кіберпросторі наведено на рисунку 3.1.

Рисунок 3.1 — Структурне подання інформаційного процесу оцінювання операційних ризиків у кіберпросторі

Вхідні дані (джерела інформації)		**Етапи інформаційного процесу оцінювання**			**Результати (вихідна інформація)**
Самооцінювання анкети; опитувальники; внутрішня документація.	⇨	1	**Визначення об'єкта оцінювання** встановлення меж, цілей та складу оцінювання. ⇩	⇨	**Показники та індикатори** чисельні значення; якісні оцінки, перетворені у чисельну форму.
Експертні оцінки		2	**Збирання вихідних**		**Групові оцінки**

внутрішні та зовнішні експерти.			**даних** отримання даних з різних джерел. ⇩		окремих складових об’єкта оцінювання.
Нормативні та організаційні документи нормативні вимоги; політики; регламенти; результати аудиту.		3	**Перевірка та структуризація даних** оцінювання повноти, придатності та віднесення до показників. ⇩		**Доменні та інтегральна індексні оцінки** інтегральні індексні оцінки.
Технічні дані засоби моніторингу; виявлення та реагування; аналіз вразливостей; журнали подій.		4	**Визначення показників та індикаторів** формування системи показників. ⇩		**Профіль операційних ризиків** структуроване подання результатів; виявлення критичних складових; порівняння у динаміці.
Дані про інциденти та загрози кіберінциденти; кібератаки; вразливості.		5	**Чисельне представлення їх значень** застосування шкал, критеріїв та правил перетворення. ⇩		**Інформація для підтримки прийняття рішень** андеррайтинг; визначення умов страхування; страхове покриття; управління ризиками.
Інформація про об’єкт оцінювання інформаційні активи; інформаційні та комп’ютерні системи; процеси; заходи кіберзахисту; стан управління ризиками.		6	**Групування показників** об’єднання за функціональними, предметними або нормативними ознаками ⇩		
		7	**Формування групових оцінок** оцінювання окремих складових об’єкта ⇩		
		8	**Агрегування результатів** отримання агрегатних індексних оцінок ⇩		
		9	**Формування профілю оцінювання**		

			структуроване подання результатів ⇩		
		10	**Підготовка інформації для підтримки прийняття рішень** використання результатів у процесах кіберстрахування		

Джерело: розроблено автором за [37].

Першим етапом є визначення об’єкта, мети та меж оцінювання. Об’єктом оцінювання може бути організація, інформаційна або комп’ютерна система, окремий інформаційний актив, операційний процес чи сукупність взаємопов’язаних об’єктів. Встановлення меж оцінювання необхідне для визначення складу даних, джерел їх отримання та критеріїв, що застосовуватимуться на наступних етапах [37].

Другим етапом є збирання вихідних даних. Їх джерелами можуть бути анкети самооцінювання, нормативні й організаційно-розпорядчі документи, результати аудиту, експертні оцінки, технічні дані засобів моніторингу, відомості про кіберінциденти, кібератаки, кіберзагрози, вразливості, інформаційні активи та впроваджені заходи кіберзахисту. Для кожного джерела мають бути визначені склад, форма подання та спосіб отримання даних.

Третім етапом є перевірка достовірності і структуризація зібраних даних. На цьому етапі оцінюються їх повнота, достовірність і придатність для подальшого оброблення, а також встановлюється відповідність даних визначеним показникам, індикаторам і групам показників. Необхідність такої перевірки зумовлена різнорідністю джерел та одночасним використанням кількісних і якісних характеристик.

Після структуризації вихідних даних здійснюються визначення показників та індикаторів і чисельне представлення їх значень. Для показників, що мають безпосереднє кількісне представлення, використовуються відповідні чисельні значення. Для індикаторів, поданих у формі тверджень, може застосовуватися

процедура чисельної індикації, під якою розуміється встановлення відповідності чисельного значення, бала або вагової характеристики індикатору, що має вигляд твердження. Алгоритм визначення такої відповідності встановлюється в межах відповідної моделі [37].

Чисельне представлення показників створює можливість їх подальшого групування за функціональними, предметними або нормативними ознаками. У межах доменної структури показники та індикатори об'єднуються за належністю до відповідних доменів і піддоменів. Сформовані групи використовуються для одержання групових і доменних оцінок, що характеризують окремі складові стану об'єкта оцінювання.

Наступним етапом є агрегування результатів. Відповідно до індексного підходу, розглянутого в другому розділі, значення окремих показників та індикаторів послідовно об'єднуються у групові й доменні оцінки, на основі яких може формуватися інтегральна індексна оцінка. Склад показників, правила їх групування, порядок урахування вагових характеристик і метод агрегування встановлюються відповідною моделлю оцінювання [37].

Результатом інформаційного процесу є не лише окреме чисельне значення, а й структурований профіль операційних ризиків. Такий профіль відображає стан окремих складових об'єкта оцінювання, дає змогу виявляти критичні складові, порівнювати результати повторних оцінювань і використовувати одержану інформацію для підтримки прийняття рішень у процесах кіберстрахування [37].

Важливою властивістю формалізованого процесу є можливість використання декількох джерел даних. Результати самооцінювання можуть доповнюватися експертними оцінками, результатами зовнішнього оцінювання, нормативними даними та технічними показниками. Поєднання відповідних джерел дає змогу уточнювати інформацію про об'єкт оцінювання, здійснювати взаємну перевірку одержаних даних і зменшувати залежність результатів від одного джерела інформації.

Технічні дані можуть надходити з інформаційних і комп'ютерних систем та засобів кібербезпеки, зокрема систем моніторингу, засобів виявлення кіберінцидентів і реагування на них, засобів аналізу вразливостей, журналів подій та інших засобів контролю. Використання автоматизованих джерел дає змогу доповнювати результати самооцінювання об'єктивними технічними показниками стану об'єкта та створює передумови для автоматизації окремих операцій збирання, перевірки й оброблення даних.

Формалізація процесу оцінювання не визначає наперед конкретного програмного засобу або інформаційної системи. Її результатом є структурне подання процесу, у межах якого визначено джерела і склад вхідних даних, правила їх перевірки, способи представлення, послідовність операцій оброблення, процедури формування показників та індикаторів, структуру вихідних результатів та інформаційні зв'язки між окремими етапами оцінювання.

Таке структурне подання створює основу для алгоритмізації процесу оцінювання. Відповідний алгоритм має передбачати послідовне виконання операцій збирання даних, перевірки їх повноти й придатності, віднесення до визначених показників, чисельного представлення значень індикаторів, групування та агрегування результатів, формування профілю операційних ризиків і підготовки інформації для підтримки прийняття рішень у процесах кіберстрахування [37].

Результати формалізації дають змогу визначити вимоги до інформаційних технологій, які можуть застосовуватися для оцінювання операційних ризиків у кіберпросторі. Відповідні технології мають забезпечувати роботу з різнорідними джерелами даних, їх перевірку і структуризацію, зберігання значень показників та індикаторів, формування групових, доменних та інтегральної індексних оцінок, порівняння профілів і підготовку результатів для підтримки прийняття рішень.

Таким чином, формалізація інформаційного процесу оцінювання кіберризиків забезпечує перехід від систематизованої сукупності процесів

кіберстрахування до структурованої послідовності операцій над даними. Визначення джерел і складу вхідних даних, правил їх перевірки та структуризації, процедур формування показників й індикаторів, а також способів групування й агрегування результатів створює основу для алгоритмізації процедур оцінювання та їх подальшої реалізації із застосуванням інформаційних технологій.

Одержані результати визначають інформаційну структуру процесу оцінювання операційних ризиків у кіберпросторі та створюють основу для визначення класів інформаційних технологій, які можуть застосовуватися для автоматизації відповідних процесів кіберстрахування. Основні класи й функціональні можливості таких технологій розглянуто в наступному підрозділі.

3.3. Інформаційні технології страхування та кіберстрахування

Застосування інформаційних технологій у страхуванні та кіберстрахуванні супроводжується цифровою трансформацією інформаційних і бізнес-процесів. Основними напрямами відповідних змін є врахування специфічних ризиків реалізації страхових подій у кіберпросторі та впровадження програмних і технічних засобів для автоматизації збирання, представлення, оброблення й аналізу даних, оцінювання кіберризиків та інформаційної підтримки прийняття рішень у процесах кіберстрахування [68, 69].

На сучасному етапі розвиток інформаційних технологій кіберстрахування пов’язаний з автоматизацією збирання й оброблення даних про кіберризики, інтеграцією результатів самооцінювання з технічними даними, застосуванням спеціалізованих платформ, а також використанням методів штучного інтелекту та машинного навчання для виявлення закономірностей і підтримки прийняття рішень. Окремого значення набувають технології моніторингу стану

кібербезпеки, аналізу вразливостей, прогнозування кіберінцидентів та оцінювання можливих наслідків їх реалізації [17, 68, 91, 92, 112].

Проведений аналіз засвідчив відмінності між рівнем технологічного забезпечення кіберстрахування в Україні та практиками, що застосовуються на розвинених страхових ринках. В Україні використання спеціалізованих інформаційних систем і програмних засобів кіберстрахування залишається обмеженим, а автоматизація відповідних процесів має переважно фрагментарний характер. Це зумовлює необхідність системного дослідження класів інформаційних технологій, їх функціональних можливостей та придатності до реалізації формалізованих процесів оцінювання кіберризиків [13, 68, 69].

Водночас нормативні передумови для розвитку цього напряму поступово формуються. ISO/IEC 27102:2019 містить настанови щодо оцінювання кіберризиків, обміну інформацією між страховиком і страхувальником та врахування стану інформаційної безпеки під час визначення умов страхового покриття [12]. Нормативно-правові акти Національного банку України встановлюють вимоги до визначення профілю ризику надавачів фінансових послуг, здійснення діяльності за класами страхування, обліку договорів і захисту інформації страховика [119–121]. Сукупність відповідних положень формує передумови для подальшої формалізації й автоматизації інформаційних процесів страхування та кіберстрахування.

До основних напрямів подальшого розвитку інформаційного забезпечення кіберстрахування належать:

- удосконалення нормативно-методичної бази;
- упровадження практик кіберстрахування;
- використання автоматизованих технічних засобів оцінювання кіберризиків, спеціалізованих платформ і програмного забезпечення;
- застосування методів моделювання та інформаційно-аналітичної діяльності;

- накопичення, систематизація й аналіз страхових, фінансових і кібербезпекових даних [13, 68, 69].

Питання управління кіберризиками у страхуванні та розвитку кіберстрахування в Україні досліджували О. Є. Гудзь, Н. Г. Нагайчук, Л. С. Селіверстова, Р. В. Пікус, М. В. Дубина та інші науковці [108–110, 137–140]. У відповідних працях розглянуто економічні, фінансові й організаційні аспекти кіберстрахування, особливості формування страхового покриття та управління кіберризиками.

Концептуальні засади кіберстрахування, підходи до моделювання кіберризиків, оцінювання можливих збитків, ціноутворення та використання даних про стан кібербезпеки під час прийняття страхових рішень досліджено у працях A. Marotta зі співавторами, S. Romanosky зі співавторами, R. Böhme і G. Schwartz, а також L. A. Odell, J. C. Fauntleroy та R. R. Wagner [106–108, 110].

Застосування інформаційних технологій у кіберстрахуванні досліджено у працях I. Vakilinia, S. Sengupta, T. Lepoint, G. F. Ciocarlie, K. Eldefrawy, S. Kumar, L. Loo та L. Kocian. У відповідних дослідженнях розглянуто застосування розподілених платформ, блокчейну та смартконтрактів для обміну даними й автоматизації окремих процесів кіберстрахування [18, 141–143]. Правові та організаційні аспекти страхування кіберризиків і врегулювання відповідних страхових випадків висвітлено у праці D. Armstrong, T. Steward і S. Thakerar [144].

Проведений аналіз показав, що інформаційні технології у страхуванні та кіберстрахуванні застосовуються для реалізації різних за функціональним призначенням інформаційних процесів. Формалізація процесів оцінювання кіберризиків, виконана у підрозділі 3.2, зумовлює необхідність систематизації технологій і методів, які забезпечують збирання, представлення, передавання, зберігання, інтеграцію, оброблення й аналіз різнорідних даних, формування результатів оцінювання та їх використання для підтримки прийняття рішень у процесах кіберстрахування.

За результатами проведеного аналізу систематизовано основні напрями застосування інформаційних технологій і методів у процесах страхування та кіберстрахування [13]: технології електронного бізнесу; методи контент-аналізу; мобільні інформаційні системи; технології інтеграції інформаційних ресурсів; технології аналітики великих даних, штучного інтелекту, машинного навчання та оброблення природної мови; блокчейн-технології та смартконтракти; методи математичного, імітаційного і статистичного моделювання.

Наведені напрями можуть бути використані як складові системи оцінювання рівня застосування інформаційних технологій у процесах кіберстрахування. Їх перелік може уточнюватися залежно від мети, задач і особливостей об'єкта оцінювання. Межі між окремими напрямами є умовними, оскільки під час реалізації одного інформаційного процесу можуть спільно застосовуватися декілька взаємопов'язаних технологій і методів.

Технології електронного бізнесу. До цієї групи належать технології електронної комерції, цифрові платформи, інформаційні системи управління бізнесом, засоби електронного документообігу, маркетингові та платіжні технології [13, 145]. Електронна взаємодія може здійснюватися за моделями «бізнес — бізнес» (Business-to-Business, B2B), «бізнес — споживач» (Business-to-Consumer, B2C) і «споживач — споживач» (Consumer-to-Consumer, C2C). Окрему групу становлять моделі електронної взаємодії бізнесу і споживачів з органами публічного управління [145].

Інфраструктурні технології охоплюють вебсайти, цифрові платформи, програмні застосунки, бази та сховища даних, засоби зберігання й оброблення даних, системи керування контентом та електронного документообігу. До технологій управління бізнесом належать системи управління взаємовідносинами з клієнтами, планування ресурсів підприємства, управління ланцюгами постачання та бізнес-аналітики [145].

Маркетингові технології охоплюють пошукову оптимізацію, контекстну рекламу, електронний маркетинг, таргетинг та аналіз поведінки користувачів. До

платіжних технологій належать електронні гаманці, карткові й мобільні платіжні системи та засоби обліку відповідних операцій [145].

У процесах кіберстрахування технології електронного бізнесу забезпечують електронну взаємодію між страховиком, страхувальником, страховим посередником, експертами та іншими учасниками; збирання і первинне оброблення даних заяв та анкет; обмін документами; укладання й супроводження договорів; управління клієнтськими даними; виконання платежів та інформаційну підтримку прийняття страхових рішень [13].

Контент-аналіз полісів кіберстрахування. Контент-аналіз є методом систематизованого дослідження змісту текстових документів, а не окремою інформаційною технологією. Його застосування до полісів, заяв, анкет та інших документів кіберстрахування дає змогу формалізувати відомості про структуру страхового покриття, виключення, умови договорів, вимоги до страхувальників, фактори ціноутворення та врахування показників кібербезпеки [107].

У процесах кіберстрахування контент-аналіз може застосовуватися для:

- визначення видів збитків, що покриваються договором страхування;
- виявлення виключень і обмежень страхового покриття;
- аналізу умов покриття відповідальності перед третіми особами;
- систематизації даних заяв і анкет щодо стану інформаційної безпеки та кібербезпеки;
- визначення факторів, які враховуються під час оцінювання ризику й встановлення параметрів страхування;
- дослідження зв’язку між характеристиками об’єкта страхування, станом його кібербезпеки та умовами страхового покриття [107].

Автоматизація контент-аналізу може здійснюватися із застосуванням методів оброблення природної мови, семантичного аналізу, класифікації текстів і пошуку ключових умов страхування. Це забезпечує перетворення неструктурованих текстових даних на формалізовані показники, придатні для

подальшого оброблення, порівняння й використання у процесах оцінювання кіберризиків та підтримки прийняття страхових рішень.

Мобільні інформаційні системи. У процесах страхування та кіберстрахування мобільні застосунки й адаптовані до мобільних пристроїв цифрові сервіси забезпечують віддалений доступ користувачів до інформаційних ресурсів, страхових документів, електронних форм, інструкцій, реєстрів і баз даних [13].

Мобільні інформаційні системи можуть використовуватися для подання заявок і анкет, збирання первинних даних про об'єкт страхування, передавання документів, повідомлення про кіберінциденти, реєстрації страхових випадків, отримання рекомендацій щодо реагування та взаємодії зі страховиком. Зібрані дані можуть передаватися до інформаційних систем страховика для перевірки, подальшого оброблення, аналізу й використання під час оцінювання кіберризиків та прийняття страхових рішень.

Засоби централізованого управління мобільними пристроями забезпечують контроль їх конфігурацій, встановлення політик безпеки, керування доступом до інформаційних ресурсів і захист даних під час їх зберігання та передавання. У процесах кіберстрахування відповідні засоби можуть використовуватися як для забезпечення захищеної електронної взаємодії між учасниками, так і для отримання окремих технічних показників, необхідних для формування профілю кіберризику [13].

Інтеграція інформаційних ресурсів. Інтеграція інформаційних ресурсів у процесах кіберстрахування передбачає узгоджене збирання, представлення, об'єднання та оброблення фінансово-економічних, страхових, організаційних і кібербезпекових даних, що надходять із різних інформаційних систем та інших джерел [13, 92].

До відповідних інформаційних ресурсів можуть належати:

- дані страхових інформаційних систем;

- відомості про договори, страхові премії, страхові випадки, заявлені збитки та виплати;
- дані систем управління інформаційною безпекою;
- результати оцінювання кіберризиків;
- журнали кіберінцидентів;
- дані моніторингу інформаційних і комп'ютерних систем;
- результати аудиту, тестування та оцінювання відповідності;
- фінансові показники суб'єкта оцінювання;
- відомості про сертифікацію, відповідність установленим вимогам і впроваджені заходи кіберзахисту [13, 92, 107].

Використання зазначених ресурсів залежить від їх доступності, повноти, достовірності, актуальності, сумісності форматів і правових обмежень щодо оброблення та передавання даних. Їх інтеграція створює передумови для переходу від оцінювання, заснованого переважно на окремих анкетах і самооцінюванні, до комплексного аналізу фінансових, страхових, технічних і кібербезпекових показників. Водночас у межах цієї дисертації визначено методологічні засади такого переходу, а не реалізовано завершену інтеграційну інформаційну систему.

Аналітика великих даних. Технології аналітики великих даних застосовуються у страхуванні для оброблення значних обсягів структурованих і неструктурованих даних, оцінювання ризиків, виявлення закономірностей, протидії шахрайству та підтримки прийняття рішень [15, 16]. Їх використання у кіберстрахуванні обмежується доступністю, повнотою і порівнянністю страхових та кібербезпекових даних, частина яких може належати до інформації з обмеженим доступом або становити комерційну таємницю.

У процесах кіберстрахування до аналітичного контуру можуть надходити:

- дані систем управління інформацією та подіями безпеки;
- дані систем виявлення і реагування на загрози на кінцевих пристроях;
- дані систем розширеного виявлення та реагування;

- журнали кіберінцидентів і результати моніторингу;
- дані про вразливості та стан упровадження заходів кіберзахисту;
- відомості про заявлені збитки, страхові випадки, виплати та страхові премії;
- результати оцінювання кіберризиків і зрілості кібербезпеки [13, 15, 16].

Системи управління інформацією та подіями безпеки забезпечують збирання, агрегування й кореляцію даних із різних джерел для виявлення кіберзагроз і кіберінцидентів. Системи виявлення та реагування забезпечують моніторинг кінцевих пристроїв, мережевої інфраструктури і хмарних середовищ. Водночас ці системи не є самостійними технологіями великих даних, але сформовані ними відомості можуть використовуватися як вхідні дані для подальшого аналітичного оброблення.

Для зберігання й оброблення значних масивів структурованих і неструктурованих даних можуть застосовуватися розподілені обчислювальні платформи, хмарні сховища, системи керування базами даних, засоби бізнес-аналітики та візуалізації. Їх використання створює можливості для комплексного аналізу даних про кіберінциденти, вразливості, збитки, страхові випадки й заходи кіберзахисту та формування інформаційної основи для оцінювання кіберризиків і підтримки страхових рішень [15, 16].

Штучний інтелект, машинне навчання та оброблення природної мови. Методи штучного інтелекту й машинного навчання можуть застосовуватися у страхуванні та кіберстрахуванні для виявлення закономірностей у накопичених даних, класифікації ризиків, прогнозування несприятливих подій та інформаційної підтримки прийняття рішень [15–17, 92]. До основних неактуарних напрямів їх застосування належать автоматизація андеррайтингу й опрацювання заявлених збитків, виявлення страхового шахрайства, аналіз поведінки страхувальників, класифікація документів та оброблення значних масивів текстових даних.

В актуарних процесах методи машинного навчання можуть використовуватися для оцінювання частоти й розміру збитків, класифікації та сегментації ризиків, прогнозування страхових виплат і резервів, визначення факторів ризику та підтримки ціноутворення. Відповідні методи можуть поєднуватися з регресійним, статистичним та імовірнісним моделюванням, однак достовірність одержаних результатів залежить від обсягу, якості, репрезентативності й актуальності вхідних даних [15–17].

Методи оброблення природної мови можуть застосовуватися для автоматизованого аналізу полісів, анкет, договорів, листування, заяв про страхові випадки, аудиторських матеріалів і звітів про кіберінциденти. Їх використання дає змогу виділяти з неструктурованих текстів відомості про умови страхового покриття, виключення, характеристики кіберризиків і впроваджені заходи кіберзахисту та перетворювати ці відомості на структуровані показники для подальшого оброблення. Застосування штучного інтелекту й машинного навчання має передбачати контроль якості даних, пояснюваність одержаних результатів, захист персональних і конфіденційних даних та врахування нормативних обмежень [16, 17].

Блокчейн-технології та смартконтракти. Застосування блокчейн-технологій у кіберстрахуванні пов’язане з необхідністю забезпечення цілісності й простежуваності записів, узгодженої взаємодії між учасниками страхового процесу та автоматизації окремих операцій із даними [18, 141–143]. Розподілений реєстр може використовуватися для фіксації фактів подання і перевірки відомостей, реєстрації подій, збереження історії операцій та контролю внесення змін до відповідних записів. Смартконтракти можуть забезпечувати автоматизоване виконання визначених правил після настання формалізованих умов, зокрема під час перевірки даних, реєстрації страхового випадку, супроводження договору та виконання передбачених ним операцій [18, 141]. Поєднання блокчейн-технологій із засобами самосуверенної ідентичності може використовуватися для управління цифровими ідентифікаторами та

контрольованого обміну ідентифікаційними даними між учасниками процесів кіберстрахування [18].

Водночас застосування блокчейн-технологій у кіберстрахуванні потребує подальшого дослідження практичної ефективності відповідних рішень, нормативного регулювання та інтеграції з наявними страховими інформаційними системами. Використання розподіленого реєстру саме по собі не гарантує достовірності первинних даних або збереження їх конфіденційності, тому має супроводжуватися процедурами перевірки даних, управління доступом і захисту інформації.

Математичне, імітаційне та статистичне моделювання. У кіберстрахуванні методи моделювання застосовуються для формалізованого подання кіберризиків, встановлення залежностей між їх факторами, оцінювання частоти й розміру можливих збитків, визначення параметрів страхового покриття та підтримки прийняття рішень [17, 106, 146–149].

Математичні й статистичні моделі дають змогу кількісно описувати характеристики ризику та досліджувати залежності між показниками. Ймовірнісні та стохастичні моделі використовуються для врахування невизначеності, випадкового характеру кіберінцидентів і варіативності їх наслідків. Імітаційне моделювання дає змогу відтворювати сценарії реалізації кіберризиків, досліджувати їх сукупний вплив і порівнювати можливі варіанти страхових рішень [146–149].

Вибір виду моделі та методу її побудови залежить від поставленої задачі, доступності й якості вхідних даних, рівня невизначеності, масштабу досліджуваного ризику та необхідної форми подання результатів. Основні моделі й методи моделювання, які можуть застосовуватися для оцінювання та страхування кіберризиків, систематизовано в таблиці 3.2.

Таблиця 3.2 — Основні моделі та методи моделювання кіберризиків у процесах кіберстрахування

Модель або метод	Стислий опис	Основні переваги та обмеження	Застосування у процесах кіберстрахування
FAIR (Factor Analysis of Information Risk)	Кількісне оцінювання частоти реалізації загроз і величини можливих втрат на основі даних про активи, загрози, вразливості та наслідки	Забезпечує фінансове подання ризику і проведення сценарного аналізу; залежить від повноти вхідних даних та обґрунтованості експертних оцінок	Кількісне оцінювання кіберризику та інформаційна підтримка визначення параметрів страхового покриття [43]
Байєсівські мережі	Імовірнісне подання причинно-наслідкових зв'язків між факторами кіберризику, подіями та їх наслідками	Враховують невизначеність і допускають оновлення оцінок у разі надходження нових даних; побудова структури та визначення ймовірностей можуть бути складними	Сценарне оцінювання кіберризиків і прогнозування можливих наслідків кіберінцидентів [148]
Частотно-збиткові та регресійні моделі	Статистичне оцінювання частоти страхових випадків і розподілу можливих збитків	Придатні для актуарних розрахунків і сегментації ризиків; обмежуються неповнотою та неоднорідністю історичних даних	Оцінювання частоти й розміру збитків, підтримка ціноутворення та визначення страхових резервів [146, 147]
Метод Монте-Карло	Імітаційне відтворення множини можливих сценаріїв реалізації кіберризику	Дає змогу враховувати невизначеність і проводити аналіз чутливості; результати залежать від вихідних припущень і заданих розподілів	Оцінювання розподілу можливих збитків і порівняння варіантів страхового покриття [147, 148]
Агентні моделі	Моделювання поведінки та взаємодії учасників, зокрема організацій, користувачів і суб'єктів кіберзагроз	Дають змогу досліджувати взаємозалежності та мережеві ефекти; потребують складного калібрування	Сценарний аналіз поширення кіберінцидентів та оцінювання накопичувального ризику [148]

Моделі системного і накопичувального кіберризику	Аналіз взаємозалежностей між об'єктами, концентрації ризику та каскадних наслідків кіберінцидентів	Придатні для портфельного аналізу і перестрахування; складність полягає у визначенні залежностей і калібруванні моделей	Оцінювання сукупних збитків, концентрації ризику та можливих катастрофічних сценаріїв [148, 149]
Моделі машинного навчання	Класифікація і сегментація ризиків, виявлення закономірностей та прогнозування на основі накопичених даних	Забезпечують оброблення багатовимірних і різнорідних даних; потребують репрезентативних вибірок та пояснюваності результатів	Виявлення факторів ризику, прогнозування збитків, підтримка андеррайтингу та виявлення шахрайства [17, 146]

Примітка. Систематизовано автором за [17, 43, 146–149].

Проблемні напрями подальших досліджень. Проведений аналіз сучасних моделей, методів та інформаційних технологій засвідчив, що подальшого дослідження потребують:

- формалізація процесів збирання, представлення, перевірки, оброблення й аналізу різнорідних даних про кіберризики;
- автоматизація оцінювання кіберризиків та інформаційна підтримка андеррайтингу;
- інтеграція страхових, фінансових і кібербезпекових даних;
- моделювання частоти й розміру збитків за умов обмеженості та неоднорідності вихідних даних;
- оцінювання системних і накопичувальних кіберризиків у взаємопов'язаних інформаційних системах;
- розроблення пояснюваних моделей підтримки прийняття рішень із використанням методів штучного інтелекту та машинного навчання;
- формування й актуалізація баз даних про кіберінциденти, збитки, страхові випадки та впроваджені заходи кіберзахисту;
- визначення показників і рівнів зрілості застосування інформаційних технологій у процесах кіберстрахування [13, 17, 146–149].

Проведений аналіз показав, що процеси кіберстрахування передбачають використання технологій електронного бізнесу, інтеграції інформаційних ресурсів, аналітики великих даних, штучного інтелекту, машинного навчання, блокчейн-технологій, математичного й статистичного моделювання та технічних засобів кібербезпеки. Рівень їх застосування є неоднорідним: частина технологій використовується у традиційному страхуванні, тоді як автоматизоване оцінювання кіберризиків, інтеграція технічних показників кібербезпеки з процесами андеррайтингу та динамічне оновлення профілю ризику залишаються напрямами подальшого розвитку.

Отже, інформаційні технології забезпечують можливості формалізації, цифровізації й автоматизації процесів кіберстрахування. Проведена систематизація дала змогу визначити основні групи технологій, джерела даних, моделі та методи, які можуть використовуватися для реалізації формалізованих у підрозділі 3.2 інформаційних процесів. Одержані результати створюють основу для визначення структури застосування інформаційних технологій та оцінювання рівня їх впровадження у процесах кіберстрахування, що розглядається в наступному підрозділі.

3.4. Трикомпонентна п’ятирівнева модель впровадження інформаційних технологій у процеси кіберстрахування

Ринок кіберстрахування в Україні перебуває на етапі формування. Його розвиток відбувається за умов обмеженості відкритих статистичних даних про обсяги страхових премій, кількість укладених договорів, страхові випадки та фінансові результати відповідного сегмента. Використання спеціалізованих інформаційних систем і технічних засобів кіберстрахування залишається

фрагментарним, що ускладнює комплексне оцінювання рівня автоматизації відповідних процесів [13, 68, 69].

Розвиток глобального ринку кіберстрахування пов'язаний зі збільшенням кількості кібератак, витоків даних, випадків застосування програм-вимагачів, порушень функціонування інформаційних систем та зростанням фінансових втрат внаслідок кіберінцидентів [150–152]. За таких умов розвиток кіберстрахування в Україні потребує не лише запровадження окремих страхових продуктів, а й системного впровадження інформаційних технологій для збирання, представлення, оброблення й аналізу даних про кіберризики та підтримки прийняття страхових рішень.

Для характеристики передумов розроблення моделі доцільно врахувати істотну відмінність між рівнем розвитку світового та українського ринків кіберстрахування. За даними Міжнародної асоціації органів страхового нагляду, обсяг валових страхових премій на світовому ринку кіберстрахування у 2024 році становив 15,3 млрд дол. США, що приблизно вдвічі перевищує відповідний показник 2020 року [153]. Водночас офіційні статистичні дані про обсяги премій і кількість договорів саме з кіберстрахування в Україні у відкритих джерелах окремо не представлені.

Обмеженість статистичних даних не дає змоги виконати належне кількісне зіставлення світового й українського ринків кіберстрахування. Тому наведені відомості використовуються не для визначення потенційної місткості українського ринку, а для обґрунтування необхідності систематизації інформаційних технологій, які можуть застосовуватися у процесах кіберстрахування.

На основі аналізу стандартизованих процесів кіберстрахування, інформаційних технологій, методів оцінювання кіберризиків і спеціалізованих технічних засобів запропоновано трикомпонентну п'ятирівневу модель впровадження інформаційних технологій у процеси кіберстрахування [19]. Модель призначена для структурованого подання відповідних технологій і

засобів, визначення послідовних рівнів їх застосування та формування інформаційної основи для оцінювання зрілості процесів кіберстрахування.

Запропонована модель передбачає виокремлення трьох взаємопов'язаних компонентів: інформаційних технологій і технічних засобів страхування; моделей, методів та інформаційних засобів оцінювання страхових кіберризиків; спеціалізованих інформаційних технологій і технічних засобів кіберстрахування.

Перший компонент характеризує базові засоби цифровізації та автоматизації страхових процесів. Другий компонент охоплює моделі, методи, алгоритми та дані, необхідні для ідентифікації, аналізу й оцінювання кіберризиків. Третій компонент відображає спеціалізовані інформаційні технології та технічні засоби, які забезпечують реалізацію процесів кіберстрахування. Структуру компонентів запропонованої моделі наведено в таблиці 3.3.

Таблиця 3.3 — Компоненти трикомпонентної п'ятирівневої моделі впровадження інформаційних технологій у процеси кіберстрахування

Компонент моделі	**Зміст компонента**	**Основні об'єкти оцінювання**
Інформаційні технології та технічні засоби страхування	Технології та засоби цифровізації й автоматизації загальних страхових процесів	системи управління взаємовідносинами з клієнтами; системи планування ресурсів; засоби бізнес-аналітики; електронний документообіг; електронні форми; мобільні застосунки; платіжні системи; клієнтські та брокерські платформи
Моделі, методи та інформаційні засоби оцінювання страхових кіберризиків	Засоби збирання, представлення, оброблення й аналізу даних для ідентифікації та оцінювання кіберризиків	Анкети; профілі ризику; моделі й методи оцінювання; системи моніторингу; показники стану кібербезпеки; індикатори кіберризику; оцінки ймовірних збитків

Інформаційні технології та технічні засоби кіберстрахування	Спеціалізовані технології та засоби, інтегровані у процеси кіберстрахування	Засоби автоматизованої підтримки андеррайтингу; платформи кіберстрахування; системи моніторингу кіберризиків; засоби реагування на кіберінциденти; системи керованого виявлення та реагування; засоби управління страховими претензіями; блокчейн-технології та смартконтракти

Примітка. Розроблено автором за результатами попереднього дослідження [19].

Перший компонент охоплює інформаційні технології та технічні засоби, що застосовуються для цифровізації й автоматизації загальних страхових процесів. До них належать системи управління взаємовідносинами з клієнтами, системи планування ресурсів підприємства, засоби бізнес-аналітики, електронного документообігу та здійснення платежів, а також мобільні застосунки, клієнтські, брокерські й інші цифрові платформи [13, 69].

Виокремлення першого компонента зумовлено тим, що частина процесів кіберстрахування є спільною з процесами традиційного страхування. До них належать ведення даних про клієнтів, приймання й опрацювання заяв, укладання та супроводження договорів, обмін документами, здійснення платежів, врегулювання страхових випадків, управління страховими претензіями та взаємодія з брокерами. Автоматизація цих процесів може здійснюватися із застосуванням інформаційних технологій, які вже використовуються у страхуванні.

Другий компонент охоплює моделі, методи, алгоритми та інформаційні засоби ідентифікації, аналізу й оцінювання кіберризиків. Його призначення полягає у забезпеченні збирання, формалізованого представлення, перевірки, оброблення та аналізу даних, необхідних для формування профілю кіберризику і підтримки прийняття страхових рішень.

Вхідними даними другого компонента можуть бути відомості зі структурованих анкет, результати самооцінювання й експертного оцінювання, технічні показники стану інформаційних і комп’ютерних систем, дані моніторингу, характеристики інформаційних активів, відомості про

кіберінциденти та оцінки можливих збитків. Результатом їх оброблення є формалізований профіль кіберризику, який може використовуватися під час андеррайтингу, визначення умов страхування та прийняття інших страхових рішень.

Третій компонент охоплює спеціалізовані інформаційні технології та технічні засоби, інтегровані безпосередньо у процеси кіберстрахування. До них належать засоби автоматизованої підтримки андеррайтингу, платформи кіберстрахування, системи моніторингу кіберризиків, інструменти реагування на кіберінциденти, системи керованого виявлення та реагування, засоби інформаційної підтримки врегулювання страхових випадків, блокчейн-технології та смартконтракти [13, 69].

Виокремлення третього компонента дає змогу розмежувати інформаційні технології загального призначення, які застосовуються у традиційному страхуванні, та спеціалізовані засоби роботи з даними про кіберризики. Таке розмежування необхідне для визначення рівня впровадження відповідних технологій, виявлення недостатньо автоматизованих процесів і формування напрямів подальшого розвитку інформаційного забезпечення кіберстрахування.

Три компоненти моделі є взаємопов'язаними. Інформаційні технології та технічні засоби страхування формують базову цифрову інфраструктуру; моделі, методи й алгоритми оцінювання забезпечують оброблення даних і формування профілю кіберризику; спеціалізовані інформаційні технології кіберстрахування забезпечують використання одержаних результатів у процесах андеррайтингу, супроводження договорів, реагування на кіберінциденти та врегулювання страхових випадків.

Для характеристики послідовного розвитку визначених компонентів у моделі передбачено п'ять рівнів впровадження інформаційних технологій у процеси кіберстрахування:

1) початковий, або хаотичний;
2) повторюваний;

3) встановлений;

4) керований;

5) оптимізований.

Зазначені рівні характеризують перехід від несистемного використання окремих програмних і технічних засобів до формалізованого, вимірюваного, інтегрованого та оптимізованого застосування інформаційних технологій. Віднесення до певного рівня здійснюється на підставі ступеня формалізації процесів, організації роботи з даними, інтеграції інформаційних систем, використання результатів оцінювання кіберризиків та можливостей контролю й удосконалення відповідних процесів.

Початковий, або хаотичний, рівень. На початковому рівні процеси кіберстрахування неформалізовані або виконуються фрагментарно. Використання інформаційних технологій має несистемний характер і залежить від поточних потреб, рішень окремих виконавців та доступності конкретних програмних або технічних засобів.

Збирання та оброблення даних про кіберризики здійснюються переважно вручну із застосуванням загальних анкет, електронних документів та окремих експертних оцінок. Спеціалізовані технічні дані про стан кібербезпеки об'єкта страхування використовуються обмежено або несистемно, а результати оцінювання не інтегруються з іншими інформаційними процесами кіберстрахування.

На цьому рівні відсутні узгоджена структура показників, встановлені правила перевірки й агрегування даних та формалізовані інформаційні зв'язки між процесами. Накопичення відомостей про об'єкти страхування, кіберінциденти, страхові випадки та прийняті рішення має нерегулярний характер, що обмежує можливості їх повторного використання й аналізу.

Повторюваний рівень. На повторюваному рівні окремі процеси кіберстрахування виконуються за практиками, які вже застосовувалися організацією та можуть бути повторно відтворені. Формуються типові процедури

збирання даних, оцінювання кіберризиків, андеррайтингу, супроводження договорів і реагування на кіберінциденти, однак вони ще не об'єднані в цілісну систему.

Для реалізації відповідних процесів використовуються типові анкети, електронні форми, клієнтські й брокерські платформи та окремі програмні засоби оцінювання кіберризиків. Частина операцій виконується автоматизовано, проте обмін даними між інформаційними системами залишається обмеженим, а результати оцінювання можуть опрацьовуватися окремо від інших страхових даних.

На цьому рівні накопичуються відомості про об'єкти страхування, кіберризики, кіберінциденти та страхові випадки. Водночас структура, повнота, формат і якість даних можуть відрізнятися залежно від конкретного процесу, підрозділу або застосованого інформаційного засобу, що ускладнює їх інтегроване оброблення й порівняльний аналіз.

Встановлений рівень. На встановленому рівні процеси кіберстрахування формально визначені, документовані та стандартизовані. Для їх виконання застосовуються встановлені процедури, політики, методики, інформаційні системи та програмні засоби, а функції учасників і послідовність виконання основних операцій є узгодженими.

На цьому рівні формується структурована система показників кіберстрахування, визначаються джерела і формати вхідних даних, правила їх перевірки, оброблення та зберігання, а також склад вихідних результатів. Процеси оцінювання кіберризиків, андеррайтингу, супроводження договорів і управління інформацією узгоджуються між собою.

Інформаційні технології та технічні засоби страхування поєднуються з окремими спеціалізованими засобами кіберстрахування. Забезпечується систематичне накопичення страхових, фінансових і кібербезпекових даних, а їх уніфіковане представлення створює можливість для подальшого агрегування, порівняння та аналізу.

Керований рівень. На керованому рівні формалізовані процеси кіберстрахування систематично вимірюються, контролюються та аналізуються. Для цього використовуються кількісні та якісні показники, критерії результативності процесів, індикатори впровадження інформаційних технологій та формалізовані профілі оцінювання.

Результати оцінювання використовуються для управління процесами, планування змін і підтримки прийняття рішень. Здійснюється порівняння фактичних значень показників із визначеними критеріями та цільовими значеннями, виявляються відхилення, а також установлюються процеси й технологічні засоби, що потребують удосконалення.

Інформаційні системи забезпечують інтеграцію даних із різних джерел, їх перевірку, нормування, агрегування та подальший аналіз. Спеціалізовані технічні засоби можуть надавати актуальні дані про стан кібербезпеки об’єкта страхування, а результати їх оброблення використовуються під час оцінювання кіберризиків, андеррайтингу, супроводження договорів і реагування на кіберінциденти.

Оптимізований рівень. На оптимізованому рівні процеси кіберстрахування постійно вдосконалюються на основі результатів їх вимірювання, аналізу накопичених емпіричних даних, технологічних змін і зворотного зв’язку. Виявлені відхилення та результати оцінювання використовуються для коригування процедур, показників, алгоритмів оброблення даних і застосованих інформаційних технологій.

Інформаційні технології інтегруються в основні процеси життєвого циклу кіберстрахування. Автоматизовані засоби можуть використовуватися для збирання та перевірки даних, оцінювання кіберризиків, підтримки андеррайтингу, моніторингу стану об’єкта страхування, реагування на кіберінциденти, інформаційного супроводження врегулювання страхових випадків і перегляду умов страхування.

На цьому рівні можуть застосовуватися технології аналітики великих даних, штучного інтелекту, машинного навчання, блокчейну та смартконтрактів. Їх застосування може забезпечувати виявлення закономірностей у накопичених даних, прогнозування змін характеристик кіберризику, автоматизоване оновлення профілю ризику та формування рекомендацій для підтримки прийняття страхових рішень.

Узагальнені характеристики рівнів впровадження інформаційних технологій у процеси кіберстрахування наведено в таблиці 3.4.

Таблиця 3.4 — Характеристики рівнів впровадження інформаційних технологій у процеси кіберстрахування

Рівень	**Характеристика процесів**	**Використання інформаційних технологій**	**Стан роботи з даними**
Початковий (хаотичний)	Процеси виконуються несистемно та формально не визначені	Окремі програмні засоби й переважно ручні операції	Фрагментарне збирання та оброблення даних
Повторюваний	Окремі процедури можуть бути повторно відтворені	Електронні форми, типові анкети, клієнтські та брокерські платформи	Накопичення частково структурованих даних без належної інтеграції
Встановлений	Процеси документовані, стандартизовані та узгоджені	Інформаційні системи страхування поєднуються з окремими спеціалізованими засобами кіберстрахування	Визначено джерела, структуру, формати та правила оброблення даних
Керований	Процеси систематично вимірюються, контролюються й аналізуються	Інтеграція інформаційних систем, моніторинг і аналітичні засоби	Перевірка, нормування, агрегування й аналіз даних із різних джерел
Оптимізований	Процеси постійно вдосконалюються на основі результатів оцінювання та зворотного зв’язку	Аналітика великих даних, штучний інтелект, машинне навчання, блокчейн-технології та	Виявлення закономірностей, прогнозування та можливість автоматизованого

		автоматизовані засоби оцінювання	оновлення профілю кіберризику

Примітка. Розроблено автором за результатами попереднього дослідження [19].

Застосування запропонованої моделі дає змогу визначити стан впровадження інформаційних технологій у трьох взаємопов'язаних компонентах: загальних процесах страхування, оцінюванні страхових кіберризиків і спеціалізованих процесах кіберстрахування. Для кожного компонента можуть бути встановлені відповідні показники, джерела даних, критерії оцінювання та ознаки досягнення певного рівня.

Оцінювання має охоплювати ступінь формалізації процесів, повноту й структурованість даних, рівень автоматизації операцій, інтеграцію інформаційних систем, застосування спеціалізованих засобів оцінювання кіберризиків і використання одержаних результатів для підтримки прийняття страхових рішень. Склад показників може уточнюватися залежно від мети оцінювання, особливостей об'єкта страхування та доступності вихідних даних.

Таким чином, трикомпонентна п'ятирівнева модель забезпечує структуроване подання напрямів і рівнів впровадження інформаційних технологій у процеси кіберстрахування. Для формування узагальненої кількісної оцінки результати оцінювання окремих компонентів і показників мають бути приведені до порівнянного вигляду та агреговані, що потребує розроблення відповідного індексу зрілості кіберстрахування.

Практичне застосування трикомпонентної п'ятирівневої моделі передбачає послідовний перехід від визначення структури показників до накопичення даних, оцінювання одержаних результатів та формалізації перевірених практик. Для цього запропоновано таку послідовність дій:

1) формування структури фінансово-економічних, організаційних, технологічних і кібербезпекових показників кіберстрахування;

2) проведення первинного оцінювання стану процесів та рівня впровадження інформаційних технологій;

3) визначення пріоритетних напрямів розвитку процесів та інформаційно-технологічного забезпечення кіберстрахування;

4) накопичення, систематизація й аналіз емпіричних даних фінансового, страхового та технічного характеру;

5) формалізація й нормативно-технічне закріплення практик, ефективність яких підтверджено за результатами апробації.

На першому етапі формується структура показників, яка має враховувати міждисциплінарний характер кіберстрахування та поєднувати страхові, фінансово-економічні, організаційні, технологічні й кібербезпекові характеристики. Структурування показників забезпечує визначення логічно пов'язаних груп даних та створює основу для їх подальшого формалізованого представлення, оброблення й оцінювання.

На другому етапі проводиться первинне оцінювання фактичного стану процесів кіберстрахування та рівня впровадження відповідних інформаційних технологій. Оцінювання може здійснюватися із застосуванням структурованих опитувальників, самооцінювання, експертного оцінювання та аналізу наявних даних. Одержані результати дають змогу визначити рівень кожного компонента моделі та виявити процеси, які потребують подальшої формалізації й автоматизації.

На третьому етапі на підставі результатів первинного оцінювання визначаються пріоритетні напрями розвитку процесів та інформаційно-технологічного забезпечення кіберстрахування. Для кожного напряму можуть бути встановлені цільові характеристики, необхідні зміни, відповідні інформаційні технології, джерела даних і критерії перевірки досягнутих результатів.

На четвертому етапі здійснюються накопичення, систематизація та аналіз емпіричних даних фінансового, страхового і технічного характеру. До них можуть належати відомості про страхові премії, страхові виплати й збитки, витрати на реагування та відновлення, характеристики страхового покриття,

показники стану кібербезпеки, відомості про кіберінциденти й уразливості, результати моніторингу та дані про застосовані заходи кіберзахисту.

Накопичення емпіричних даних є необхідною умовою уточнення структури показників, перевірки практичної придатності моделі та вдосконалення процедур оцінювання. Порівняння даних, отриманих у різні періоди, дає змогу аналізувати зміни стану процесів, визначати результативність впровадження інформаційних технологій і коригувати пріоритетні напрями їх подальшого розвитку.

На п’ятому етапі здійснюється формалізація практик, доцільність та результативність яких підтверджено за результатами апробації. Такі практики можуть бути закріплені у внутрішніх документах страхових компаній, методиках оцінювання, технічних вимогах, галузевих рекомендаціях або нормативних документах. Їх формалізація створює умови для повторюваного застосування відповідних процедур та подальшої автоматизації операцій із даними.

Повномасштабна перевірка запропонованої моделі потребує накопичення репрезентативних даних і залучення ширшого кола страхових компаній та інших учасників процесів кіберстрахування. З огляду на обмежений розвиток українського ринку кіберстрахування практичну перевірку окремих положень моделі доцільно здійснювати поетапно із застосуванням структурованих опитувальників, системи показників і процедур первинного оцінювання.

Запропонована трикомпонентна п’ятирівнева модель поєднує інформаційні технології загальних страхових процесів, моделі й методи оцінювання страхових кіберризиків та спеціалізовані інформаційні технології кіберстрахування. Її застосування дає змогу структуровано представити відповідні технології та процеси, визначити стан роботи з даними й встановити послідовність переходу від фрагментарної автоматизації до інтегрованого та керованого використання інформаційних засобів [19].

На відміну від моделі оцінювання ризиків та зрілості кіберстрахування RA&CIMM, що розглядається у розділі 4, запропонована в цьому підрозділі модель характеризує передусім рівень впровадження інформаційних технологій

у процеси кіберстрахування. Вона є методичною передумовою для подальшого визначення показників, їх групування та формування узагальненої індексної оцінки.

Таким чином, для кількісного подання результатів оцінювання окремих компонентів і показників необхідно привести різнорідні дані до порівнянного вигляду та здійснити їх агрегування. Методичні положення формування відповідного індексу зрілості кіберстрахування розглянуто в наступному підрозділі.

3.5. Формування індексу зрілості кіберстрахування

Результати систематизації процесів кіберстрахування, інформаційних технологій та моделей їх впровадження створюють основу для формування узагальненого показника, що характеризує рівень розвитку, формалізації, технологічного забезпечення та практичного впровадження відповідних процесів. Для розв’язання цієї задачі у попередніх дослідженнях автора запропоновано індекс кіберстрахування, який у межах цього дослідження розглядається як індекс зрілості кіберстрахування.

Необхідність формування окремого індексу зумовлена тим, що в розглянутих у розділі 1 індексних моделях кібербезпеки процеси кіберстрахування не представлені як самостійний об’єкт оцінювання. Такі індекси орієнтовані переважно на оцінювання стану кібербезпеки держави, сектору, організації, інформаційної системи або сукупності технічних та організаційних заходів кіберзахисту. Водночас кіберстрахування охоплює додаткові процеси оцінювання страхових кіберризиків, андеррайтингу, управління страховим покриттям, інформаційної взаємодії страхувальника і

страховика, реагування на кіберінциденти та використання спеціалізованих інформаційних технологій.

Індекс зрілості кіберстрахування розглядається як багатодоменний індикатор високого рівня в межах розроблюваного індексного підходу. Його призначення полягає в узагальненому поданні стану процесів кіберстрахування та рівня впровадження інформаційних технологій і технічних засобів у відповідній предметній області.

Формування індексу ґрунтується на системному підході, відповідно до якого кіберстрахування розглядається як сукупність взаємопов'язаних процесів, показників та інформаційних технологій. Структура індексу формується з урахуванням міждисциплінарного характеру кіберстрахування та поєднання страхових, фінансово-економічних, технологічних і кібербезпекових складових.

Для характеристики стану процесів кіберстрахування та рівня їх впровадження запропоновано використовувати індекс кіберстрахування, або індекс зрілості кіберстрахування I_{ci}. У попередньому дослідженні автора [19] до показників p_j, які можуть використовуватися під час його формування, віднесено:

- кількість або частку впроваджених процесів кіберстрахування;
- рівень зрілості або ефективність впроваджених процесів кіберстрахування;
- глибину проникнення інформаційних технологій до основних процесів кіберстрахування, визначену із застосуванням методу експертного оцінювання, зокрема шляхом самооцінювання;
- кількість або частку та рівень зрілості або ефективність процесів із застосуванням технологій Індустрії 4.0 [19, 154];
- відсоток збільшення виручки, отриманої після впровадження інформаційних технологій, зокрема технологій Індустрії 4.0.

Зазначений перелік показників p_j визначено у попередньому дослідженні автора [19] і може уточнюватися залежно від поставленої задачі та обраної структури індексу. У межах цього дисертаційного дослідження основну увагу

зосереджено на показниках, що характеризують ступінь впровадження, формалізації та зрілості процесів кіберстрахування, а також рівень використання інформаційних технологій у відповідних процесах. Показники результативності діяльності, зокрема зміни виручки після впровадження інформаційних технологій, можуть використовуватися як додаткові характеристики результатів їх застосування.

Показник кількості або частки впроваджених процесів кіберстрахування характеризує ступінь практичної реалізації основних процесів, розглянутих у підрозділі 3.1. До них належать оцінювання кіберризиків, кіберзбитків та засобів їх контролю; управління кіберризиками; типізація та категоризація кіберінцидентів; управління наслідками кіберінцидентів; управління інформаційною безпекою під час обміну даними зі страховиком; управління полісом кіберстрахування, підтвердженнями, витратами на реагування на кіберінциденти та кіберстраховим покриттям; андеррайтинг кіберстрахування; збирання інформації з інформаційних активів; виконання зобов'язань, пов'язаних з інформаційною безпекою.

Рівень зрілості впроваджених процесів характеризує не лише факт їх наявності, а й ступінь формалізації, повторюваності, керованості та використання інформаційних технологій під час їх реалізації. Відповідний показник пов'язаний із рівнями впровадження інформаційних технологій, визначеними у трикомпонентній п'ятирівневій моделі, розглянутій у підрозділі 3.4.

Глибина проникнення інформаційних технологій до основних процесів кіберстрахування характеризує ступінь використання відповідних технологій та засобів автоматизації у процесах збирання, представлення, оброблення й аналізу даних, оцінювання кіберризиків, андеррайтингу, супроводження договорів, моніторингу стану кібербезпеки, реагування на кіберінциденти та управління страховими претензіями. Відповідно до запропонованого підходу глибина проникнення інформаційних технологій може визначатися із застосуванням експертного оцінювання, зокрема шляхом самооцінювання.

Кількість або частка та рівень зрілості процесів із застосуванням технологій Індустрії 4.0 характеризують ступінь використання сучасних інформаційних технологій у процесах кіберстрахування.

Показник зміни виручки після впровадження інформаційних технологій характеризує результативний економічний ефект їх застосування та може використовуватися як додаткова характеристика поряд із показниками зрілості процесів і рівня їх технологічного забезпечення.

Для формування доменної структури індексу предметні області застосування інформаційних технологій, систематизовані у підрозділі 3.3, можуть використовуватися як домени d_l, у межах яких групуються відповідні показники p_j індексу зрілості кіберстрахування I_{ci}. У попередньому дослідженні автора [19] до таких предметних областей віднесено:

1) технології електронного бізнесу;
2) контент-аналіз;
3) мобільні системи підтримки;
4) інтеграцію інформаційних ресурсів;
5) аналітику великих даних, штучний інтелект, машинне навчання та оброблення природної мови;
6) блокчейн і смартконтракти;
7) математичне, імітаційне та статистичне моделювання.

Зазначений перелік відповідає класифікації інформаційних технологій, використаній у попередньому дослідженні автора [19]. Відповідні предметні області утворюють доменну структуру, призначену для систематизації та групування показників індексу. Перелік доменів може уточнюватися залежно від поставленої задачі, складу показників та особливостей об'єкта оцінювання.

Доменну структуру індексу I_{ci}, сформовану за предметними областями застосування інформаційних технологій, слід відрізняти від доменної структури RA&CIMM, у межах якої здійснюється комплексне поєднання результатів

оцінювання ризиків інформаційної безпеки, кіберризиків та зрілості процесів кіберстрахування.

Для узагальненого математичного подання індексу кіберстрахування показники p_j розглядаються у межах відповідних доменів d_l. З урахуванням перехресних вагових коефіцієнтів індекс кіберстрахування I_{ci} у попередньому дослідженні автора [19] представлено у вигляді:

$$I_{ci} = \sum_{jl} \alpha_{jl} p_j d_l$$

де I_{ci} — індекс кіберстрахування, або індекс зрілості кіберстрахування;

p_j — показники індексу;

d_l — домени, що відповідають визначеним предметним областям застосування інформаційних технологій;

α_{jl} — перехресні вагові коефіцієнти.

Значення показників p_j характеризують окремі аспекти впровадження процесів та інформаційних технологій кіберстрахування. Їх систематизація за визначеними доменами d_l та подальше агрегування з урахуванням вагових коефіцієнтів забезпечують формування узагальненого кількісного подання рівня зрілості кіберстрахування.

Перелік доменів d_l, як і перелік показників p_j, не є остаточним і може уточнюватися залежно від поставленої задачі та обраної структури індексу. Такий підхід забезпечує можливість адаптації структури індексу до особливостей об’єкта оцінювання, доступних вихідних даних та складу інформаційних технологій, що використовуються у процесах кіберстрахування.

Формування індексу зрілості кіберстрахування передбачає послідовне виконання операцій з отримання, структуризації та агрегування даних. На першому етапі визначаються значення показників p_j, що характеризують відповідні процеси та рівень використання інформаційних технологій. На другому етапі показники систематизуються за визначеними доменами d_l. На

третьому етапі здійснюється їх приведення до порівнянного вигляду та агрегування з урахуванням встановлених вагових коефіцієнтів. Приведення значень показників до порівнянного вигляду здійснюється відповідно до процедур чисельної індикації та нормування, обґрунтованих у розділі 2. Результатом є узагальнене значення індексу I_{ci} та сукупність оцінок за окремими доменами і показниками.

Результати оцінювання можуть бути представлені не лише узагальненим значенням індексу, а й у вигляді профілю, що характеризує стан окремих доменів і показників. Таке подання дає змогу виявляти складові з відносно нижчим або вищим рівнем зрілості та використовувати одержану інформацію для визначення напрямів подальшого розвитку процесів і інформаційно-технологічного забезпечення кіберстрахування.

Поточний профіль характеризує фактичний стан процесів, інформаційних технологій і технічних засобів на момент проведення оцінювання. Цільовий профіль визначає бажаний стан відповідних процесів і технологій. Порівняння поточного та цільового профілів дає змогу визначити відхилення за окремими показниками і доменами та сформувати напрями подальшого вдосконалення.

На початковому етапі джерелом даних для визначення окремих показників може бути самооцінювання. Застосування самооцінювання передбачено, зокрема, для визначення глибини проникнення інформаційних технологій до основних процесів кіберстрахування [19]. Результати самооцінювання формують структурований масив вихідних даних, який може використовуватися для визначення значень показників, формування доменних оцінок та побудови поточного профілю.

Індекс зрілості кіберстрахування може використовуватися для характеристики стану процесів та рівня впровадження інформаційних технологій, а також для порівняння результатів оцінювання у різні моменти часу за умови застосування узгодженої структури показників, доменів і процедури їх оброблення.

Результати індексного оцінювання можуть використовуватися як структурована інформаційна основа для аналізу стану процесів кіберстрахування та інформаційної підтримки прийняття управлінських і страхових рішень.

При цьому індекс зрілості кіберстрахування не слід ототожнювати з безпосереднім визначенням страхового тарифу, страхової премії або умов страхового договору. Його призначення полягає у кількісному та профільному поданні рівня розвитку, формалізації та технологічного забезпечення процесів кіберстрахування. Одержані результати можуть використовуватися разом з іншими показниками оцінювання кіберризиків як інформаційна основа для підтримки прийняття страхових рішень.

Практичне застосування індексу потребує накопичення емпіричних даних, необхідних для подальшого уточнення складу показників p_j, доменів d_l, вагових коефіцієнтів та критеріїв інтерпретації одержаних результатів. У попередньому дослідженні автора [19] подальше розроблення узагальненої моделі індексу кіберстрахування та оцінювання ефективності її застосування визначено як напрям подальших досліджень.

Подальший розвиток запропонованого індексного підходу полягає у його інтеграції з оцінюванням ризиків інформаційної безпеки та кіберризиків. Якщо індекс I_{ci} характеризує насамперед зрілість процесів кіберстрахування та рівень впровадження відповідних інформаційних технологій, то комплексне поєднання оцінювання ризиків і зрілості здійснюється у моделі оцінювання ризиків та зрілості кіберстрахування RA&CIMM, розглянутій у розділі 4.

Таким чином, у межах цього розділу здійснено перехід від систематизації та формалізації процесів кіберстрахування до визначення інформаційних технологій їх автоматизації, розроблення трикомпонентної п’ятирівневої моделі їх впровадження та формування індексу зрілості кіберстрахування I_{ci}. Запропонований індекс забезпечує структуроване кількісне та профільне подання стану процесів і рівня впровадження інформаційних технологій у

кіберстрахуванні та створює передумови для його подальшого використання у комплексному оцінюванні ризиків і зрілості в межах RA&CIMM.

Висновки до розділу 3

У результаті дослідження процесів кіберстрахування, інформаційних технологій їх автоматизації та підходів до оцінювання рівня їх впровадження одержано такі результати.

1. Проведено аналіз нормативних документів, стандартів і фреймворків, що визначають процеси кіберстрахування, оцінювання кіберризиків, інформаційний обмін між страховиком і страхувальником, управління страховим покриттям та виконання зобов'язань у сфері інформаційної безпеки. Систематизовано основні процеси кіберстрахування, пов'язані з оцінюванням і управлінням кіберризиками, обробленням інформації про кіберінциденти, андеррайтингом, управлінням страховим покриттям, реагуванням на кіберінциденти та виконанням зобов'язань, пов'язаних з інформаційною безпекою.

2. Визначено, що систематизовані процеси кіберстрахування можуть розглядатися як об'єкти алгоритмізації та автоматизації, оскільки передбачають виконання послідовних операцій зі збирання, представлення, перевірки, передавання, накопичення, класифікації, систематизації, оброблення та аналізу даних. Формалізовано структуру відповідних інформаційних процесів через визначення вхідних даних, правил їх перевірки й оброблення та вихідних результатів, що створює основу для подальшої алгоритмічної реалізації відповідних процедур.

3. Систематизовано інформаційні технології, які застосовуються або можуть застосовуватися у процесах страхування та кіберстрахування. До

основних предметних областей віднесено технології електронного бізнесу; контент-аналіз; мобільні системи підтримки; інтеграцію інформаційних ресурсів; аналітику великих даних, штучний інтелект, машинне навчання та оброблення природної мови; блокчейн і смартконтракти; математичне, імітаційне та статистичне моделювання. Визначено можливості їх застосування для автоматизації операцій з даними, оцінювання кіберризиків, андеррайтингу, моніторингу стану кібербезпеки, реагування на кіберінциденти та інформаційної підтримки прийняття страхових рішень.

4. Систематизовано моделі та методи, що можуть використовуватися під час оцінювання кіберризиків і підтримки процесів кіберстрахування. Встановлено, що вибір відповідного математичного або інформаційного інструментарію визначається метою оцінювання, структурою і доступністю вихідних даних, необхідністю врахування невизначеності та видом результатів, які мають бути сформовані.

5. Розроблено трикомпонентну п’ятирівневу модель впровадження інформаційних технологій у процеси кіберстрахування. Модель охоплює три взаємопов’язані компоненти: інформаційні технології та технічні засоби страхування; моделі, методи та інформаційні засоби оцінювання страхових кіберризиків; спеціалізовані інформаційні технології та технічні засоби кіберстрахування. Визначено п’ять послідовних рівнів їх впровадження: початковий, або хаотичний; повторюваний; встановлений; керований; оптимізований. Модель забезпечує структуроване подання стану впровадження інформаційних технологій та визначення напрямів переходу від фрагментарного до інтегрованого і керованого використання інформаційних засобів у процесах кіберстрахування.

6. Сформовано підхід до побудови індексу кіберстрахування, який у межах дисертаційного дослідження розглядається як індекс зрілості кіберстрахування I_{ci}. Визначено показники p_j, що характеризують ступінь впровадження і зрілості процесів, рівень використання інформаційних технологій

та окремі результативні характеристики їх застосування. Предметні області інформаційних технологій використано для формування доменної структури d_l, у межах якої здійснюється систематизація відповідних показників.

7. Запропоновано математичне подання індексу зрілості кіберстрахування I_{ci} на основі показників p_j, доменів d_l та перехресних вагових коефіцієнтів. Формування індексу передбачає визначення значень показників, їх систематизацію за доменами, приведення до порівнянного вигляду та агрегування з урахуванням вагових характеристик. Результат оцінювання може бути представлений у вигляді узагальненого значення індексу та профілю окремих доменів і показників, що забезпечує структуроване кількісне подання рівня зрілості процесів і впровадження інформаційних технологій у кіберстрахуванні.

Таким чином, у Розділі 3 здійснено перехід від систематизації процесів кіберстрахування до їх формалізованого представлення як інформаційних процесів, визначення можливостей алгоритмізації й автоматизації, систематизації інформаційних технологій, розроблення трикомпонентної п’ятирівневої моделі їх впровадження та формування індексу зрілості кіберстрахування I_{ci}.

Одержані у Розділі 3 результати надалі використовуються для поєднання оцінювання зрілості процесів кіберстрахування з оцінюванням ризиків інформаційної безпеки та кіберризиків у межах моделі оцінювання ризиків та зрілості кіберстрахування RA&CIMM.

РОЗДІЛ 4. МОДЕЛЬ, МЕТОД ТА АЛГОРИТМ ОЦІНЮВАННЯ РИЗИКІВ І ЗРІЛОСТІ КІБЕРСТРАХУВАННЯ

4.1. Концептуальні засади та структура моделі RA&CIMM

У розділі 2 встановлено, що індексний підхід дає змогу структурувати різнорідні показники у вигляді доменів, піддоменів та індикаторів і здійснювати перехід від окремих значень показників до групових, доменних та інтегральних оцінок. Використання базових індикаторів забезпечує скорочення початкової множини показників і формування профілю захищеності або зрілості об'єкта оцінювання.

У розділі 3 систематизовано й формалізовано інформаційні процеси кіберстрахування, визначено інформаційні технології їх автоматизації, розроблено трикомпонентну п'ятирівневу модель їх упровадження та сформовано підхід до побудови індексу зрілості кіберстрахування I_{ci}.

Подальше розв'язання поставленого науково-прикладного завдання потребує інтеграції зазначених результатів у межах єдиної моделі, що забезпечує структуризацію, оброблення та аналіз різнорідних даних про ризики інформаційної безпеки, кіберризики, технічний стан інформаційно-комунікаційної системи та зрілість процесів кіберстрахування для формування комплексної оцінки й інформаційної підтримки прийняття рішень.

У попередньому дослідженні автора запропоновано модель оцінювання ризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model, RA&CIMM). RA&CIMM є гібридною моделлю, призначеною для комплексного оцінювання ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування суб'єкта оцінювання з урахуванням технічного стану його інформаційно-комунікаційної системи [37].

Методологічну основу RA&CIMM становить ризик-орієнтований підхід. Відповідно до нього управлінські рішення щодо впровадження заходів з інформаційної безпеки та кіберзахисту приймаються на підставі аналізу й порівняння поточних рівнів ризиків інформаційної безпеки та кіберризиків із прийнятними рівнями.

Процедура оцінювання, покладена в основу моделі, передбачає збирання, структуризацію, оброблення й аналіз даних, що характеризують процеси управління ризиками інформаційної безпеки та кіберризиками, заходи із забезпечення інформаційної безпеки й кіберзахисту, а також особливості функціонування інформаційно-комунікаційної системи суб'єкта оцінювання.

Нормативну основу відповідного підходу становлять положення ДСТУ IEC/ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику», ISO/IEC 27102:2019 «Інформаційна безпека, кібербезпека та захист приватності. Настанови щодо кіберстрахування», Рамкової основи кібербезпеки NIST 2.0, Європейської рамки сертифікації кібербезпеки, визначеної Регламентом (ЄС) 2019/881, а також нормативні вимоги Національного банку України щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг [3, 12, 60, 123, 155].

Вихідним положенням RA&CIMM є взаємозв'язок операційного ризику, ризику інформаційної безпеки та кіберризику. Кіберризик пов'язаний із можливістю виникнення негативних наслідків унаслідок реалізації кіберзагроз щодо інформаційних ресурсів та інформаційної інфраструктури. Якщо реалізація кіберзагрози призводить до порушення операційних процесів суб'єкта оцінювання, відповідний кіберризик розглядається як складова операційного ризику [3, 44, 61].

Ризик інформаційної безпеки пов'язаний із можливістю виникнення негативних наслідків унаслідок порушення конфіденційності, цілісності або доступності інформації та інформаційних систем [3, 58]. У межах RA&CIMM ризик інформаційної безпеки та кіберризик розглядаються як взаємопов'язані

категорії, а їх вплив на операційний ризик визначається з урахуванням джерела загрози, об'єкта впливу та можливих наслідків для операційних процесів.

У нормативних актах Національного банку України, що регулюють діяльність окремих суб'єктів фінансового сектору, операційний ризик пов'язується, зокрема, з недоліками внутрішніх процесів, діями персоналу, неналежним функціонуванням інформаційних систем і впливом зовнішніх подій [156, 157]. Ризик інформаційної безпеки при цьому розглядається як складова операційного ризику, що може виникати внаслідок порушення конфіденційності, цілісності або доступності інформації, кібератак та інших зовнішніх подій [157]. Відповідні нормативні визначення використано в дослідженні для уточнення взаємозв'язку операційного ризику, ризику інформаційної безпеки та кіберризику, без їх безпосереднього перенесення на діяльність страховиків.

У межах RA&CIMM оцінюється сукупність взаємопов'язаних характеристик ризиків інформаційної безпеки та кіберризиків, процесів управління ними, заходів із забезпечення інформаційної безпеки й кіберзахисту, технічного стану інформаційно-комунікаційної системи та зрілості процесів кіберстрахування.

RA&CIMM ґрунтується на принципах системного та ризик-орієнтованого підходів, доменної структуризації показників і багаторівневої перевірки результатів. Функціональним призначенням моделі є формування комплексної оцінки на основі часткових показників і доменних підіндексів, кожен із яких характеризує окрему складову стану суб'єкта оцінювання. Одержані результати використовуються для формування структурованого профілю ризиків і зрілості та інформаційної підтримки прийняття рішень у процесах кіберстрахування.

Структура RA&CIMM охоплює три взаємопов'язані домени: експертний домен оцінювання ризиків інформаційної безпеки та кіберризиків; мережевий домен оцінювання ризиків інформаційної безпеки та кіберризиків; домен оцінювання зрілості процесів кіберстрахування [37].

Перший домен призначений для експертного оцінювання ризиків інформаційної безпеки та кіберризиків. Вхідними даними для такого оцінювання є показники, що характеризують управління кібербезпекою, технічні вразливості, кіберзагрози та їх можливий вплив, операційну стійкість, людський фактор, ризики третіх сторін і ланцюгів постачання, відповідність нормативним вимогам, а також фінансові та страхові характеристики ризику.

За результатами експертного оцінювання формується структуроване подання характеристик ризику, які не завжди можуть бути безпосередньо визначені засобами технічного моніторингу. До них належать наявність і стан реалізації політик, розподіл відповідальності, участь керівництва в управлінні кібербезпекою, організація резервування та відновлення, рівень обізнаності персоналу, залежність від постачальників і стан виконання нормативних вимог. Одержані значення використовуються для формування експертної складової профілю ризику.

Другий домен RA&CIMM призначений для мережевого оцінювання ризиків інформаційної безпеки та кіберризиків. Його застосування забезпечує доповнення результатів експертного оцінювання технічними даними, одержаними під час дослідження інформаційно-комунікаційної системи суб'єкта оцінювання.

Мережеве оцінювання може охоплювати результати тестування на проникнення, аналізу вразливостей, мережевого трафіку, журналів подій та інших технічних даних, що характеризують стан інформаційно-комунікаційної системи. Відповідні дані підлягають перевірці, структуризації та перетворенню на показники, які формують технічну складову профілю ризику.

Виділення експертного та мережевого доменів забезпечує використання двох взаємопов'язаних груп даних. Перша група характеризує організаційні, управлінські, кадрові, нормативні, фінансові та страхові аспекти ризику. Друга група характеризує технічний стан інформаційно-комунікаційної системи.

Поєднання цих груп дає змогу зіставляти результати експертного оцінювання з даними технічного дослідження.

Третій домен RA&CIMM призначений для оцінювання зрілості процесів кіберстрахування. Його основу становлять результати систематизації стандартизованих процесів кіберстрахування, інформаційних технологій їх реалізації, трикомпонентної п'ятирівневої моделі впровадження інформаційних технологій та підходу до формування індексу зрілості кіберстрахування I_{ci}, розглянутих у розділі 3 [19, 37].

Оцінювання зрілості процесів кіберстрахування передбачає визначення рівня їх розроблення, формалізації та впровадження, ступеня використання й інтеграції інформаційних технологій, рівня автоматизації операцій з даними, а також застосування сучасних технологічних і технічних рішень.

Результати оцінювання відповідних показників використовуються для формування доменного підіндексу та профілю зрілості процесів кіберстрахування. Отже, ця складова включається до загальної структури RA&CIMM поряд із результатами експертного та мережевого оцінювання ризиків.

Тридоменна структура RA&CIMM забезпечує поєднання різнорідних даних, що відрізняються за джерелами та способами отримання. Експертні показники формуються на основі структурованого оцінювання організаційних, управлінських і процесних характеристик. Мережеві показники формуються на основі результатів технічного дослідження інформаційно-комунікаційної системи. Показники зрілості характеризують стан процесів кіберстрахування та рівень впровадження відповідних інформаційних технологій.

Використання доменної структури відповідає розробленому в розділі 2 підходу до подання складного об'єкта оцінювання у вигляді сукупності логічно пов'язаних груп показників. Кожний домен RA&CIMM утворює окрему область оцінювання та містить відповідні підіндекси й індикатори.

Поряд із доменною структурою в RA&CIMM застосовується багаторівнева процедура отримання, перевірки та уточнення даних. Вона охоплює чотири послідовні рівні: самооцінювання (self-assessment); зовнішнє оцінювання (external assessment); експертна перевірка (expert review); повторне оцінювання (re-assessment) [37].

Самооцінювання є початковим рівнем збирання даних. Суб'єкт оцінювання надає інформацію за структурованими опитувальниками відповідно до визначених критеріїв RA&CIMM. Використання таких опитувальників забезпечує уніфікацію первинного збирання та представлення даних, оскільки кожне питання або критерій пов'язується з відповідними показниками й підіндексами моделі.

Зовнішнє оцінювання передбачає перевірку, підтвердження та уточнення результатів самооцінювання на основі доступних документів, відомостей про стан відповідних процесів та іншої інформації про суб'єкта оцінювання. За результатами такої перевірки первинні значення показників можуть бути підтверджені або скориговані.

Експертна перевірка як третій рівень процедури застосовується для визначення складних багатофакторних характеристик ризику, які не можуть бути повністю встановлені за результатами самооцінювання, зовнішньої перевірки документів або автоматизованого технічного контролю. Одержані експертні оцінки подаються у формалізованому вигляді та пов'язуються з відповідними показниками й підіндексами RA&CIMM.

Технічне дослідження інформаційно-комунікаційної системи здійснюється в межах мережевого домену RA&CIMM і не утворює окремого рівня процедури оцінювання. Його результати проходять перевірку та формалізоване оброблення, після чого використовуються для визначення показників і підіндексів мережевого домену.

Повторне оцінювання передбачає збирання нового набору даних після завершення попереднього циклу оцінювання. Порівняння одержаних значень із

результатами попереднього циклу дає змогу визначити зміни окремих показників, підіндексів і загального профілю ризиків та зрілості в різні моменти часу.

Отже, домени RA&CIMM визначають логічну структуру показників і результатів оцінювання, а рівні процедури — послідовність збирання, перевірки, уточнення та повторного отримання даних. Таке розмежування дає змогу окремо визначити склад оцінюваних характеристик і порядок виконання операцій над відповідними даними.

Основною структурною одиницею результату оцінювання є підіндекс, що характеризує окрему логічно пов'язану групу показників у межах відповідного домену RA&CIMM.

Сукупність доменних підіндексів формує профіль ризиків та зрілості, який відображає співвідношення окремих характеристик суб'єкта оцінювання і дає змогу визначити складові з відносно вищими або нижчими значеннями оцінки.

Використання такого профілю має принципове значення, оскільки однакове значення інтегрального індексу може бути одержане за різного співвідношення доменних підіндексів. Тому інтегральний індекс доцільно аналізувати разом із результатами доменного та підіндексного оцінювання.

У RA&CIMM використовується початковий експертний профіль, що визначає основні й додаткові підіндекси, їх початкові вагові характеристики та зміст відповідних областей оцінювання [37]. Структуру початкового експертного профілю детально розглянуто в підрозділі 4.2.

Для інтерпретації результатів оцінювання ризиків у RA&CIMM використовується стобальна шкала, за якою значення 100 відповідає максимальному рівню ризику. За цілими значеннями шкали встановлено такі інтервали: 0–20 — дуже низький ризик; 21–40 — низький ризик; 41–60 — середній ризик; 61–80 — високий ризик; 81–100 — критичний ризик.

Для оцінювання зрілості процесів кіберстрахування також використовується стобальна шкала, за якою значення 100 відповідає максимальному рівню зрілості. Встановлено такі інтервали: 0–20 — початковий,

або хаотичний, рівень; 21–40 — повторюваний; 41–60 — встановлений; 61–80 — керований; 81–100 — оптимізований рівень [37].

Для дробових оцінок наведені діапазони застосовуються без розривів: від 0 до 20 балів включно; понад 20 до 40 балів включно; понад 40 до 60 балів включно; понад 60 до 80 балів включно; понад 80 до 100 балів включно.

Застосування двох шкал забезпечує окрему інтерпретацію ризику та зрілості. Для показників ризику збільшення значення відповідає зростанню рівня ризику, тоді як для показників зрілості збільшення значення характеризує підвищення рівня зрілості процесів кіберстрахування.

Результати оцінювання ризиків і зрілості за RA&CIMM можуть використовуватися як інформаційна основа для визначення пріоритетності заходів реагування, обґрунтування потреби у страховому покритті, підготовки рекомендацій щодо його умов і визначення напрямів інвестування в інформаційну безпеку та кіберзахист. Водночас одержані оцінки не є безпосереднім розрахунком страхової премії, франшизи або ліміту страхового покриття та потребують подальшого актуарного обґрунтування.

Результатом застосування RA&CIMM є не лише чисельне значення інтегрального індексу, а й структурований профіль ризиків і зрілості, представлений сукупністю доменних підіндексів та окремих показників. Такий профіль дає змогу визначити складові з підвищеними значеннями ризику або недостатнім рівнем зрілості та підготувати інформацію для підтримки прийняття рішень у процесах кіберстрахування.

RA&CIMM може бути адаптована для оцінювання організацій різних форм власності, зокрема операторів критичної інфраструктури, а також для інформаційної підтримки страхового андеррайтингу. Практичне застосування моделі потребує врахування особливостей об’єкта оцінювання, складу доступних даних, галузевих вимог і визначених критеріїв прийнятності ризику.

RA&CIMM визначає формальну структуру представлення та оброблення різнорідних даних оцінювання. Доменна декомпозиція забезпечує

структуризацію показників за логічними областями, багаторівнева процедура визначає послідовність збирання, перевірки й уточнення даних, а підіндекси та інтегральний індекс відображають результати їх агрегування на відповідних рівнях моделі.

Отже, RA&CIMM є центральною моделлю, що інтегрує результати попередніх етапів дослідження. У її межах поєднано індексний підхід, систему базисних параметрів, доменну структуризацію показників, стандартизовані процеси кіберстрахування та оцінювання зрілості процесів кіберстрахування. Модель визначає склад і взаємозв'язки основних компонентів оцінювання, створюючи основу для подальшого розроблення відповідних методів та алгоритмічних процедур.

Подальша деталізація RA&CIMM потребує визначення структури її доменів, складу основних і додаткових підіндексів та початкового експертного профілю моделі. Зазначені складові розглянуто в підрозділі 4.2.

4.2. Доменна структура та початковий експертний профіль RA&CIMM

В основу RA&CIMM покладено доменне представлення даних і результатів оцінювання. Такий підхід передбачає розподіл показників за окремими логічними областями відповідно до джерел даних, способів їх отримання та змісту характеристик суб'єкта оцінювання.

Доменна структура RA&CIMM охоплює експертний домен оцінювання ризиків інформаційної безпеки та кіберризиків, мережевий домен їх оцінювання і домен оцінювання зрілості процесів кіберстрахування. У межах кожного домену окремі індикатори об'єднуються у відповідні підіндекси, які характеризують визначені складові ризику або зрілості [37].

Побудова RA&CIMM на основі доменної декомпозиції відповідає системному підходу, за якого складний об’єкт оцінювання подається у вигляді сукупності взаємопов’язаних компонентів. У моделі такими компонентами є організаційні та процесні характеристики ризику, технічний стан інформаційно-комунікаційної системи та зрілість процесів кіберстрахування.

Функціональним призначенням доменної декомпозиції є формування структури даних, придатної для їх послідовного збирання, перевірки, групування та агрегування. Значення окремих індикаторів утворюють часткові внески, на основі яких формуються підіндекси, а результати підіндексного оцінювання використовуються для обчислення інтегрального індексу RA&CIMM.

У початковій редакції RA&CIMM структуру складових моделі та їх вагові характеристики подано у вигляді початкового експертного профілю. Профіль містить основні й додаткові підіндекси, їх початкові вагові значення та характеристики відповідних областей оцінювання [37].

У початковому експертному профілі RA&CIMM визначено три основні групи, що охоплюють 15 додаткових складових оцінювання. Основні групи початкового профілю співвіднесено з трьома доменами RA&CIMM: експертним, мережевим і доменом оцінювання зрілості процесів кіберстрахування. Їх структуру, початкові вагові значення та характеристики наведено в таблиці 4.1.

Таблиця 4.1 — Структура початкового експертного профілю RA&CIMM

Основні підіндекси	**Складові оцінювання**	**Початкове вагове значення**	**Характеристика**
Експертне оцінювання ризиків	Підіндекс ризику управління кібербезпекою (Governance Risk)	0,08	Характеризує якість управління кібербезпекою, наявність політик, розподіл відповідальності та участь керівництва
	Підіндекс ризику технічних вразливостей (Technical Vulnerability Risk)	0,10	Оцінює технічні вразливості, швидкість патч-менеджменту та рівень захищеності інфраструктури

	Підіндекс впливу кіберзагроз (Threat Exposure Risk)	0,07	Характеризує рівень зовнішнього впливу кіберзагроз і доступність інформаційної інфраструктури для потенційного атакувальника
	Підіндекс ризику операційної стійкості (Operational Resilience Risk)	0,05	Характеризує резервне копіювання, аварійне відновлення та стійкість до кіберінцидентів
	Підіндекс ризику людського фактора (Human Factor Risk)	0,05	Враховує рівень обізнаності персоналу, його сприйнятливість до фішингових атак і ризики, пов'язані з діями внутрішніх порушників.
	Підіндекс ризику третіх сторін і ланцюгів постачання (Third-Party and Supply Chain Risk)	0,05	Характеризує ризики постачальників і залежність від зовнішніх сервісів
	Підіндекс ризику невідповідності нормативним вимогам (Compliance Risk)	0,05	Характеризує ризик невиконання встановлених нормативних вимог
	Підіндекс фінансового та страхового ризику (Financial and Insurance Risk)	0,05	Оцінює очікувані збитки, наявне страхове покриття та можливість страхування відповідного ризику
Мережеве оцінювання ризиків	Тестування на проникнення (Penetration Testing)	0,10	Характеризує рівень захищеності інформаційно-комунікаційної системи за результатами контрольованого моделювання кібератак і перевірки можливості експлуатації виявлених вразливостей
	Оцінювання вразливостей (Vulnerability Assessment)	0,10	Відображає наявність, критичність і кількість технічних вразливостей у програмному забезпеченні, мережах та інформаційній інфраструктурі

	Автоматизоване оцінювання за відкритими джерелами (Automated OSINT Assessment)	0,02	Оцінює рівень зовнішньої інформаційної експозиції за даними з відкритих джерел
	Управління поверхнею атаки (Attack Surface Management)	0,03	Враховує масштаб, видимість та рівень захищеності зовнішньої цифрової поверхні
Оцінювання зрілості процесів кіберстрахування	Самооцінювання (Self-assessment)	0,10	Передбачає внутрішнє оцінювання політик, процесів, засобів контролю та ресурсів організації
	Зовнішнє оцінювання (External Assessment)	0,10	Передбачає незалежну перевірку й уточнення результатів самооцінювання на основі документів, відомостей про стан процесів та інших доступних даних
	Повторне оцінювання (Re-assessment)	0,05	Характеризує динаміку зміни рівня ризику та результативність впроваджених заходів кіберзахисту

Примітка. Наведені значення є початковими ваговими характеристиками складових експертного профілю RA&CIMM і не є результатами оцінювання конкретного суб'єкта. Самооцінювання, зовнішнє та повторне оцінювання подано як процедурні складові початкового профілю, що визначають джерела та цикли отримання даних для оцінювання зрілості. Вони не є самостійними змістовими підіндексами. Експертна перевірка використовується як окремий процедурний рівень уточнення результатів і не має самостійного вагового значення.

Джерело: сформовано автором за [37].

Початковий експертний профіль є вихідним поданням структури RA&CIMM. Його призначення полягає у визначенні груп показників, що враховуються під час формування підіндексів моделі, а також початкових вагових характеристик відповідних складових.

Сума початкових вагових значень складових експертного домену становить 0,50, мережевого домену — 0,25, домену оцінювання зрілості процесів

кіберстрахування — 0,25. Загальна сума початкових вагових значень усіх складових профілю дорівнює 1,00.

У межах експертного домену найбільше початкове вагове значення встановлено для підіндексу ризику технічних вразливостей — 0,10. Вагове значення підіндексу ризику управління кібербезпекою становить 0,08, а підіндексу впливу кіберзагроз — 0,07. Для підіндексів ризику операційної стійкості, людського фактора, третіх сторін і ланцюгів постачання, невідповідності нормативним вимогам, а також фінансового та страхового ризику встановлено вагові значення по 0,05.

Розподіл початкових вагових значень відображає експертне подання відносного внеску окремих складових у результат оцінювання. Надалі ці значення можуть уточнюватися із застосуванням формалізованих експертних методів.

Підіндекс ризику управління кібербезпекою (Governance Risk) характеризує якість управління кібербезпекою, наявність і стан реалізації відповідних політик, розподіл відповідальності, порядок прийняття рішень та участь керівництва у процесах управління кіберризиками. Зазначені характеристики доповнюють результати технічного оцінювання, оскільки наявність засобів захисту сама по собі не забезпечує належної організації управління ризиками.

У початковому експертному профілі вагове значення підіндексу ризику управління кібербезпекою становить 0,08. Це значення характеризує початкову відносну вагу підіндексу в структурі інтегрального індексу RA&CIMM, а не фактичний рівень ризику конкретного суб'єкта оцінювання.

Підіндекс ризику технічних вразливостей (Technical Vulnerability Risk) призначений для оцінювання характеристик технічних вразливостей, стану процесів управління оновленнями та рівня захищеності інформаційних і комп'ютерних систем суб'єкта оцінювання.

Під час формування підіндексу можуть враховуватися дані про наявність, критичність і можливість експлуатації виявлених вразливостей, своєчасність

встановлення оновлень, а також стан реалізації відповідних технічних заходів захисту. Оброблення цих даних забезпечує формування окремої складової профілю ризику, пов'язаної з можливістю реалізації кіберзагроз через технічні вразливості.

У початковому експертному профілі вагове значення підіндексу ризику технічних вразливостей становить 0,10. Це найбільша початкова вага серед додаткових підіндексів експертного домену RA&CIMM.

Підіндекс впливу кіберзагроз (Threat Exposure Risk) характеризує рівень зовнішньої експозиції інформаційних ресурсів, сервісів та інформаційної інфраструктури суб'єкта оцінювання, а також можливість їх використання потенційним атакувальником.

Під час формування підіндексу можуть враховуватися дані про доступні із зовнішніх мереж ресурси й сервіси, актуальні кіберзагрози, виявлені ознаки небезпечної активності та інші характеристики зовнішнього середовища. Їх структуризація й оброблення забезпечують подання впливу кіберзагроз як окремої складової профілю ризику.

У початковому експертному профілі вагове значення підіндексу впливу кіберзагроз становить 0,07.

Підіндекс ризику операційної стійкості (Operational Resilience Risk) характеризує здатність інформаційно-комунікаційної системи підтримувати критичні операційні процеси, протистояти наслідкам кіберінцидентів і відновлювати функціонування після їх виникнення.

Під час формування підіндексу можуть ураховуватися дані про організацію резервного копіювання, аварійного відновлення, забезпечення безперервності операційних процесів і готовність до відновлення після кіберінцидентів. Перебої в роботі інформаційних і комп'ютерних систем можуть спричиняти скорочення, погіршення або припинення надання послуг, що визначає зв'язок цього підіндексу з операційним ризиком.

У початковому експертному профілі вагове значення підіндексу ризику операційної стійкості становить 0,05.

Підіндекс ризику людського фактора (Human Factor Risk) характеризує ризики, пов’язані з недостатнім рівнем обізнаності персоналу, помилками користувачів, порушенням установлених правил, фішинговими атаками та діями внутрішніх порушників.

Під час формування підіндексу можуть враховуватися дані про навчання й обізнаність персоналу, результати перевірок його стійкості до фішингових атак, випадки порушення вимог інформаційної безпеки, компрометацію облікових записів та інциденти, пов’язані з внутрішніми загрозами. Структуризація цих даних забезпечує формування окремої кадрової складової профілю ризику.

У початковому експертному профілі вагове значення підіндексу ризику людського фактора становить 0,05.

Підіндекс ризику третіх сторін і ланцюгів постачання (Third-Party and Supply Chain Risk) характеризує ризики, пов’язані із залежністю суб’єкта оцінювання від постачальників програмного забезпечення, хмарних сервісів, телекомунікаційних послуг та інших зовнішніх учасників.

Під час формування підіндексу можуть враховуватися дані про критичних постачальників, умови доступу третіх сторін до інформаційних ресурсів і систем, залежність операційних процесів від зовнішніх сервісів, установлені вимоги до кібербезпеки постачальників, а також інциденти та загрози, пов’язані з ланцюгами постачання. Оброблення цих даних дає змогу оцінити вплив зовнішніх залежностей на профіль ризику суб’єкта оцінювання.

У початковому експертному профілі вагове значення підіндексу ризику третіх сторін і ланцюгів постачання становить 0,05.

Підіндекс ризику невідповідності нормативним вимогам (Compliance Risk) характеризує ризики, пов’язані з невиконанням установлених законодавчих, нормативних і договірних вимог у сфері інформаційної безпеки, кіберзахисту та кіберстрахування.

Під час формування підіндексу можуть враховуватися дані про виконання вимог ДСТУ IEC/ISO 31010:2013, ISO/IEC 27102:2019, Рамкової основи кібербезпеки NIST 2.0, Європейської рамки сертифікації кібербезпеки, визначеної Регламентом (ЄС) 2019/881, а також нормативно-правових актів Національного банку України. Для операторів критичної інфраструктури перелік нормативних орієнтирів доповнюється актами щодо визначення об'єктів критичної інфраструктури, загальними вимогами та методичними рекомендаціями щодо їх кіберзахисту, а також положеннями організаційно-технічної моделі кіберзахисту [45, 95, 158, 159]. Результати перевірки відповідності формують нормативну складову профілю ризику RA&CIMM [3, 12, 60, 123, 155].

У початковому експертному профілі вагове значення підіндексу ризику невідповідності нормативним вимогам становить 0,05.

Підіндекс фінансового та страхового ризику (Financial and Insurance Risk) характеризує можливі фінансові наслідки реалізації кіберризиків, наявне страхове покриття та можливість передавання частини відповідного ризику механізмами кіберстрахування.

Під час формування підіндексу можуть враховуватися дані про потенційні прямі й непрямі збитки, витрати на реагування та відновлення, наявність і обсяг страхового покриття, установлені виключення й обмеження, а також інші характеристики, необхідні для інформаційної підтримки страхового андеррайтингу. Одержана оцінка не є актуарним розрахунком страхової премії, франшизи або ліміту відповідальності.

У початковому експертному профілі вагове значення підіндексу фінансового та страхового ризику становить 0,05.

Сукупність восьми підіндексів експертного домену забезпечує структуроване подання організаційних, технічних, зовнішніх, операційних, кадрових, нормативних і фінансово-страхових характеристик ризику, які не можуть бути повністю визначені автоматизованими технічними засобами.

Результати їх оцінювання формують експертну складову профілю ризику RA&CIMM.

Другим доменом RA&CIMM є мережевий домен оцінювання ризиків інформаційної безпеки та кіберризиків. Він призначений для збирання, перевірки й оброблення технічних даних про стан інформаційно-комунікаційної системи, одержаних унаслідок її технічного дослідження.

У мережевому домені RA&CIMM передбачено використання результатів тестування на проникнення (Penetration Testing) як одного з джерел технічних даних про стан інформаційно-комунікаційної системи. У початковому експертному профілі вагове значення цієї складової становить 0,10.

Тестування на проникнення дає змогу перевірити можливість практичної експлуатації виявлених вразливостей шляхом контрольованого моделювання кібератак. Одержані результати можуть використовуватися для формування технічних показників рівня захищеності інформаційно-комунікаційної системи.

Результати тестування на проникнення доповнюють експертне оцінювання ризику технічних вразливостей. В експертному домені відповідний підіндекс характеризує вразливості та стан управління ними на основі структурованих даних оцінювання, тоді як у мережевому домені здійснюється технічна перевірка можливості їх практичної експлуатації.

Оцінювання вразливостей (Vulnerability Assessment) передбачає збирання та оброблення технічних даних про наявність, кількість, критичність і розташування вразливостей у програмному забезпеченні, мережах та інформаційній інфраструктурі. Відповідні результати використовуються для формування показників технічного стану об’єкта оцінювання. У початковому експертному профілі вагове значення цієї складової становить 0,10.

Додатковим джерелом технічних даних для мережевого домену можуть бути результати мережевого моніторингу, структуровані у вигляді відповідних показників та індексних оцінок [160]. Їх використання дає змогу доповнювати

результати технічного дослідження даними про зміну стану інформаційно-комунікаційної системи в часі.

Автоматизоване оцінювання за відкритими джерелами (Automated OSINT Assessment) призначене для виявлення й аналізу доступних у відкритому доступі відомостей про інформаційні ресурси, мережеві адреси, доменні імена, сервіси та інші цифрові об'єкти суб'єкта оцінювання. Одержані дані можуть використовуватися для визначення рівня зовнішньої інформаційної експозиції. Початкове вагове значення цієї складової становить 0,02.

Управління поверхнею атаки (Attack Surface Management) передбачає виявлення, інвентаризацію та оцінювання зовнішньо доступних цифрових активів, сервісів і точок потенційного доступу до інформаційно-комунікаційної системи. Результати такого оцінювання характеризують масштаб, видимість і рівень захищеності зовнішньої цифрової поверхні. У початковому експертному профілі вагове значення цієї складової становить 0,03.

Поєднання експертного та мережевого доменів є визначальною ознакою гібридної структури RA&CIMM. Експертний домен забезпечує оцінювання складних організаційних, процесних, нормативних, кадрових і фінансово-страхових характеристик ризику, тоді як мережевий домен забезпечує отримання та оброблення технічних даних про стан інформаційно-комунікаційної системи. Сума початкових вагових значень складових мережевого домену становить 0,25.

Третім доменом RA&CIMM є домен оцінювання зрілості процесів кіберстрахування. Його призначення полягає у визначенні рівня розроблення, формалізації, упровадження та технологічного забезпечення відповідних процесів.

Підіндекс зрілості процесів кіберстрахування формується на основі показників, що характеризують стан стандартизованих процесів кіберстрахування, організацію управління кіберризиками й ризиками інформаційної безпеки, а також рівень використання та інтеграції інформаційних технологій у відповідні процеси [19, 37].

Методологічна основа оцінювання зрілості процесів кіберстрахування формується з урахуванням положень ISO/IEC 27102:2019 та нормативних вимог щодо організації заходів із забезпечення інформаційної безпеки й кіберзахисту надавачами фінансових послуг. Оцінюванню підлягають розроблення, формалізація та впровадження процесів управління кіберризиками й ризиками інформаційної безпеки, а також заходів інформаційної безпеки та кіберзахисту з урахуванням особливостей функціонування інформаційно-комунікаційної системи [12, 37, 155].

Для суб'єктів, на яких поширюються вимоги законодавства про критичну інфраструктуру, під час організації зовнішньої перевірки можуть також враховуватися встановлені нормативні засади проведення незалежного аудиту інформаційної безпеки [161]. У RA&CIMM результати такого аудиту можуть використовуватися як одне із джерел підтвердження відомостей, отриманих у процесі самооцінювання.

Для збирання первинних даних використовуються структуровані опитувальники, адаптовані до нормативних вимог і доменної структури RA&CIMM. Питання та критерії опитувальників співвідносяться з відповідними індикаторами й підіндексами, а одержані відповіді проходять перевірку, формалізацію та чисельне подання для подальшого агрегування.

Домен зрілості забезпечує включення до RA&CIMM характеристик процесів кіберстрахування та рівня впровадження відповідних інформаційних технологій. Цим RA&CIMM відрізняється від моделей, орієнтованих виключно на технічне оцінювання стану інформаційної безпеки або кіберзахисту.

Для експертного домену вхідними є дані самооцінювання, зовнішньої перевірки та експертної перевірки організаційних, процесних, кадрових, нормативних, фінансових і страхових характеристик. Вони можуть надходити зі структурованих опитувальників, внутрішніх документів та інших доступних відомостей про суб'єкта оцінювання.

Для мережевого домену вхідними є технічні дані, одержані за результатами дослідження інформаційно-комунікаційної системи, зокрема оцінювання вразливостей, тестування на проникнення, аналізу відкритих джерел та управління поверхнею атаки. Склад доступних даних визначається обсягом фактично проведеного технічного дослідження.

Для домену зрілості процесів кіберстрахування вхідними є дані про стан, рівень формалізації та впровадження відповідних процесів, застосування заходів управління кіберризиками й ризиками інформаційної безпеки, а також використання інформаційних технологій у процесах кіберстрахування.

З позицій інформаційного оброблення така структура забезпечує формування трьох груп вхідних даних: експертних, технічних і процесних. Для кожної групи окремо виконуються перевірка, формалізоване представлення, нормування та оцінювання відповідних показників.

Формування підіндексів становить проміжний рівень агрегування даних. Значення окремих індикаторів групуються відповідно до доменної структури RA&CIMM та з урахуванням визначених вагових характеристик об’єднуються у відповідні підіндекси.

Початкові вагові значення визначають відносний внесок окремих підіндексів у формування інтегрального індексу RA&CIMM. В опублікованій моделі ці значення подано як складові початкового експертного профілю [37].

Початковий характер експертного профілю передбачає можливість подальшого уточнення складу індикаторів і підіндексів, а також їх вагових характеристик. Таке уточнення має здійснюватися з урахуванням предметної області, особливостей суб’єкта оцінювання та складу доступних даних. Зміна базової тридоменної структури RA&CIMM потребує окремого наукового обґрунтування та перевірки узгодженості моделі.

Необхідність уточнення початкового профілю може бути зумовлена накопиченням результатів оцінювання, розвитком процесів кіберстрахування,

зміною структури ризиків інформаційної безпеки й кіберризиків, а також появою нових джерел даних і засобів їх автоматизованого оброблення.

Для формалізованого визначення відносної пріоритетності критеріїв і подальшого уточнення вагових коефіцієнтів у RA&CIMM передбачено можливість застосування методу аналізу ієрархій [162]. Детальну процедуру його можливого застосування для уточнення ваг наведено в підрозділі 4.3. Його застосування потребує формування ієрархії критеріїв, проведення їх попарних порівнянь, обчислення ваг і перевірки узгодженості експертних суджень.

Верхній рівень ієрархії RA&CIMM утворює цільовий результат комплексного оцінювання. Наступний рівень становлять три домени моделі, у межах яких визначаються відповідні підіндекси, індикатори та вагові характеристики їх внеску.

Така ієрархія відповідає багаторівневому поданню результатів, сформованому в попередніх розділах дисертації:

значення окремого індикатора → група логічно пов'язаних індикаторів → підіндекс → доменний результат → інтегральний індекс RA&CIMM.

Доменна структура та початковий експертний профіль RA&CIMM забезпечують формалізоване представлення різнорідних характеристик суб'єкта оцінювання. Організаційні, процесні, технічні, кадрові, нормативні, фінансові та страхові характеристики включаються до єдиної структури даних із визначеними взаємозв'язками та рівнями агрегування.

У результаті визначення доменів, індикаторів і підіндексів сформовано структуру вхідних даних RA&CIMM, правила їх логічного групування та склад проміжних результатів оцінювання. Це створює основу для алгоритмізації процедур перевірки, нормування, зважування й агрегування даних та їх подальшої програмної реалізації.

Отже, початковий експертний профіль RA&CIMM визначає склад основних і додаткових підіндексів та їх початкові вагові характеристики. Експертний домен забезпечує оцінювання багатофакторних характеристик ризику, мережевий

домен — оброблення технічних даних про стан інформаційно-комунікаційної системи, а домен зрілості — оцінювання стану й рівня впровадження процесів кіберстрахування.

Перехід від визначеної структури моделі до формування інтегрального індексу потребує встановлення способів чисельного подання окремих показників, правил їх включення до підіндексів і порядку врахування вагових коефіцієнтів. Метод формування підіндексів та інтегрального індексу RA&CIMM розглянуто в підрозділі 4.3.

4.3. Метод формування підіндексів та інтегрального індексу RA&CIMM

Метою методу є формування підіндексів та інтегрального індексу RA&CIMM на основі сукупності часткових показників, структурованих відповідно до визначених доменів моделі. Одержані результати характеризують профіль ризиків і зрілості процесів кіберстрахування суб'єкта оцінювання та можуть використовуватися для інформаційної підтримки прийняття рішень у процесах кіберстрахування.

Формування інтегрального індексу ґрунтується на доменній структурі RA&CIMM. Результати експертного оцінювання ризиків, мережевого оцінювання та оцінювання зрілості процесів кіберстрахування спочатку формуються окремо у вигляді відповідних доменних підіндексів, після чого агрегуються в інтегральний індекс RA&CIMM.

Метод передбачає послідовний перехід від значень окремих показників до їх агрегованого подання. Окремий показник характеризує визначену властивість суб'єкта оцінювання або його інформаційно-комунікаційної системи. Логічно пов'язані показники об'єднуються у групи та формують відповідні підіндекси. На наступному рівні підіндекси агрегуються в доменний підіндекс I_l, що

характеризує результат оцінювання в межах відповідного домену. Сукупність доменних підіндексів використовується для формування інтегрального індексу I.

Отже, ієрархія формування результату RA&CIMM має такий вигляд: **значення окремого показника → група логічно пов'язаних показників → підіндекс → доменний підіндекс I_l → інтегральний індекс I.**

Інтегральний індекс RA&CIMM подано у вигляді [37]:

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

де:

I — інтегральний індекс RA&CIMM;

I_l — підіндекс l-го домену моделі;

p_j — нормоване значення j-го показника;

d_l — ваговий коефіцієнт l-го домену моделі;

α_{jl} — ваговий коефіцієнт внеску j-го у формування підіндексу l-го домену.

Для забезпечення нормованого агрегування сума вагових коефіцієнтів доменів дорівнює одиниці, а сума вагових коефіцієнтів показників у межах кожного домену також дорівнює одиниці:

$$\sum_{l=1}^{L} d_l = 1, \qquad \sum_{j=1}^{n_l} \alpha_{jl} = 1.$$

У такому поданні добуток $\alpha_{jl} d_l$ визначає сукупний внесок j-го показника у формування інтегрального індексу RA&CIMM з урахуванням ваги відповідного домену.

Вагові коефіцієнти α_{jl} забезпечують урахування різного внеску окремих показників у результат оцінювання відповідного домену. Базова структура RA&CIMM охоплює три визначені домени, тоді як склад показників і підіндексів у їх межах може уточнюватися залежно від мети оцінювання, особливостей суб'єкта оцінювання та складу доступних даних.

Наведене математичне представлення визначає багаторівневу структуру формування результату. На першому рівні здійснюються збирання, перевірка та чисельне подання значень окремих показників. На другому рівні логічно пов'язані показники групуються відповідно до структури доменів RA&CIMM. На третьому рівні формуються відповідні підіндекси. Далі підіндекси агрегуються в доменні підіндекси I_l, сукупність яких використовується для формування інтегрального індексу I.

Початкові вагові значення складових оцінювання визначаються відповідно до початкового експертного профілю RA&CIMM, наведеного в таблиці 4.1. Сумарне вагове значення складових експертного домену становить 0,50, мережевого домену — 0,25, домену оцінювання зрілості процесів кіберстрахування — 0,25. Загальна сума початкових вагових значень дорівнює 1,00.

Для кожного домену оброблення даних здійснюється окремо з урахуванням їх джерел і способів отримання. В експертному домені обробляються формалізовані дані самооцінювання, зовнішньої перевірки та експертної перевірки; у мережевому домені — технічні дані про стан інформаційно-комунікаційної системи; у домені зрілості — дані про стан, формалізацію та рівень упровадження процесів кіберстрахування. Одержані доменні підіндекси надалі агрегуються в інтегральний індекс RA&CIMM.

Початкові вагові характеристики RA&CIMM мають експертний характер і визначають вихідну структуру агрегування показників у межах моделі. Вони можуть уточнюватися за результатами накопичення даних, повторного оцінювання та подальшого експертного аналізу [37].

Для формалізованого уточнення відносної пріоритетності критеріїв і вагових коефіцієнтів у RA&CIMM передбачено можливість застосування методу аналізу ієрархій (Analytic Hierarchy Process, AHP), розробленого Т. Сааті на основі ієрархічного структурування задачі, попарного порівняння критеріїв і визначення їх відносних пріоритетів [162, 163].

Застосування методу аналізу ієрархій для уточнення вагових коефіцієнтів RA&CIMM передбачає формування матриці попарних порівнянь

$$A = (\alpha_{ij})_{n \times n}$$

де α_{ij} характеризує відносну перевагу i-го критерію над j-м критерієм; $\alpha_{ii}, = 1$, $\alpha_{ji} = 1/\alpha_{ij}$. Попарні порівняння можуть виконуватися окремо для доменів, складових у межах доменів та відповідних показників за дев'ятибальною шкалою Сааті [162].

Відносну вагу i-го критерію визначають шляхом нормування середнього геометричного елементів відповідного рядка:

$$g_i = \left(\prod_{j=1}^{n} a_{ij} \right)^{1/n}, \qquad w_i = \frac{g_i}{\sum_{k=1}^{n} g_k}.$$

Узгодженість експертних суджень перевіряють за індексом узгодженості

$$CI = \frac{\lambda_{\max} - n}{n - 1}$$

та відношенням узгодженості

$$CR = \frac{CI}{RI},$$

де $\lambda_{\max}$— найбільше власне значення матриці; RI — випадковий індекс узгодженості. Прийнятним вважається $CR \leq 0{,}10$ [162].

Одержані за методом аналізу ієрархій вагові коефіцієнти можуть використовуватися для подальшого уточнення початкових ваг доменів і складових RA&CIMM. У межах цієї дисертації наведена процедура визначає спосіб подальшого уточнення ваг; початкові значення таблиці 4.1 сформовано без застосування методу аналізу ієрархій.

Його застосування передбачає побудову ієрархії критеріїв, проведення їх попарних порівнянь, обчислення відносних вагових коефіцієнтів і перевірку узгодженості експертних суджень. У межах дисертаційної роботи AHP

розглянуто як засіб подальшого формалізованого уточнення початкових вагових характеристик; наведені в таблиці 4.1 вагові значення сформовано в межах початкового експертного профілю RA&CIMM, а не за результатами застосування AHP.

Ієрархія застосування AHP у RA&CIMM охоплює мету комплексного оцінювання, три домени моделі, відповідні складові та показники. Вагові коефіцієнти, визначені на кожному рівні ієрархії, мають відображати відносний внесок її складових у формування доменних підіндексів та інтегрального індексу RA&CIMM.

Поряд із методом аналізу ієрархій для подальшого уточнення вагових характеристик та оцінювання складних багатофакторних характеристик можуть застосовуватися метод Дельфі (Delphi) [164], експертне ранжування і сценарний аналіз. Вибір конкретного методу залежить від мети оцінювання, складу критеріїв, кількості залучених експертів та доступності даних. Зазначені методи визначають напрями подальшого розвитку RA&CIMM і не розглядаються як фактично реалізовані складові проведеної апробації.

Формування доменних підіндексів забезпечує окреме подання результатів за кожним доменом RA&CIMM. Це дає змогу аналізувати не лише значення інтегрального індексу, а й структуру ризиків і зрілості процесів кіберстрахування за відповідними доменами, підіндексами та окремими показниками. Такий спосіб подання результатів забезпечує виявлення складових із відносно вищими значеннями ризику або недостатнім рівнем зрілості.

Для інтерпретації результатів оцінювання використовується стобальна шкала [37]. Для показників ризику збільшення чисельного значення відповідає зростанню рівня ризику: 0–20 — дуже низький ризик; 21–40 — низький; 41–60 — середній; 61–80 — високий; 81–100 — критичний. Для показників зрілості процесів кіберстрахування збільшення чисельного значення відповідає підвищенню рівня зрілості: 0–20 — початковий, або хаотичний, рівень; 21–40 —

повторюваний; 41–60 — встановлений; 61–80 — керований; 81–100 — оптимізований рівень.

Інтерпретація дробових оцінок здійснюється за неперервними інтервалами, визначеними в підрозділі 4.1.

Показники ризику та зрілості мають протилежну змістову спрямованість.

Для приведення показників до єдиної спрямованості нормовані значення показників ризику перетворюються за правилом

$$p_j^* = 100 - p_j ,$$

тоді як значення показників зрілості зберігаються без зміни:

$$p_j^* = p_j .$$

Після такого перетворення більше значення p_j^* відповідає кращому стану суб'єкта оцінювання: нижчому рівню ризику або вищому рівню зрілості. У формулі інтегрального індексу використовується узгоджене значення p_j^*.

Інтегральний індекс RA&CIMM забезпечує узагальнене подання результатів оцінювання, а доменні підіндекси та профіль окремих показників — їх деталізацію. Тому значення інтегрального індексу необхідно аналізувати разом із доменними підіндексами та відповідними показниками. Спільне використання цих результатів дає змогу визначати складові, що найбільше впливають на профіль ризиків і зрілості процесів кіберстрахування, та формувати інформацію для підтримки прийняття рішень.

Багаторівневе агрегування забезпечує формалізований перехід від різнорідних вхідних даних до структурованих чисельних результатів. Послідовність операцій охоплює збирання і перевірку даних, їх формалізоване представлення, чисельне кодування, нормування, групування за доменами, зважування, формування підіндексів та обчислення інтегрального індексу. Така послідовність створює основу для алгоритмізації методу та його подальшої реалізації в інформаційних і комп'ютерних системах кіберстрахування.

Отже, запропонований метод забезпечує послідовне формування підіндексів і доменних підіндексів RA&CIMM та їх подальше агрегування в

інтегральний індекс. Доменна структура, початковий експертний профіль і вагові коефіцієнти визначають порядок оброблення й агрегування окремих показників, а одержані доменні та інтегральні результати формують структуроване подання профілю ризиків і зрілості процесів кіберстрахування.

Практичне застосування запропонованого методу потребує визначення послідовності операцій збирання вхідних даних, їх перевірки, формалізованого представлення, нормування, зважування, агрегування та повторного оцінювання. Багаторівневий алгоритм виконання зазначених операцій розглянуто в наступному підрозділі.

4.4. Алгоритм багаторівневого оцінювання ризиків та зрілості процесів кіберстрахування

Алгоритм багаторівневого оцінювання ґрунтується на доменній структурі RA&CIMM та передбачає послідовне збирання, перевірку, уточнення й оброблення даних. У межах алгоритму визначено чотири процедурні рівні: самооцінювання, зовнішнє оцінювання, експертна перевірка та повторне оцінювання. Результати попереднього рівня використовуються як вхідні дані для перевірки або уточнення результатів на наступному рівні [37].

Основу алгоритму становить оцінювання стану розроблення, формалізації та впровадження процесів управління кіберризиками й ризиками інформаційної безпеки, а також реалізації заходів інформаційної безпеки та кіберзахисту. Оцінювання здійснюється з урахуванням особливостей функціонування інформаційно-комунікаційної системи суб’єкта оцінювання та визначених критеріїв прийнятності ризику.

Початковим етапом алгоритму є визначення суб’єкта й об’єкта оцінювання. Суб’єктом оцінювання може бути учасник страхового ринку, надавач фінансових

послуг, оператор критичної інфраструктури або інша організація, для якої здійснюється оцінювання ризиків і зрілості процесів кіберстрахування. Об'єктом оцінювання може бути організація загалом, її окремий структурний підрозділ, визначений бізнес-процес або інформаційно-комунікаційна система.

Вибір об'єкта оцінювання визначає склад вхідних даних, перелік показників, джерела їх отримання та особливості застосування показників у межах визначених доменів RA&CIMM. На цьому етапі також установлюються межі оцінювання, відповідальні особи, доступні інформаційні ресурси та вимоги до перевірки одержаних даних.

Після визначення суб'єкта й об'єкта оцінювання формується набір показників відповідно до доменної структури RA&CIMM. Показники розподіляються між експертним доменом оцінювання ризиків, мережевим доменом та доменом оцінювання зрілості процесів кіберстрахування. Для кожного показника визначаються джерело даних, спосіб їх отримання, форма представлення та правило подальшого чисельного оброблення.

Для експертного домену формуються показники, що характеризують управління кібербезпекою, технічні вразливості, вплив кіберзагроз, операційну стійкість, людський фактор, ризики третіх сторін і ланцюгів постачання, відповідність нормативним вимогам, а також фінансові та страхові характеристики. Вхідними даними є результати структурованого опитування, документи суб'єкта оцінювання, відомості зовнішньої перевірки та формалізовані експертні судження.

Для мережевого домену формуються показники технічного стану інформаційно-комунікаційної системи. Вхідними є дані, одержані за результатами тестування на проникнення, оцінювання вразливостей, автоматизованого аналізу відкритих джерел та управління поверхнею атаки. Одержані дані перевіряються, кодуються та перетворюються на чисельні значення відповідних показників мережевого домену.

Для домену зрілості процесів кіберстрахування формуються показники, що характеризують стан розроблення, формалізації та впровадження стандартизованих процесів кіберстрахування, організацію управління кіберризиками й ризиками інформаційної безпеки, а також рівень застосування інформаційних технологій у відповідних процесах. Вхідні дані одержуються зі структурованих опитувальників, внутрішніх документів, відомостей про реалізовані процеси та доступних результатів їх перевірки.

Після формування структури показників здійснюється перший процедурний рівень — самооцінювання (self-assessment). Суб'єкт оцінювання надає первинні дані шляхом заповнення структурованих опитувальників і подання відповідних документів. Одержані відповіді перевіряються на повноту, логічну узгодженість і відповідність установленому формату, після чого кодуються та співвідносяться з відповідними показниками й підіндексами RA&CIMM.

Другим процедурним рівнем є зовнішнє оцінювання (external assessment). Його необхідність зумовлена тим, що результати самооцінювання формуються переважно на основі відомостей, наданих самим суб'єктом оцінювання. У межах зовнішнього оцінювання перевіряються повнота, достовірність і логічна узгодженість одержаних відповідей, а також їх відповідність визначеним критеріям RA&CIMM.

За наявності відповідних даних результати самооцінювання зіставляються з внутрішніми документами, відомостями про стан процесів, результатами зовнішніх перевірок та іншою доступною інформацією про об'єкт оцінювання. Виявлені розбіжності фіксуються, а значення відповідних показників підтверджуються або уточнюються. Результатом зовнішнього оцінювання є перевірений набір значень показників, який передається на наступний процедурний рівень.

Третім процедурним рівнем є експертна перевірка (expert review). Вона застосовується для оцінювання складних багатофакторних характеристик ризику,

які не можуть бути повністю визначені автоматизованими технічними засобами або безпосередньо встановлені за результатами самооцінювання та зовнішньої перевірки. Експертна перевірка передбачає аналіз наявних даних, з'ясування причин виявлених розбіжностей, уточнення значень окремих показників і формування відповідного експертного висновку.

Мережеве оцінювання не утворює окремого процедурного рівня алгоритму, а здійснюється в межах мережевого домену RA&CIMM. Воно забезпечує збирання технічних даних про стан інформаційно-комунікаційної системи за результатами тестування на проникнення, оцінювання вразливостей, автоматизованого аналізу відкритих джерел та управління поверхнею атаки. Результати технічного дослідження формалізуються та використовуються для визначення значень показників і підіндексів мережевого домену.

Отже, під час формування часткових результатів використовуються дані різного походження: результати самооцінювання, зовнішньої перевірки, експертної перевірки та технічного дослідження інформаційно-комунікаційної системи. Незалежно від джерела одержані дані перевіряються, приводяться до визначеного формату, кодуються та співвідносяться з відповідними показниками, підіндексами й доменами RA&CIMM.

Після збирання і перевірки вхідних даних формуються чисельні значення окремих показників. Кожний показник пов'язується з відповідним доменом і підіндексом RA&CIMM, а його значення визначається згідно з установленим правилом чисельного подання. Сукупність значень логічно пов'язаних показників утворює основу для подальшого формування відповідних підіндексів.

Наступним етапом алгоритму є формування підіндексів. У межах кожного домену значення логічно пов'язаних показників групуються відповідно до структури RA&CIMM, нормуються та агрегуються з урахуванням визначених вагових характеристик. У такий спосіб окремо формуються підіндекси експертного домену, мережевого домену та домену оцінювання зрілості процесів кіберстрахування.

Сукупність сформованих підіндексів утворює профіль ризиків і зрілості процесів кіберстрахування. Профіль відображає значення окремих складових оцінювання та дає змогу виявити показники й підіндекси з відносно вищими значеннями ризику або недостатнім рівнем зрілості. Таке подання зберігає інформацію про внутрішню структуру результату, яка може бути втрачена під час використання лише одного узагальненого значення.

Після формування підіндексів здійснюється їх агрегування відповідно до методу, розглянутого в підрозділі 4.3. Результатом агрегування є інтегральний індекс I, який використовується разом із доменними підіндексами та профілем окремих показників. Показники ризику й зрілості інтерпретуються за відповідними стобальними шкалами з урахуванням їх протилежної змістової спрямованості.

Після інтерпретації результатів визначаються складові профілю ризиків і зрілості, що потребують першочергової уваги. На цій основі може формуватися інформація щодо пріоритетності заходів реагування, необхідності вдосконалення процесів кіберстрахування та доцільності страхового покриття. Одержані результати не є безпосереднім розрахунком страхової премії, франшизи або ліміту страхового покриття та потребують окремого актуарного обґрунтування.

Четвертим процедурним рівнем є повторне оцінювання (re-assessment). Воно здійснюється після завершення попереднього циклу оцінювання, реалізації рекомендованих заходів або закінчення визначеного періоду спостереження. Під час повторного оцінювання застосовуються та сама доменна структура, система показників і правила їх оброблення, що забезпечує порівнянність одержаних результатів.

Результати повторного оцінювання порівнюються з результатами попереднього циклу за окремими показниками, підіндексами, доменними підіндексами та загальним профілем. Таке порівняння дає змогу визначити напрями й величину змін, оцінити результативність упроваджених заходів та

уточнити поточний стан ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування.

На основі визначеної багаторівневої процедури алгоритм оцінювання ризиків і зрілості процесів кіберстрахування формалізовано у вигляді такої послідовності операцій:

1) визначення суб'єкта, об'єкта та меж оцінювання;

2) визначення доменів, підіндексів і показників оцінювання;

3) визначення джерел даних і правил їх чисельного подання;

4) збирання вхідних даних із використанням структурованих опитувальників, документів та доступних технічних відомостей;

5) проведення самооцінювання та формування первинних значень показників;

6) перевірка повноти й логічної узгодженості одержаних даних;

7) проведення зовнішнього оцінювання та уточнення результатів самооцінювання;

8) проведення експертної перевірки складних багатофакторних характеристик ризику;

9) одержання та оброблення результатів технічного дослідження інформаційно-комунікаційної системи;

10) кодування і нормування значень показників та приведення їх до узгодженої спрямованості за правилами, визначеними в підрозділі 4.3;

11) застосування початкових або окремо обґрунтованих уточнених вагових коефіцієнтів;

12) формування підіндексів і доменних підіндексів RA&CIMM;

13) формування профілю ризиків і зрілості процесів кіберстрахування;

14) агрегування доменних підіндексів і визначення інтегрального індексу RA&CIMM;

15) інтерпретація результатів за відповідними шкалами ризику та зрілості;

16) формування інформації та рекомендацій для підтримки прийняття рішень;

17) проведення повторного оцінювання;

18) порівняння результатів послідовних циклів оцінювання та визначення змін показників, підіндексів і загального профілю.

Наведена послідовність операцій визначає інформаційний процес перетворення первинних різнорідних даних про суб'єкта й об'єкт оцінювання на структурований результат у вигляді показників, підіндексів, доменних підіндексів, профілю ризиків і зрілості процесів кіберстрахування та інтегрального індексу RA&CIMM.

Вхідними даними алгоритму є відповіді на структуровані опитувальники, внутрішні й зовнішні документи, відомості про процеси управління кіберризиками та ризиками інформаційної безпеки, дані про реалізовані заходи інформаційної безпеки й кіберзахисту, характеристики процесів кіберстрахування, а також результати технічного дослідження інформаційно-комунікаційної системи.

Проміжними результатами алгоритму є перевірені й нормовані значення окремих показників, сформовані підіндекси та доменні підіндекси. Вихідними результатами є профіль ризиків і зрілості процесів кіберстрахування, інтегральний індекс RA&CIMM, інтерпретація одержаних значень та інформація, підготовлена для підтримки прийняття рішень у процесах кіберстрахування.

Запропонований алгоритм визначає послідовність операцій збирання, перевірки, структуризації, формалізованого представлення, кодування, нормування, зважування, агрегування та інтерпретації різнорідних даних оцінювання. Алгоритм забезпечує перехід від первинних даних до структурованих чисельних результатів, придатних для подальшого автоматизованого оброблення й використання під час підтримки прийняття рішень.

Розроблений алгоритм є складовою методологічних основ оцінювання ризиків і зрілості процесів кіберстрахування. Його застосування забезпечує формалізоване подання процесів оброблення даних про кіберризики, стан інформаційної безпеки, реалізацію заходів кіберзахисту та рівень упровадження процесів кіберстрахування з урахуванням особливостей функціонування інформаційно-комунікаційної системи суб'єкта оцінювання.

Формалізація послідовності одержання та оброблення даних створює методологічну й алгоритмічну основу для подальшої автоматизації відповідних операцій і формування інформації, необхідної для підтримки прийняття рішень у процесах кіберстрахування. Порядок формування та використання такої інформації розглянуто в наступному підрозділі.

4.5. Формування інформації для підтримки прийняття рішень у процесах кіберстрахування

Результати досліджень, наведені в попередніх розділах, визначають послідовність переходу від формування системи показників операційних ризиків у кіберпросторі до їх структуризації, формалізованого представлення, оброблення, індексації та використання одержаних результатів у процесах кіберстрахування. Поєднання індексного підходу, доменної структуризації показників, моделі RA&CIMM, методу формування підіндексів та інтегрального індексу і багаторівневого алгоритму оцінювання створює методологічну й алгоритмічну основу для підготовки інформації, необхідної для підтримки прийняття рішень у процесах кіберстрахування [37].

Необхідність формування відповідної інформації зумовлена різнорідністю даних, що використовуються під час оцінювання ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування. Такі дані характеризують

управління кібербезпекою, технічні вразливості, вплив кіберзагроз, операційну стійкість, людський фактор, ризики третіх сторін і ланцюгів постачання, відповідність нормативним вимогам, фінансові та страхові характеристики ризику, технічний стан інформаційно-комунікаційної системи та стан упровадження процесів кіберстрахування.

Збирання, представлення, оброблення й аналіз зазначених даних можуть здійснюватися з використанням технологій електронного бізнесу, мобільних інформаційних систем, інтеграції інформаційних ресурсів, аналітики великих даних, штучного інтелекту, машинного навчання, оброблення природної мови, блокчейн-технологій, а також методів математичного, імітаційного і статистичного моделювання [13, 19, 68, 69]. Застосування відповідних технологій створює передумови для автоматизації окремих операцій оцінювання та формування структурованої інформації для підтримки прийняття рішень у процесах кіберстрахування.

У розділі 3 основні напрями застосування інформаційних технологій у процесах кіберстрахування структуровано за відповідними предметними областями, які можуть бути використані як домени індексу зрілості кіберстрахування. Склад таких доменів може уточнюватися залежно від мети оцінювання, особливостей суб'єкта оцінювання та доступних джерел даних, оскільки межі між окремими технологіями й методами є умовними [19].

Подальший розвиток зазначеного підходу в RA&CIMM забезпечив перехід від оцінювання рівня застосування інформаційних технологій до комплексного оцінювання ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування. RA&CIMM поєднує відповідні показники в межах трьох доменів і забезпечує формування доменних підіндексів, профілю ризиків і зрілості та інтегрального індексу [37].

Формування інформації для підтримки прийняття рішень ґрунтується на послідовному використанні результатів проведених досліджень. Індексний підхід і система базисних параметрів забезпечують структуризацію та чисельне подання

різнорідних показників; формалізація процесів кіберстрахування визначає склад інформаційних входів, операцій оброблення та результатів; модель RA&CIMM, метод формування підіндексів та інтегрального індексу і багаторівневий алгоритм оцінювання визначають порядок перетворення вхідних даних на структуровану інформацію для підтримки прийняття рішень.

Отже, одержані результати утворюють взаємопов'язану систему інформаційних процесів, що забезпечує перетворення первинних різнорідних даних про суб'єкта й об'єкт оцінювання на структуровані результати, придатні для використання під час підтримки прийняття рішень у процесах кіберстрахування.

Узагальнена послідовність інформаційного оброблення даних відповідно до моделі, методу й алгоритму RA&CIMM охоплює такі операції:

1) збирання вхідних даних;
2) структуризацію даних;
3) перевірку й уточнення даних;
4) чисельне подання та нормування значень показників;
5) визначення вагових характеристик;
6) формування підіндексів;
7) формування доменних підіндексів;
8) формування профілю ризиків і зрілості процесів кіберстрахування;
9) формування інтегрального індексу;
10) інтерпретацію одержаних результатів;
11) формування інформації для підтримки прийняття рішень;
12) накопичення результатів і проведення повторного оцінювання.

Вхідними даними є відомості, що характеризують суб'єкта й об'єкт оцінювання: результати самооцінювання; внутрішні та зовнішні документи; дані про процеси управління кіберризиками й ризиками інформаційної безпеки; відомості про впроваджені заходи інформаційної безпеки та кіберзахисту; характеристики процесів кіберстрахування; результати зовнішньої й експертної

перевірки; технічні дані про стан інформаційно-комунікаційної системи. Склад вхідних даних визначається межами оцінювання, структурою застосованих доменів і доступністю відповідних джерел інформації.

Основним засобом збирання даних самооцінювання є структуровані опитувальники, адаптовані до нормативних вимог, доменної структури та критеріїв RA&CIMM. Кожне питання або критерій опитувальника співвідноситься з відповідним показником і підіндексом моделі. Одержані відповіді перевіряються, кодуються та перетворюються на чисельні значення, придатні для подальшого оброблення.

Першим інформаційним процесом є збирання вхідних даних. Воно здійснюється відповідно до визначених меж оцінювання, доменної структури RA&CIMM, складу показників і встановлених вимог до джерел інформації. На цьому етапі забезпечуються ідентифікація джерел, одержання необхідних відомостей, їх реєстрація та встановлення зв'язків із відповідними показниками й підіндексами моделі.

Дані самооцінювання формують початковий набір значень показників. Результати зовнішнього оцінювання й експертної перевірки використовуються для перевірки, підтвердження або уточнення цих значень, а результати технічного дослідження інформаційно-комунікаційної системи — для формування показників мережевого домену. Результатом збирання є початковий набір даних, структурно пов'язаний із відповідними доменами, підіндексами та показниками RA&CIMM.

Другим інформаційним процесом є структуризація даних. Одержані відомості розподіляються відповідно до доменної структури RA&CIMM, а кожний елемент даних співвідноситься з визначеним показником, підіндексом і доменом моделі.

Організаційні, управлінські, кадрові, нормативні, фінансові та страхові характеристики ризику належать до експертного домену. Технічні дані про стан інформаційно-комунікаційної системи, одержані за результатами оцінювання

вразливостей, тестування на проникнення, автоматизованого аналізу відкритих джерел та управління поверхнею атаки, належать до мережевого домену. Дані про стан розроблення, формалізації, упровадження та технологічного забезпечення процесів кіберстрахування належать до домену оцінювання зрілості процесів кіберстрахування.

Доменна структуризація забезпечує однозначне віднесення кожного показника до відповідної області оцінювання, визначає логічні зв'язки між вхідними даними та результатами їх оброблення і створює основу для подальшого формування підіндексів, доменних підіндексів та інтегрального індексу RA&CIMM.

Третім інформаційним процесом є перевірка й уточнення даних. Його реалізація ґрунтується на багаторівневій процедурі RA&CIMM, відповідно до якої результати самооцінювання послідовно перевіряються та уточнюються на рівнях зовнішнього оцінювання й експертної перевірки.

Під час зовнішнього оцінювання перевіряються повнота, достовірність, логічна узгодженість і відповідність установленому формату даних, одержаних у процесі самооцінювання. За наявності необхідних відомостей результати самооцінювання зіставляються з внутрішніми документами, даними про стан відповідних процесів та іншими доступними джерелами. Виявлені розбіжності фіксуються, а значення показників підтверджуються або уточнюються.

Експертна перевірка застосовується до складних багатофакторних характеристик ризику, які не можуть бути повністю визначені за результатами самооцінювання, документальної перевірки або автоматизованого технічного контролю. Технічні характеристики інформаційно-комунікаційної системи доповнюються даними мережевого домену, одержаними за результатами її технічного дослідження. Результатом цього інформаційного процесу є перевірений і уточнений набір значень показників, придатний для подальшого чисельного оброблення.

Четвертим інформаційним процесом є чисельне подання та нормування значень показників. Для кожного показника визначаються критерії оцінювання, шкала, допустимі значення та правило перетворення одержаних даних у чисельну форму, придатну для подальшого порівняння й агрегування.

Значення показників ризику характеризують рівень відповідної складової ризику, тоді як значення показників зрілості характеризують стан розроблення, формалізації та впровадження процесів кіберстрахування. Ураховуючи протилежну змістову спрямованість цих показників, перед їх спільним агрегуванням здійснюються нормування та приведення значень до узгодженої спрямованості.

Результатом зазначеного інформаційного процесу є сукупність перевірених і нормованих чисельних значень показників, структурованих за відповідними підіндексами й доменами RA&CIMM. Таке подання забезпечує зіставність різнорідних даних і створює основу для застосування вагових коефіцієнтів та подальшого формування підіндексів.

П’ятим інформаційним процесом є визначення вагових характеристик. Початкові вагові значення складових оцінювання встановлюються відповідно до початкового експертного профілю RA&CIMM, наведеного в таблиці 4.1, і відображають відносний внесок окремих складових у формування доменних підіндексів та інтегрального індексу.

Початкові вагові характеристики мають експертний характер і можуть уточнюватися за результатами накопичення даних, повторного оцінювання та подальшого експертного аналізу. Для їх формалізованого уточнення можуть застосовуватися метод аналізу ієрархій, метод Delphi, експертне ранжування та сценарний аналіз. У межах дисертаційної роботи зазначені методи розглядаються як напрями подальшого розвитку RA&CIMM і не є джерелом початкових вагових значень, наведених у таблиці 4.1.

Результатом цього інформаційного процесу є набір вагових коефіцієнтів, пов’язаних із відповідними показниками, підіндексами й доменами RA&CIMM.

Застосування вагових коефіцієнтів забезпечує врахування різного внеску окремих складових під час формування доменних та інтегральної оцінок.

Шостим інформаційним процесом є формування підіндексів. Нормовані значення логічно пов'язаних показників групуються відповідно до структури RA&CIMM та агрегуються з урахуванням визначених вагових коефіцієнтів. Результатом цього процесу є значення підіндексів, що характеризують окремі складові ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування.

У межах експертного домену формуються підіндекси ризику управління кібербезпекою, технічних вразливостей, впливу кіберзагроз, операційної стійкості, людського фактора, третіх сторін і ланцюгів постачання, невідповідності нормативним вимогам, а також фінансового та страхового ризику. У межах мережевого домену формуються підіндекси на основі результатів тестування на проникнення, оцінювання вразливостей, автоматизованого аналізу відкритих джерел та управління поверхнею атаки. У домені зрілості формуються підіндекси, що характеризують стан розроблення, формалізації, упровадження та технологічного забезпечення процесів кіберстрахування.

Сьомим інформаційним процесом є формування доменних підіндексів. Значення підіндексів кожного домену агрегуються з урахуванням установлених вагових характеристик. Результатом є три доменні підіндекси, які окремо характеризують експертну складову ризику, технічну складову ризику та зрілість процесів кіберстрахування.

Восьмим інформаційним процесом є формування профілю ризиків і зрілості процесів кіберстрахування. Профіль утворюється як структурована сукупність значень окремих показників, підіндексів і доменних підіндексів RA&CIMM. Його використання забезпечує збереження внутрішньої структури результатів і дає змогу визначати складові з відносно вищими значеннями ризику або недостатнім рівнем зрілості.

Дев’ятим інформаційним процесом є формування інтегрального індексу RA&CIMM. Доменні підіндекси після приведення їх значень до узгодженої спрямованості агрегуються відповідно до методу, розглянутого в підрозділі 4.3. Результатом є узагальнене чисельне значення, що характеризує сукупний результат оцінювання ризиків і зрілості процесів кіберстрахування.

Інтегральний індекс використовується разом із доменними підіндексами, підіндексами та профілем окремих показників. Таке спільне подання забезпечує одержання узагальненого результату без втрати інформації про його внутрішню структуру та складові, які найбільше вплинули на сформовану оцінку.

Десятим інформаційним процесом є інтерпретація одержаних результатів. Значення показників ризику інтерпретуються за стобальною шкалою від дуже низького до критичного рівня ризику, а значення показників зрілості процесів кіберстрахування — за стобальною шкалою від початкового, або хаотичного, до оптимізованого рівня зрілості.

Під час інтерпретації враховується протилежна змістова спрямованість відповідних шкал: збільшення значення показника ризику свідчить про підвищення рівня ризику, тоді як збільшення значення показника зрілості відповідає підвищенню рівня зрілості процесів кіберстрахування. Тому результати аналізуються не лише за інтегральним індексом, а й за доменними підіндексами, підіндексами та профілем окремих показників.

Інтерпретація забезпечує перехід від чисельних результатів до змістових категорій, придатних для подальшого аналізу. Її результатом є визначення рівнів ризику і зрілості, виявлення складових, що потребують першочергової уваги, та підготовка структурованої інформації для підтримки прийняття рішень у процесах кіберстрахування.

Одинадцятим інформаційним процесом є формування інформації для підтримки прийняття рішень. Вихідні результати цього процесу охоплюють інтегральний індекс RA&CIMM, доменні підіндекси, підіндекси, профіль

окремих показників, визначені рівні ризику і зрілості, а також відомості про складові, що потребують першочергового аналізу або вдосконалення.

Підтримка прийняття рішень полягає у використанні результатів RA&CIMM для аналізу стану суб'єкта й об'єкта оцінювання, визначення пріоритетності заходів зниження ризику, формування вимог до стану інформаційної безпеки та кіберзахисту, оцінювання доцільності страхового покриття і визначення напрямів удосконалення процесів кіберстрахування. Для високих або критичних значень окремих складових ризику визначаються області, що потребують першочергового реагування, а для недостатніх значень зрілості — процеси, рівень розроблення, формалізації або впровадження яких потребує підвищення.

Сформована інформація не замінює рішення уповноваженої особи та не є безпосереднім розрахунком страхової премії, франшизи або ліміту страхового покриття. Вона становить структуровану інформаційну основу для страхового андеррайтингу, аналізу можливості страхування, визначення пріоритетних заходів реагування та підготовки обґрунтованих управлінських і страхових рішень.

Дванадцятим інформаційним процесом є накопичення результатів і проведення повторного оцінювання. Накопичення передбачає збереження в інформаційній системі вхідних даних, значень окремих показників, підіндексів, доменних підіндексів, інтегрального індексу та результатів їх інтерпретації для кожного завершеного циклу оцінювання.

Під час повторного оцінювання застосовуються та сама доменна структура, система показників і правила їх оброблення, що забезпечує порівнянність результатів, одержаних у різні моменти часу. Значення показників, підіндексів, доменних підіндексів та інтегрального індексу зіставляються з відповідними результатами попереднього циклу.

Порівняння послідовних результатів дає змогу визначити напрями й величину змін, оцінити результативність упроваджених заходів та уточнити

поточний профіль ризиків і зрілості процесів кіберстрахування. Отже, сформований інформаційний процес має циклічний характер: результати завершеного оцінювання накопичуються та використовуються як інформаційна основа для наступного циклу.

Узагальнену послідовність формування та використання інформації в межах RA&CIMM можна подати у вигляді:

вхідні дані → структуризація за доменами RA&CIMM → перевірка й уточнення даних → чисельне подання та нормування значень показників → визначення вагових характеристик → формування підіндексів → формування доменних підіндексів → формування профілю ризиків і зрілості → формування інтегрального індексу → інтерпретація результатів → формування інформації для підтримки прийняття рішень → накопичення результатів і повторне оцінювання.

Вхід зазначеної послідовності утворюють різнорідні дані про організаційний, управлінський, процесний і технічний стан суб'єкта й об'єкта оцінювання, характеристики ризиків інформаційної безпеки та кіберризиків, стан упровадження заходів інформаційної безпеки й кіберзахисту, а також зрілість процесів кіберстрахування.

Функціональне ядро оброблення даних утворюють модель RA&CIMM, метод формування підіндексів та інтегрального індексу і алгоритм багаторівневого оцінювання. Вихідними результатами є нормовані значення показників, підіндекси, доменні підіндекси, профіль ризиків і зрілості процесів кіберстрахування, інтегральний індекс, результати їх інтерпретації та структурована інформація для підтримки прийняття рішень.

Система показників та індексний підхід визначають способи чисельного подання, нормування й агрегування різнорідних даних. Формалізація інформаційних процесів кіберстрахування визначає їхні інформаційні входи, операції оброблення та вихідні результати. Модель RA&CIMM забезпечує доменну інтеграцію показників ризику і зрілості, метод формування підіндексів

та інтегрального індексу — порядок їх агрегування, а багаторівневий алгоритм — послідовність збирання, перевірки, уточнення, оброблення та повторного оцінювання даних [37].

Отже, поєднання розроблених моделей, методів та алгоритмічних процедур забезпечує формалізоване оброблення різнорідних даних про операційні ризики в кіберпросторі, їх доменну структуризацію, формування підіндексів, профілю ризиків і зрілості процесів кіберстрахування та інтегрального індексу RA&CIMM. Одержані результати створюють методологічну й алгоритмічну основу для підготовки структурованої інформації, придатної для підтримки прийняття рішень у процесах кіберстрахування.

Для практичної реалізації окремих процедур оцінювання вхідні дані можуть формуватися, зокрема, за результатами структурованого анкетного самооцінювання суб'єкта оцінювання. Кількісне оброблення та агрегування таких даних забезпечують формування часткового профілю, який використовується як одне з джерел інформації для комплексного оцінювання разом із результатами зовнішньої й експертної перевірки, технічного дослідження інформаційно-комунікаційної системи та іншими даними, передбаченими RA&CIMM. Пілотну апробацію окремих методичних та алгоритмічних положень на даних самооцінювання наведено в розділі 5.

Висновки до розділу 4

У результаті розроблення моделі оцінювання ризиків та зрілості кіберстрахування, методу формування підіндексів та інтегрального індексу, алгоритму багаторівневого оцінювання і підходу до формування інформації для підтримки прийняття рішень одержано такі результати.

1. Розроблено модель оцінювання ризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model, RA&CIMM), яка ґрунтується на системному й ризик-орієнтованому підходах і поєднує три взаємопов'язані домени: експертний домен оцінювання ризиків інформаційної безпеки та кіберризиків; мережевий домен оцінювання відповідних ризиків на основі технічних даних про стан інформаційно-комунікаційної системи; домен оцінювання зрілості процесів кіберстрахування [37].

2. Сформовано початковий експертний профіль RA&CIMM, що охоплює три основні домени та п'ятнадцять складових оцінювання з визначеними початковими ваговими характеристиками. Сумарне вагове значення складових експертного домену становить 0,50, мережевого домену — 0,25, домену оцінювання зрілості процесів кіберстрахування — 0,25. Початкові вагові значення мають експертний характер і можуть уточнюватися за результатами накопичення даних, повторного оцінювання та подальшого експертного аналізу.

3. Визначено функціональне призначення доменів RA&CIMM. Експертний домен забезпечує оцінювання організаційних, управлінських, процесних, кадрових, нормативних, фінансових і страхових характеристик ризику. Мережевий домен забезпечує формування показників на основі технічних даних про стан інформаційно-комунікаційної системи. Домен зрілості характеризує стан розроблення, формалізації, упровадження та технологічного забезпечення процесів кіберстрахування.

4. Розроблено метод формування підіндексів та інтегрального індексу RA&CIMM, що забезпечує послідовний перехід від нормованих значень окремих показників до підіндексів, доменних підіндексів, профілю ризиків і зрілості та інтегрального індексу з урахуванням вагових характеристик відповідних складових. Для подальшого формалізованого уточнення вагових коефіцієнтів передбачено можливість застосування методу аналізу ієрархій та інших експертних методів, які не використовувалися як джерело початкових вагових значень RA&CIMM.

5. Визначено критерії інтерпретації результатів оцінювання. Для показників ризику використовується стобальна шкала від дуже низького до критичного рівня ризику, а для показників зрілості процесів кіберстрахування — стобальна шкала, що охоплює початковий, повторюваний, встановлений, керований та оптимізований рівні. Установлено, що показники ризику і зрілості мають протилежну змістову спрямованість, тому їх спільне агрегування потребує попереднього нормування та приведення до узгодженої спрямованості.

6. Розроблено алгоритм багаторівневого оцінювання ризиків і зрілості процесів кіберстрахування, який формалізує послідовність операцій визначення суб'єкта й об'єкта оцінювання, збирання, перевірки, структуризації, чисельного подання, нормування, зважування, агрегування та інтерпретації різнорідних даних. Алгоритм охоплює чотири процедурні рівні: самооцінювання, зовнішнє оцінювання, експертну перевірку та повторне оцінювання. Технічне дослідження здійснюється в межах мережевого домену і не утворює окремого процедурного рівня.

7. Визначено узагальнену послідовність інформаційного оброблення даних у межах RA&CIMM: збирання вхідних даних; їх структуризація, перевірка й уточнення; чисельне подання та нормування значень показників; визначення вагових характеристик; формування підіндексів, доменних підіндексів, профілю ризиків і зрілості та інтегрального індексу; інтерпретація результатів; формування інформації для підтримки прийняття рішень; накопичення результатів і проведення повторного оцінювання.

8. Обґрунтовано спільне використання інтегрального індексу RA&CIMM, доменних підіндексів, підіндексів і профілю окремих показників. Таке подання забезпечує збереження внутрішньої структури результатів, визначення складових із відносно вищими значеннями ризику або недостатнім рівнем зрілості та формування інформації для визначення пріоритетності заходів реагування, оцінювання доцільності страхового покриття й удосконалення процесів кіберстрахування.

9. Сформовано методологічну й алгоритмічну основу підготовки структурованої інформації для підтримки прийняття рішень у процесах кіберстрахування. Її функціональне ядро утворюють модель RA&CIMM, метод формування підіндексів та інтегрального індексу і алгоритм багаторівневого оцінювання. Одержані результати забезпечують формалізований перехід від різнорідних вхідних даних до нормованих значень показників, підіндексів, доменних підіндексів, профілю ризиків і зрілості, інтегрального індексу та результатів їх інтерпретації.

Отже, у розділі 4 результати попередніх етапів дослідження інтегровано у взаємопов'язаний комплекс моделей, методів і алгоритмічних процедур, призначений для структуризації, формалізованого представлення, оброблення й аналізу різнорідних даних про ризики інформаційної безпеки, кіберризики та зрілість процесів кіберстрахування. Це забезпечує формування структурованої інформації для підтримки прийняття рішень у процесах кіберстрахування.

Одержані результати створюють основу для практичного застосування окремих положень RA&CIMM, розробленого методу й алгоритму на фактичних даних самооцінювання суб'єктів страхування. Пілотну апробацію відповідних методичних та алгоритмічних положень наведено в розділі 5.

РОЗДІЛ 5. ВИБІРКОВЕ ОЦІНЮВАННЯ ЦИФРОВОЇ ЗРІЛОСТІ СТРАХУВАЛЬНИКІВ ТА ЗРІЛОСТІ ПРОЦЕСІВ КІБЕРСТРАХУВАННЯ СТРАХОВИХ КОМПАНІЙ

Метою розділу є пілотна апробація розроблених у дисертації методу й алгоритму на фактичних даних самооцінювання суб'єктів страхування, а також визначення можливостей використання одержаних результатів для інформаційної підтримки прийняття рішень у процесах кіберстрахування. Апробацію проведено у двох взаємопов'язаних блоках: на вибірці з десяти страхувальників та за результатами первинного і повторного самооцінювання страхових компаній.

Логіка оброблення даних відповідає результатам, одержаним у розділах 3 і 4, та охоплює збирання, перевірку, кодування, нормування, структуризацію, агрегування й аналіз даних, а також формування інформації для підтримки прийняття рішень. У межах пілотного дослідження зазначені операції реалізовано з використанням структурованих електронних анкет, словників кодування, розрахункових таблиць, правил контролю якості даних, доменних профілів, часткових та інтегральних показників і рекомендацій.

Модель оцінювання ризиків та зрілості кіберстрахування (Risk Assessment & Cyber Insurance Maturity Model, RA&CIMM) використано як загальну методологічну основу пілотного дослідження. Водночас наведені в розділі результати не є остаточною комплексною оцінкою за RA&CIMM, оскільки ґрунтуються переважно на даних самооцінювання. Для комплексного застосування моделі такі дані мають доповнюватися результатами зовнішньої й експертної перевірки, технічного дослідження інформаційно-комунікаційної системи та аналізу фінансових і страхових характеристик ризику.

Інформаційну базу та призначення окремих блоків пілотної апробації систематизовано в таблиці 5.1.

Таблиця 5.1 — Інформаційна база та призначення блоків пілотної апробації

Блок оцінювання	**Обсяг даних**	**Характер даних**	**Призначення**
Страхувальники	10 анкет; 30 питань, із яких 23 включено до кількісного оцінювання	Анонімізовані результати одноразового самооцінювання	Формування часткового профілю цифрової зрілості, виявлення критичних прогалин і підготовка інформації для попереднього оцінювання страхової прийнятності
Страхові компанії	2 компанії × 2 цикли оцінювання; 188 відповідей у кожному профілі; 752 відповіді загалом	Анонімізовані результати первинного і повторного самооцінювання	Порівняння значень показників у послідовних циклах, визначення їх змін та аналіз переходу між рівнями зрілості
Розрахункові модулі	Словники кодування, правила контролю якості даних, доменні та інтегральні показники, правила формування рекомендацій	Електронні таблиці з автоматизованими розрахунковими й контрольними операціями	Перевірка відтворюваності розрахунків та підготовка алгоритмічних процедур до подальшої програмної реалізації

Джерело: складено автором за матеріалами пілотної апробації.

5.1. Вибіркове оцінювання цифрової зрілості страхувальників

Перший блок пілотної апробації спрямовано на перевірку придатності розробленого структурованого опитувальника [165] та процедур оброблення даних для формування кількісного профілю цифрової зрілості страхувальника. З огляду на невеликий обсяг вибірки та відсутність випадкового відбору одержані результати мають розвідувальний характер і не можуть без проведення додаткових досліджень поширюватися на генеральну сукупність підприємств України.

Призначення цього блоку полягає у перевірці процедур збирання, кодування, контролю якості, нормування й агрегування даних, формування доменних і узагальненого показників, виявлення критичних прогалин та підготовки попередніх рекомендацій. Одержані результати характеризують дані самооцінювання респондентів і не є результатами незалежного аудиту кібербезпеки або комплексного оцінювання за моделлю RA&CIMM.

Анкета містила 30 питань, із яких для кількісного оцінювання використано 23 позиції: Q1 та Q3–Q24. Питання Q2 характеризувало технологічний контекст; Q25 виконувало функцію контрольного самооцінювання; Q26–Q30 використовувалися для опису й сегментації профілю респондента. Такий розподіл запобігає механічному включенню контекстних, контрольних і профільних відповідей до узагальненого показника. Структуру оцінювання наведено в таблиці 5.2.

Таблиця 5.2 — Структура оцінювання цифрової зрілості страхувальників

Компонент	**Питання**	**Кількість**	**Вага**	**Зміст**
D1	Q1, Q3–Q8	7	30 %	Цифровізація та інформаційно-технологічна інфраструктура
D2	Q9–Q17	9	40 %	Кіберзахист і управління ризиками
D3	Q18–Q24	7	30 %	Конфіденційність, управління даними та відповідність вимогам
Контекст	Q2	1	Не зважується	Перелік і поширеність використовуваних технологій
Контроль	Q25	1	Не зважується	Загальне самооцінювання кіберготовності
Профіль	Q26–Q30	5	Не зважуються	Характеристики респондента та витрат на страхування

Джерело: складено автором за структурою опитувальника страхувальників.

Для кількісного узагальнення результатів анкетного самооцінювання страхувальників у межах пілотної апробації сформовано композитний індекс цифрової зрілості (Composite Digital Maturity Index, CDMI). У структурі розробленого підходу CDMI є частковим показником, сформованим за

результатами анкетного самооцінювання, і не ототожнюється з інтегральним індексом RA&CIMM. Його призначення полягає в кількісному узагальненні результатів структурованого самооцінювання для подальшого використання як одного із джерел вхідних даних у комплексній процедурі оцінювання ризиків і зрілості процесів кіберстрахування.

Якісні відповіді переведено у шкалу від 0 до 100 балів із кроком 25 балів. В основному варіанті розрахунку пропущені відповіді не включалися до середнього значення відповідного домену, а за наявності декількох відповідей на одне порядкове питання використовувалося найменше розпізнане значення. Такий підхід зменшує ризик завищення результату. Додатково для аналізу чутливості сформовано консервативний варіант розрахунку CDMI (CDMI-UW), у якому пропущені відповіді та відповіді «не застосовується» оцінювалися як нуль.

У первинному варіанті методики передбачалося оцінювання всіх 25 змістових питань. Після перевірки фактичної структури анкети цю схему уточнено: Q2 залишено контекстною змінною, оскільки сам факт використання певної технології не підтверджує зрілості її застосування, а Q25 використано як контрольне самооцінювання для зіставлення з розрахованим індексом. Тому в межах пілотного оцінювання CDMI формується за 23 показниками. Це уточнення не скорочує інформаційної бази анкети, а запобігає подвійному врахуванню та методологічно необґрунтованому зважуванню описових відповідей.

Таблиця 5.3 — Перетворення п’ятибальної якісної шкали у нормовані оцінки

Рівень	**Якісна інтерпретація**	**Нормована оцінка**
1	Контроль відсутній, стан невідомий або критично низький	0
2	Захід заплановано або реалізовано мінімально чи фрагментарно	25
3	Контроль упроваджено частково	50
4	Контроль переважно впроваджено, але він потребує вдосконалення	75
5	Контроль повністю й стабільно впроваджено	100

Джерело: розроблено автором для пілотного оцінювання.

Математичну операціоналізацію пілотного анкетного показника здійснено таким чином. Якщо l_{kj} — якісна оцінка j-го показника k-го страхувальника за шкалою від 1 до 5, то нормована оцінка s_{kj} визначають за формулою:

$$s_{kj} = 25 \cdot (l_{kj} - 1), \quad l_{kj} \in \{1, 2, 3, 4, 5\}.$$

Доменний індекс D_kd визначають як середнє арифметичне нормованих оцінок за фактично доступними показниками d-го домену:

$$D_{kd} = \frac{1}{n_{kd}} \sum_{j=1}^{n_{kd}} s_{kj},$$

де n_{kd} — кількість доступних для оцінювання показників d-го домену для k-го страхувальника. За повного заповнення анкети внесок кожного показника доменів D1 і D3 у підсумкове значення CDMI становить приблизно 4,29 %, а кожного показника домену D2 — приблизно 4,44 %. Доменні значення агрегують із ваговими коефіцієнтами 0,30; 0,40 та 0,30:

$$CDMI_k = 0{,}30 \cdot D_{k1} + 0{,}40 \cdot D_{k2} + 0{,}30 \cdot D_{k3}.$$

В основному варіанті розрахунку CDMI пропущене значення виключається з кількості доступних показників відповідного домену. У консервативному варіанті CDMI-UW пропущене значення прирівнюється до нуля. Такий поділ дає змогу проаналізувати фактично надані відповіді та одночасно сформувати консервативну оцінку для попереднього визначення страхової прийнятності. Наведений математичний опис є операціоналізацією анкетного компонента пілотного оцінювання і не замінює математичної моделі RA&CIMM, обґрунтованої в розділі 4. Значення CDMI розглядається як частковий результат анкетного самооцінювання, який може використовуватися разом з іншими джерелами даних у комплексній процедурі оцінювання.

Для інтерпретації значень CDMI використано п’ять рівнів зрілості: початковий — від 0 до 20 балів включно; повторюваний — понад 20 до 40 балів включно; встановлений — понад 40 до 60 балів включно; керований — понад 60

до 80 балів включно; оптимізований — понад 80 до 100 балів включно. Додатково в межах пілотного оцінювання застосовано авторське правило перевірки критичних контрольних умов, до яких віднесено резервне копіювання (Q12), захист комунікацій (Q13) та наявність плану реагування на кіберінциденти (Q17). Значення нижче 50 балів хоча б за одним із цих показників фіксувалося як критична прогалина незалежно від значення CDMI.

Таблиця 5.4 — Оцінки страхувальників за показниками домену D1, балів

Респондент	Q1	Q3	Q4	Q5	Q6	Q7	Q8	D1
R01	25	0	50	25	50	50	50	35,71
R02	25	50	75	50	50	50	50	50,00
R03	0	0	50	0	25	0	25	14,29
R04	50	50	75	100	50	50	100	67,86
R05	50	50	75	100	50	50	50	60,71
R06	25	50	75	50	50	25	50	46,43
R07	25	50	25	25	50	0	25	28,57
R08	50	50	75	100	50	50	100	67,86
R09	50	50	25	50	50	0	50	39,29
R10	100	100	75	100	25	100	100	85,71

Джерело: розраховано автором за результатами пілотного оцінювання.

Таблиця 5.5 — Оцінки страхувальників за показниками домену D2, балів

Респондент	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	D2
R01	0	25	0	25	0	25	0	0	0	8,33
R02	25	25	25	50	25	50	0	25	25	27,78
R03	25	0	0	25	0	25	0	0	0	8,33
R04	50	75	50	100	50	100	75	50	25	63,89
R05	25	75	75	100	50	100	0	25	25	52,78
R06	25	0	0	50	0	25	0	0	25	13,89
R07	н/д	0	н/д	25	25	25	0	25	0	14,29
R08	50	100	75	100	100	100	75	50	25	75,00
R09	50	75	0	50	н/д	25	0	0	0	25,00
R10	100	100	75	100	100	100	75	100	50	88,89

Примітка. н/д — відповідь відсутня або обрано варіант «не застосовується»; відповідне значення не включається до розрахунку середнього значення домену.
Джерело: розраховано автором за результатами пілотного оцінювання.

Таблиця 5.6 — Оцінки страхувальників за показниками домену D3 та значення CDMI, балів

Респондент	Q18	Q19	Q20	Q21	Q22	Q23	Q24	D3	CDMI
R01	100	н/д	0	25	0	0	0	20,83	20,30
R02	100	0	0	75	25	25	0	32,14	35,75
R03	100	н/д	0	0	0	0	0	16,67	12,62
R04	100	25	100	100	25	50	50	64,29	65,20
R05	100	0	25	75	25	50	0	39,29	51,11
R06	100	н/д	0	25	25	0	0	25,00	26,98
R07	100	н/д	0	25	25	0	0	25,00	21,79
R08	100	25	50	100	25	50	50	57,14	67,50
R09	100	н/д	0	0	25	0	0	20,83	28,04
R10	100	50	100	100	100	50	50	78,57	84,84

Примітка. н/д — відповідь відсутня або обрано варіант «не застосовується»; відповідне значення не включається до розрахунку середнього значення домену.
Джерело: розраховано автором за результатами пілотного оцінювання.

Таблиця 5.7 — Індивідуальні результати пілотного оцінювання страхувальників, балів

Респондент	D1	D2	D3	CDMI	Консервативний CDMI	Рівень зрілості за CDMI	Попередня категорія для подальшого страхового оцінювання
R01	35,71	8,33	20,83	20,30	19,40	Повторюваний	Потребує усунення критичних прогалин
R02	50,00	27,78	32,14	35,75	35,75	Повторюваний	Потребує усунення критичних прогалин
R03	14,29	8,33	16,67	12,62	11,90	Початковий	Потребує усунення критичних прогалин
R04	67,86	63,89	64,29	65,20	65,20	Керований	Умовно прийнятний для подальшого оцінювання
R05	60,71	52,78	39,29	51,11	51,11	Встановлений	Умовно прийнятний для подальшого оцінювання
R06	46,43	13,89	25,00	26,98	25,91	Повторюваний	Потребує усунення критичних прогалин

Респондент	D1	D2	D3	CDMI	Консервативний CDMI	Рівень зрілості за CDMI	Попередня категорія для подальшого страхового оцінювання
R07	28,57	14,29	25,00	21,79	19,44	Повторюваний	Потребує усунення критичних прогалин
R08	67,86	75,00	57,14	67,50	67,50	Керований	Умовно прийнятний для подальшого оцінювання
R09	39,29	25,00	20,83	28,04	26,03	Повторюваний	Потребує усунення критичних прогалин
R10	85,71	88,89	78,57	84,84	84,84	Оптимізований	Прийнятний для подальшого оцінювання

Примітка. Консервативний CDMI розраховано з прирівнюванням пропущених відповідей і відповідей «не застосовується» до нуля. За його значеннями профілі R01 і R07 переходять із повторюваного до початкового рівня. Наведені категорії мають попередній інформаційний характер, використовуються для визначення напряму подальшого оцінювання та не є рішеннями щодо укладення договорів страхування.
Джерело: розраховано автором за результатами пілотного оцінювання.

Середнє значення CDMI у досліджуваній вибірці становило 41,41 бала, медіана — 31,89 бала, а значення показника перебували в діапазоні від 12,62 до 84,84 бала. Перевищення середнього значення над медіаною зумовлене наявністю декількох відносно високих результатів, передусім значенням профілю R10. Вибіркове стандартне відхилення становило 24,28 бала, що свідчить про істотну варіативність результатів у межах пілотної вибірки.

Таблиця 5.8 — Узагальнені статистичні характеристики вибірки страхувальників

Показник	Значення	Інтерпретація
Кількість респондентів	10	Пілотна невипадкова вибірка
Середнє CDMI	41,41	Відповідає встановленому рівню за прийнятою шкалою
Медіана CDMI	31,89	Відповідає повторюваному рівню за прийнятою шкалою
Мінімальне / максимальне значення	12,62 / 84,84	Діапазон одержаних значень
Вибіркове стандартне відхилення	24,28	Варіативність результатів у межах вибірки
Середня повнота даних	96,52 %	Частка наявних оцінюваних відповідей
Середнє значення D1	49,64	Найвище середнє значення серед трьох доменів

Показник	Значення	Інтерпретація
Середнє значення D2	37,82	Нижче за середнє значення D1
Середнє значення D3	37,98	Нижче за середнє значення D1
Рангова кореляція CDMI з категорією загальних витрат на страхування	$\rho = 0{,}692$	Додатний ранговий зв’язок у межах пілотної вибірки

Джерело: розраховано автором за результатами пілотного оцінювання.

За основним варіантом розрахунку один профіль відповідав початковому рівню, п’ять — повторюваному, один — встановленому, два — керованому та один — оптимізованому рівню. Отже, шість із десяти профілів не досягли встановленого рівня. За консервативним варіантом розрахунку CDMI розподіл змістився в бік нижчих рівнів: три профілі відповідали початковому рівню, три — повторюваному, один — встановленому, два — керованому та один — оптимізованому. Відмінність між двома варіантами розрахунку демонструє вплив способу оброблення пропущених і неоднозначних відповідей на результат оцінювання.

Порівняння доменних значень показало, що середній результат за доменом цифровізації та інформаційно-технологічної інфраструктури був вищим, ніж за доменами кіберзахисту й управління ризиками та конфіденційності, управління даними і відповідності вимогам. Середнє значення D1 становило 49,64 бала, тоді як середні значення D2 і D3 — відповідно 37,82 та 37,98 бала. Одержані результати свідчать, що в межах досліджуваної вибірки відносно вищий рівень цифровізації не в усіх випадках супроводжувався відповідним рівнем організаційних, процедурних і контрольних механізмів кіберзахисту.

Для попередньої інтерпретації результатів пілотного оцінювання використано поєднання значення консервативного CDMI та результатів перевірки критичних контрольних умов. Якщо значення консервативного CDMI не перевищувало 40 балів, профіль відносили до категорії, що потребує усунення критичних прогалин до проведення подальшого оцінювання. Якщо значення перевищувало 40 балів, але хоча б один із критичних показників був нижчим за

50 балів, профіль вважали умовно прийнятним для подальшого оцінювання після усунення відповідної прогалини. Значення понад 40 до 80 балів за відсутності критичних прогалин відповідало категорії прийнятності для подальшого оцінювання на індивідуальних умовах, а значення понад 80 балів за відсутності критичних прогалин — категорії прийнятності для подальшого оцінювання. Зазначені правила мають пілотний характер і не є правилами автоматичного андеррайтингового рішення.

Таблиця 5.9 — Розподіл профілів за попередніми категоріями подальшого страхового оцінювання

Категорія оцінки	Кількість	Частка	Інтерпретація
Потребує усунення критичних прогалин	6	60 %	Низьке значення консервативного CDMI; подальше оцінювання доцільне після впровадження мінімально необхідних заходів
Умовно прийнятний для подальшого оцінювання	3	30 %	Подальше оцінювання можливе після документованого усунення критичних прогалин
Прийнятний для подальшого оцінювання на індивідуальних умовах	0	0 %	Профілі цієї категорії у вибірці відсутні
Прийнятний для подальшого оцінювання	1	10 %	Критичних прогалин не виявлено; необхідна зовнішня перевірка наданих відомостей і доказів

Примітка. Наведені категорії є результатом попередньої інтерпретації даних пілотного самооцінювання, використовуються для визначення подальших процедур перевірки та не є рішеннями щодо укладення договорів страхування.
Джерело: розраховано автором за результатами пілотного оцінювання.

За результатами контролю якості даних виявлено 16 випадків множинних відповідей у порядкових питаннях, чотири пропущені відповіді, п’ять відповідей «не застосовується» та три невизначені відповіді. Аналіз чутливості з використанням мінімального, середнього і максимального варіантів кодування множинних відповідей показав, що найбільша можлива зміна індивідуального результату становила 5,40 бала. Це характеризує чутливість розрахунку до способу кодування множинних відповідей і підтверджує доцільність застосування вбудованих засобів контролю електронної форми, які унеможливлюють одночасний вибір взаємовиключних варіантів.

Коефіцієнт рангової кореляції Спірмена між CDMI та категорією загальних річних витрат на страхування становив $\rho = 0{,}692$. Одержане додатне значення

характеризує напрям і силу рангового зв’язку в межах досліджуваної вибірки, однак через її невеликий обсяг і невипадковий характер не може інтерпретуватися як причинна залежність або поширюватися на генеральну сукупність. Крім того, відповідне питання характеризувало загальні витрати на страхування, а не розмір страхової премії за договором кіберстрахування. Тому одержаний результат має розвідувальне значення і не може безпосередньо використовуватися для тарифного калібрування.

Результати пілотного оцінювання страхувальників продемонстрували можливість спільного використання CDMI та критичних контрольних умов для формування структурованого профілю самооцінювання. Агреговане значення не повинно компенсувати відсутність окремих критичних заходів, зокрема резервного копіювання, захисту комунікацій або плану реагування на кіберінциденти. Результат анкетного самооцінювання доцільно розглядати не як автоматичне рішення щодо укладення договору страхування, а як структурований інформаційний вхід для подальшого комплексного оцінювання, зовнішньої й експертної перевірки, технічного дослідження інформаційно-комунікаційної системи, визначення необхідного обсягу доказів і формування рекомендацій щодо першочергових заходів.

5.2. Повторне самооцінювання зрілості процесів кіберстрахування страхових компаній

Другий блок пілотної апробації присвячено повторному самооцінюванню зрілості процесів кіберстрахування страхових компаній, анонімізованих у дослідженні як СК1 та СК2. Для кожної компанії опрацьовано результати первинного оцінювання станом на 6 червня 2026 року та повторного оцінювання

станом на 6 вересня 2026 року. Загалом сформовано профілі, кожен із яких містив 188 відповідей; загальна кількість опрацьованих відповідей становила 752.

Одержані результати ґрунтуються на даних анкетного самооцінювання і не ототожнюються з результатами незалежного аудиту, зовнішньої чи експертної перевірки або технічного дослідження фактичного стану інформаційно-комунікаційних систем і впровадження відповідних заходів. Назви страхових компаній у дисертації анонімізовано. Результати первинного і повторного самооцінювання використано для апробації процедур кількісного оброблення анкетних даних, формування часткового профілю зрілості та аналізу зміни його показників у часі.

Анкета містила 188 питань. Перші 70 питань характеризували організаційний, продуктовий та операційний контексти оцінювання і не включалися до кількісного розрахунку. Кількісний модуль охоплював 118 контрольних позицій Q71–Q188. Відповіді на ці позиції кодувалися за шкалою: «так» — 100 балів, «частково» — 50 балів, «ні» — 0 балів. У межах пілотного розрахунку всі контрольні позиції мали однакові вагові коефіцієнти. Одержаний показник характеризує результат анкетного самооцінювання за відповідним набором контрольних позицій і використовується для формування часткового профілю зрілості процесів кіберстрахування. Він не є результатом сертифікації та не замінює комплексного оцінювання за моделлю RA&CIMM.

Таблиця 5.10 — Результати первинного і повторного самооцінювання страхових компаній

Компанія	**Дата / період**	**Так**	**Частково**	**Ні**	**Показник самооцінювання, балів**	**Рівень зрілості**
СК1	06.06.2026	30	69	19	54,66	Встановлений
СК1	07.09.2026	40	67	11	62,29	Керований
Зміна	3 місяці	+10	–2	–8	+7,63	Від встановленого до керованого рівня
СК2	24.05.2026	25	69	24	50,42	Встановлений
СК2	25.08.2026	39	64	15	60,17	Керований
Зміна	3 місяці	+14	–5	–9	+9,75	Від встановленого до керованого рівня

Джерело: розраховано автором за результатами повторного самооцінювання страхових компаній.

За результатами первинного самооцінювання показник СК1 становив 54,66 бала, що відповідало встановленому рівню за прийнятою шкалою. За результатами повторного самооцінювання його значення збільшилося до 62,29 бала, що відповідало керованому рівню. Приріст за три місяці становив 7,63 бала. У структурі відповідей кількість відповідей «так» збільшилася на 10, кількість відповідей «частково» зменшилася на 2, а відповідей «ні» — на 8.

Для СК2 початкове значення показника становило 50,42 бала, що відповідало встановленому рівню. За результатами повторного самооцінювання показник збільшився до 60,17 бала і відповідав керованому рівню за прийнятою шкалою. Приріст за три місяці становив 9,75 бала. Кількість відповідей «так» збільшилася на 14, кількість відповідей «частково» зменшилася на 5, а відповідей «ні» — на 9.

Таблиця 5.11 — Зміна оцінок за контрольними напрямами, балів

№	Контрольний напрям	СК1, первинне оцінювання	СК1, повторне оцінювання	СК2, первинне оцінювання	СК2, повторне оцінювання
1	Система управління кібербезпекою	70,00	80,00	70,00	80,00
2	Внутрішні нормативні документи	50,00	61,11	44,44	55,56
3	Управління кіберризиками	41,67	58,33	41,67	58,33
4	Управління ІТ-активами	75,00	83,33	75,00	83,33
5	Управління доступом	65,00	75,00	60,00	70,00
6	Автентифікація та ідентифікація	64,29	78,57	50,00	64,29
7	Управління обліковими записами	58,33	75,00	50,00	58,33
8	Парольна політика	66,67	75,00	50,00	66,67
9	Захист кінцевих пристроїв	87,50	87,50	87,50	87,50
10	Привілейовані користувачі	33,33	33,33	16,67	16,67
11	Журналювання та моніторинг	45,83	50,00	45,83	58,33
12	Мережева безпека	50,00	56,25	43,75	56,25
13	Захист серверів і систем	66,67	66,67	66,67	66,67
14	Управління програмним забезпеченням	38,89	44,44	33,33	44,44
15	Знімні носії	33,33	33,33	33,33	41,67

№	Контрольний напрям	СК1, первинне оцінювання	СК1, повторне оцінювання	СК2, первинне оцінювання	СК2, повторне оцінювання
16	Управління інцидентами	44,44	55,56	50,00	61,11
17	Управління підрядниками	61,11	61,11	55,56	55,56

Джерело: розраховано автором за результатами первинного і повторного самооцінювання страхових компаній.

За результатами повторного самооцінювання СК1 підвищення показників зафіксовано за 12 із 17 контрольних напрямів. Найбільші зміни стосувалися управління кіберризиками — з 41,67 до 58,33 бала, управління обліковими записами — з 58,33 до 75,00 бала, а також автентифікації та ідентифікації — з 64,29 до 78,57 бала. Значення за напрямами захисту кінцевих пристроїв, управління привілейованими користувачами, захисту серверів і систем, знімних носіїв та управління підрядниками залишилися без змін.

За результатами повторного самооцінювання СК2 підвищення показників зафіксовано за 13 із 17 контрольних напрямів. Найбільші зміни виявлено за напрямами управління кіберризиками — з 41,67 до 58,33 бала, парольної політики — з 50,00 до 66,67 бала, автентифікації та ідентифікації — з 50,00 до 64,29 бала, журналювання та моніторингу — з 45,83 до 58,33 бала, а також мережевої безпеки — з 43,75 до 56,25 бала. Без змін залишилися показники захисту кінцевих пристроїв, управління привілейованими користувачами, захисту серверів і систем та управління підрядниками.

Результати двох циклів самооцінювання демонструють можливість кількісного відстеження змін окремих контрольних показників і сформованого на їх основі часткового профілю зрілості процесів кіберстрахування. Водночас підвищення показника та його відповідність вищому рівню за прийнятою шкалою не є самостійним підтвердженням фактичного підвищення зрілості системи управління. Для комплексного оцінювання одержані результати мають доповнюватися документальними доказами, зовнішньою й експертною перевіркою, технічним дослідженням інформаційно-комунікаційної системи та іншими джерелами даних, передбаченими моделлю RA&CIMM.

5.3. Автоматизація оброблення даних під час оцінювання цифрової зрілості та зрілості процесів кіберстрахування

Проведена пілотна апробація підтвердила можливість подання окремих процесів оцінювання у сфері кіберстрахування як послідовності інформаційних операцій над структурованими даними. У пілотній реалізації вхідними даними були результати самооцінювання, відомості про управління ризиками, застосування заходів кіберзахисту та стан відповідних організаційних і технологічних контролів. Оброблення даних охоплювало їх збирання, структуризацію, перевірку, кодування, нормування, зважування, агрегування, аналіз невизначеності та формування рекомендацій.

Для оцінювання страхувальників дослідний розрахунковий модуль містив окремі структурні компоненти для збереження первинних даних, словника кодування, оцінок окремих питань, доменних і узагальнених розрахунків, аналізу чутливості, контролю якості даних та формування рекомендацій. Для страхових компаній реалізовано оброблення профілів первинного і повторного самооцінювання, розрахунок показників за контрольними напрямами та порівняння результатів двох послідовних циклів. Така декомпозиція забезпечує простежуваність результату від первинної відповіді до сформованого профілю.

Послідовність інформаційних операцій, реалізованих у межах дослідного розрахункового модуля, систематизовано в таблиці 5.12.

Таблиця 5.12 — Алгоритмічні етапи автоматизованого оцінювання

Етап	**Інформаційна операція**	**Результат**	**Контроль**
1	Реєстрація суб’єкта, версії анкети та дати оцінювання	Ідентифікований профіль оцінювання	Унікальний код, дата, тип суб’єкта
2	Збирання відповідей через електронну форму або імпортування даних	Набір первинних даних	Обов’язковість полів, допустимі формати і значення

Етап	Інформаційна операція	Результат	Контроль
3	Перевірка повноти та логічної узгодженості	Журнал контролю якості даних	Пропуски, множинні та суперечливі відповіді
4	Кодування і нормування якісних відповідей	Нормовані оцінки в діапазоні від 0 до 100 балів	Версійований словник кодування
5	Групування показників за доменами, зважування й агрегування	Доменні показники та узагальнений профіль	Перевірка вагових коефіцієнтів і допустимих діапазонів
6	Аналіз невизначеності та чутливості результатів	Основний і консервативний варіанти розрахунку	Правила оброблення пропущених, множинних і неоднозначних відповідей
7	Перевірка критичних контрольних умов	Перелік критичних прогалин	Установлені для пілотного оцінювання порогові значення
8	Класифікація результатів і формування рекомендацій	Рівень зрілості, попередня категорія подальшого оцінювання та перелік рекомендованих заходів	Заборона автоматичного формування остаточного страхового рішення без верифікації
9	Збереження версії та проведення повторного оцінювання	Порівняння результатів послідовних циклів	Аудиторський слід і підтверджувальні матеріали

Джерело: розроблено автором у межах пілотної реалізації процедур оцінювання.

Автоматизація не повинна обмежуватися обчисленням середнього значення показника. Необхідними складовими є контроль структури й повноти даних, виявлення взаємовиключних відповідей, керування версіями словника кодування, збереження первинних значень, забезпечення простежуваності внеску кожного показника та окреме відображення невизначеності результату. Результат оцінювання має подаватися користувачеві не лише як одне числове значення, а й у вигляді доменного профілю, переліку критичних прогалин, пояснення сформованої категорії та пріоритетного переліку коригувальних заходів.

Розрахункові таблиці та дослідний вебзастосунок, використані під час апробації, доцільно визначати як дослідні реалізації окремих складових автоматизованого розрахункового модуля, а не як завершену програмну систему. Вони забезпечують автоматизоване виконання розрахункових і контрольних операцій, відтворюваність установлених правил оброблення даних,

представлення індивідуальних і зведених результатів та порівняння результатів повторного оцінювання. Для створення повнофункціональної захищеної інформаційної системи необхідно додатково передбачити рольове розмежування доступу, журналювання операцій, криптографічний захист інформації, механізми приєднання підтверджувальних матеріалів, керування версіями методики та інтеграцію з інформаційними системами страховика.

З урахуванням результатів пілотної апробації визначено функціональні модулі, які доцільно передбачити під час подальшого розвитку дослідного вебзастосунку до рівня повнофункціональної інформаційної системи оцінювання ризиків і зрілості процесів кіберстрахування. Запропоновану структуру модулів наведено в таблиці 5.13.

Таблиця 5.13 — Функціональні модулі автоматизації процесів оцінювання

Модуль	**Основні функції**	**Користувачі**	**Вихідні дані**
Анкетування	Налаштування електронних форм, перевірка введених даних, проведення повторних циклів	Страхувальник, страховик	Структуровані первинні дані
Управління підтверджувальними матеріалами	Завантаження документів, посилань і технічних підтверджень	Респондент, аудитор, експерт	Підтверджені та непідтверджені відомості
Розрахунок	Кодування, нормування, формування часткових і доменних показників, аналіз чутливості	Андеррайтер, аналітик	Профіль ризиків і зрілості
Підтримка прийняття рішень	Перевірка критичних умов, застосування правил ескалації, ручне погодження результатів	Андеррайтер, ризик-менеджер	Попередня категорія подальшого оцінювання
Формування рекомендацій	Виявлення прогалин і визначення пріоритетності заходів	Керівник, фахівець із кібербезпеки	Перелік рекомендованих коригувальних заходів

Модуль	Основні функції	Користувачі	Вихідні дані
Моніторинг	Порівняння версій, аналіз зміни доменних показників, формування сповіщень	Страховик, страхувальник	Звіт про зміну результатів оцінювання
Портфельна аналітика	Агрегування анонімізованих профілів і сегментація даних	Страховик, аналітик, актуарі	Розподіли, групи профілів і показники портфеля

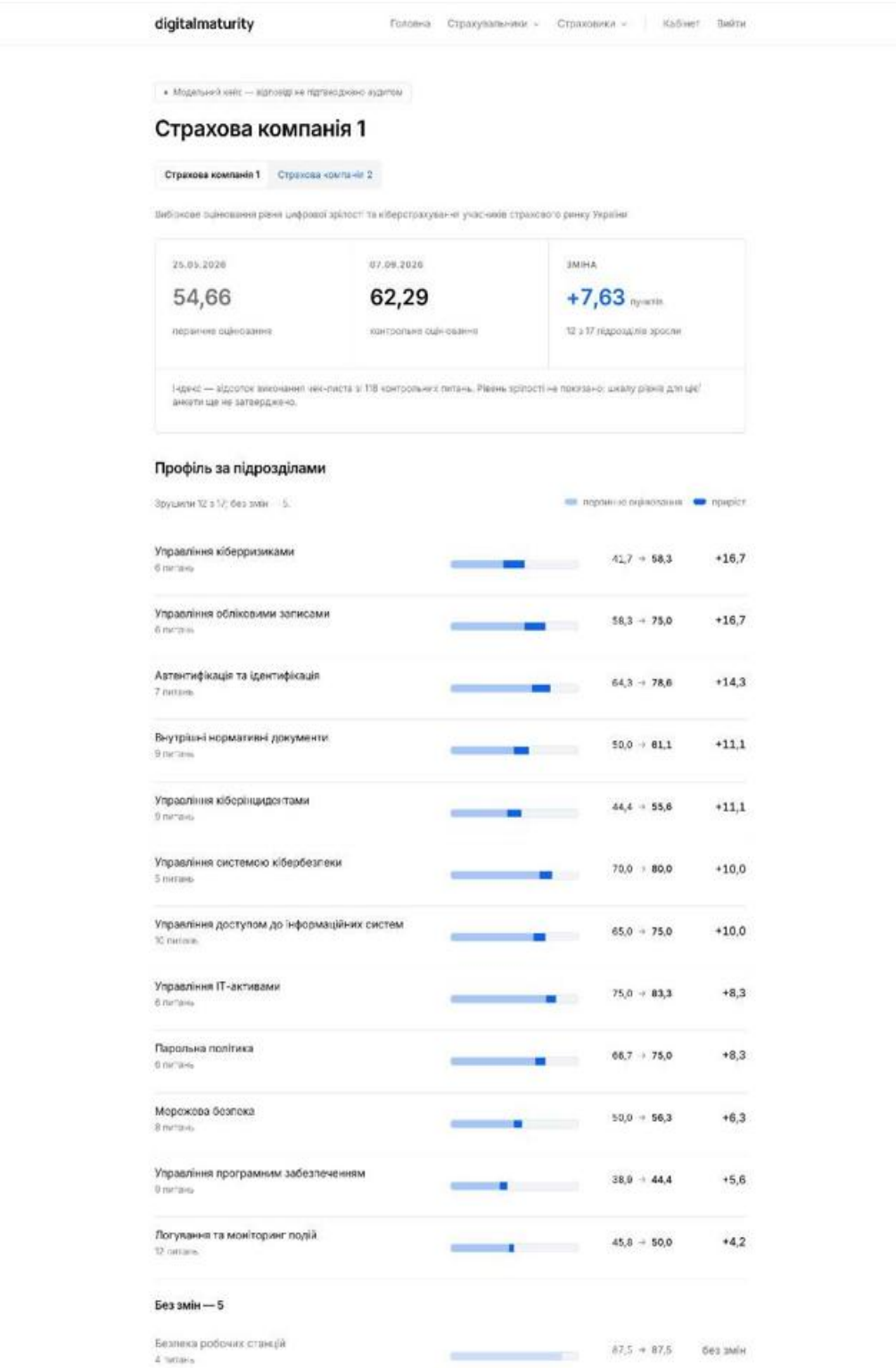
Джерело: запропоновано автором за результатами пілотної апробації.

Для перевірки можливості програмної реалізації розроблених алгоритмічних процедур створено дослідний вебзастосунок оцінювання цифрової зрілості та зрілості процесів кіберстрахування. Вебзастосунок забезпечує реєстрацію користувачів, проведення анкетного самооцінювання страхувальників і страхових компаній, перевірку та зберігання введених даних, чисельне кодування відповідей, обчислення часткових і доменних показників, формування узагальненого профілю та віднесення результату до відповідного рівня зрілості.

Для страхувальників реалізовано електронний опитувальник, індивідуальний кабінет і формування звіту з результатами оцінювання за трьома доменами. У звіті відображаються значення доменних показників, узагальнений показник, рівень зрілості та перелік рекомендацій. Для страхових компаній передбачено розширений контрольний перелік, формування профілю за окремими напрямами, порівняння результатів первинного і повторного оцінювання та відображення зміни показників у часі.

Адміністративний модуль забезпечує узагальнення результатів вибірки, розподіл профілів за рівнями зрілості, обчислення статистичних характеристик, перегляд доменних показників і вивантаження структурованих даних для подальшого аналізу. Приклади реалізованих екранних форм наведено на рисунках 5.1–5.4. Практичну реалізацію процедури первинного та повторного оцінювання в дослідному вебзастосунку наведено на рисунку 5.1.

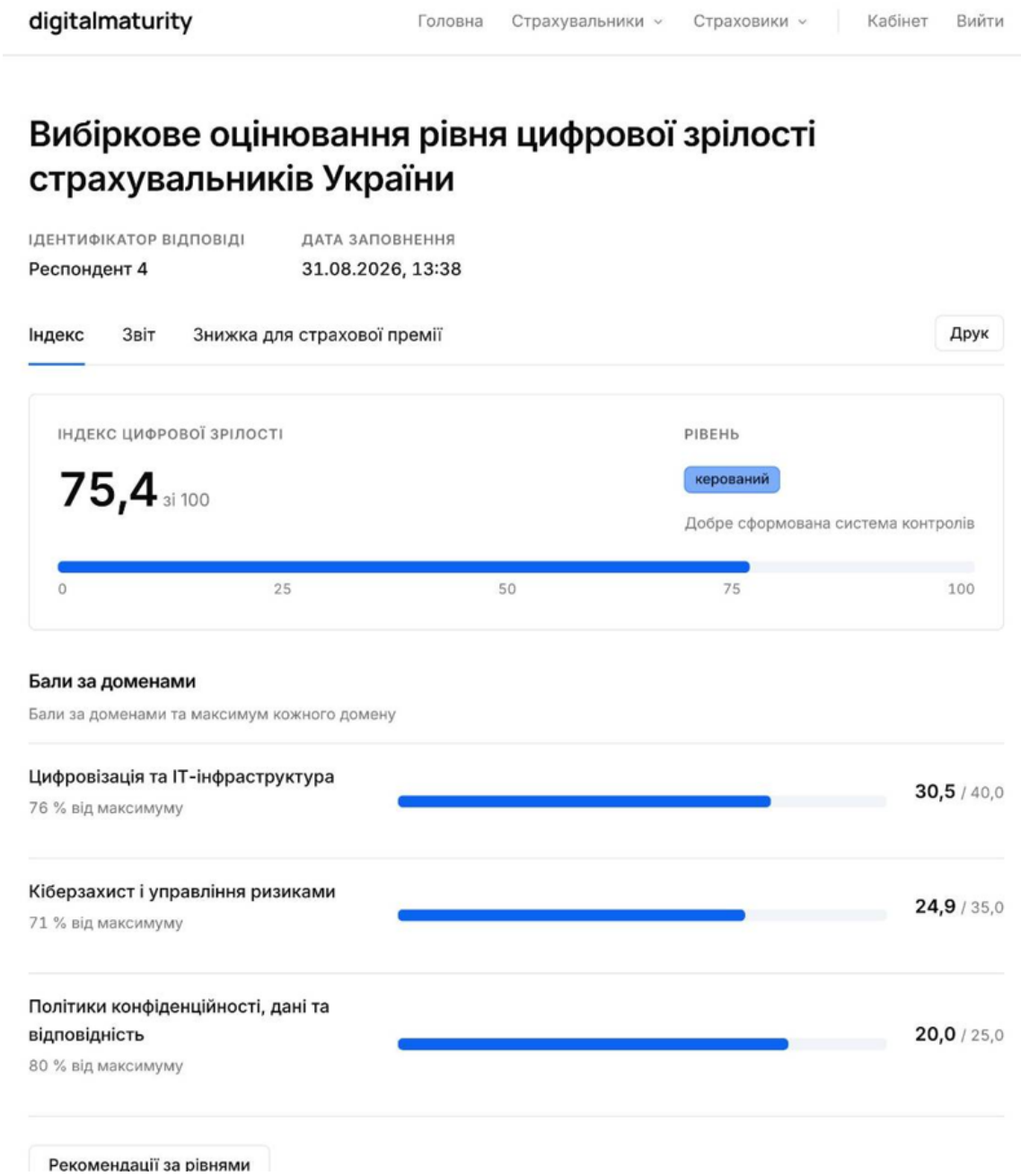
Рисунок 5.1 — Результати первинного та повторного оцінювання страхової компанії в дослідному вебзастосунку



Джерело: розроблено автором.

Сформований вебзастосунком індивідуальний профіль містить узагальнене значення показника, результати за окремими доменами та їх графічне подання (рисунок 5.2).

Рисунок 5.2 — Індивідуальний профіль результатів оцінювання страхувальника в дослідному вебзастосунку

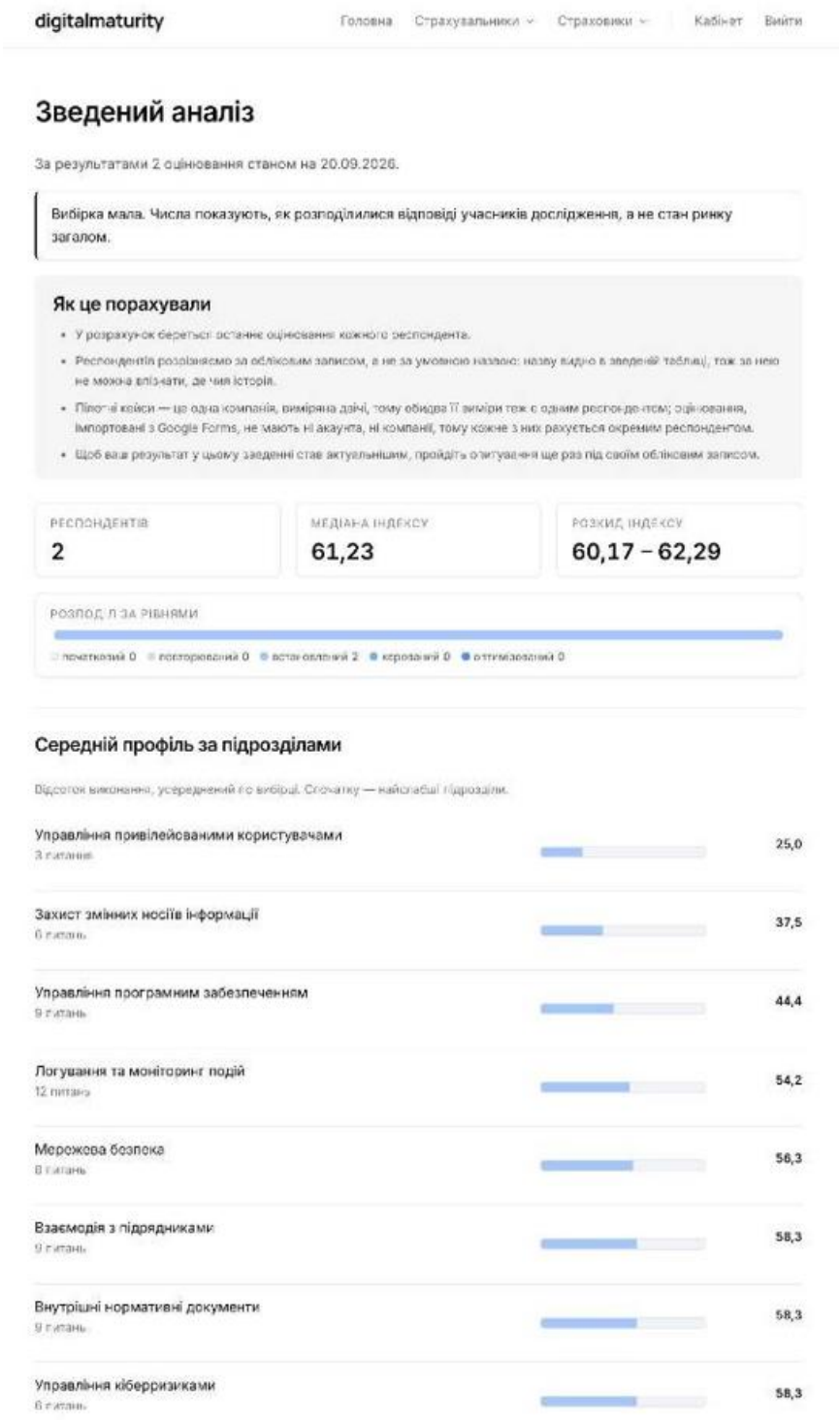


Джерело: розроблено автором.

Функціональні можливості адміністративного модуля щодо формування зведеного аналізу продемонстровано на тестовому наборі записів, який не

належить до масиву десяти анкет, використаного для одержання наведених у цьому розділі емпіричних результатів (рисунок 5.3).

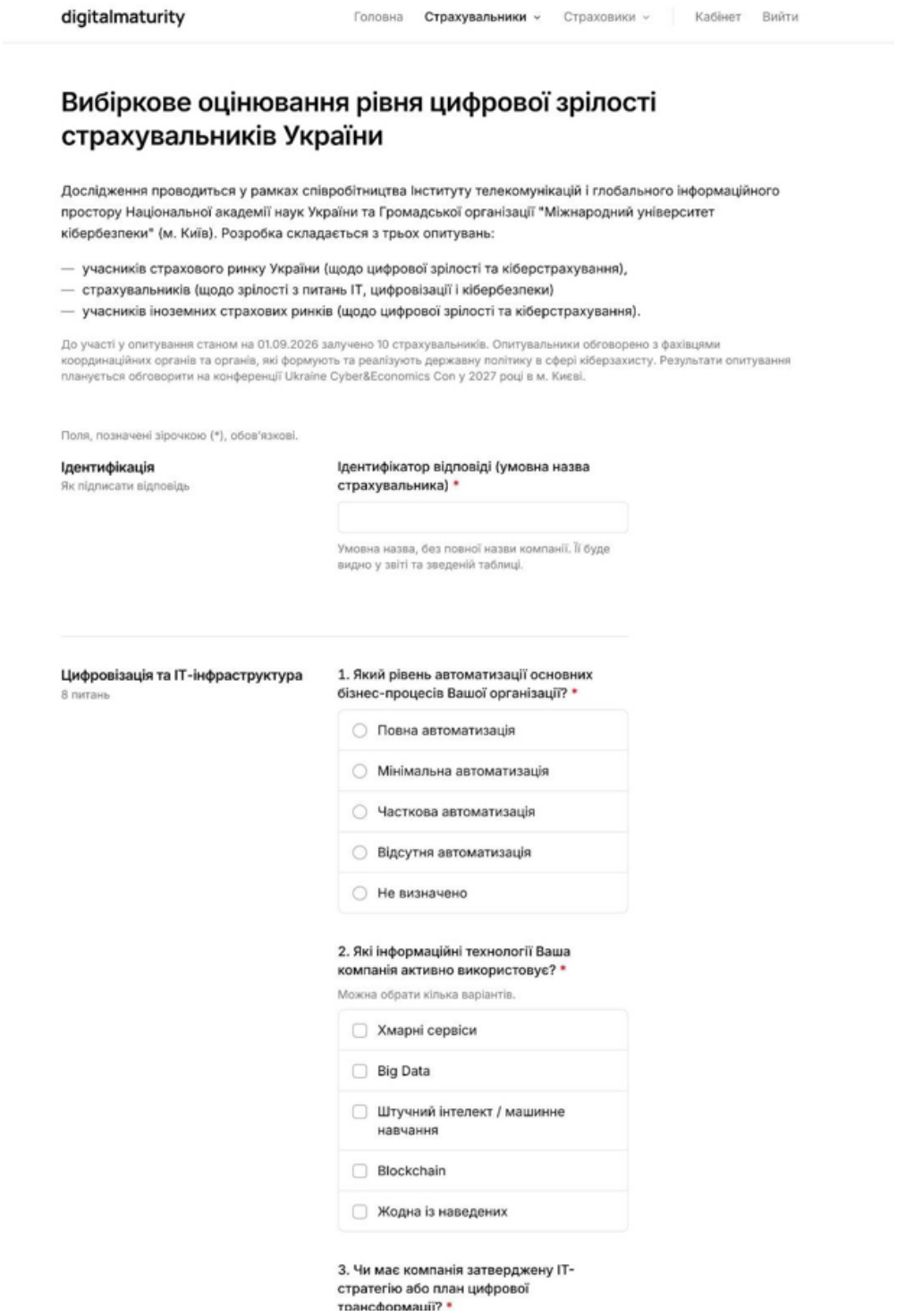
Рисунок 5.3 — Приклад зведеного аналізу тестових записів у дослідному вебзастосунку



Джерело: розроблено автором.

Збирання первинних даних страхувальників реалізовано за допомогою структурованої електронної форми самооцінювання, фрагмент якої наведено на рисунку 5.4.

Рисунок 5.4 — Електронна форма самооцінювання страхувальника в дослідному вебзастосунку



Джерело: розроблено автором.

Розроблений дослідний вебзастосунок реалізує основні операції запропонованої методики: реєстрацію користувачів, збирання і зберігання відповідей, їх перевірку, чисельне кодування, обчислення узагальнених і доменних показників, визначення рівня зрілості, формування рекомендацій та порівняння результатів послідовних циклів оцінювання. Адміністративний модуль забезпечує перегляд індивідуальних і зведених результатів та вивантаження даних для подальшого аналізу. Вебзастосунок є дослідною програмною реалізацією окремих процедур, викладених у підрозділах 4.3–4.5, і не розглядається як завершена програмна система або засіб автоматичного прийняття страхових та актуарних рішень.

Запропонована автоматизація призначена для інформаційної підтримки процесів оцінювання і не замінює професійного рішення уповноваженого фахівця. Розраховані показники, профілі ризиків і зрілості, виявлені критичні прогалини та сформовані рекомендації можуть використовуватися як структурована інформаційна основа для подальшого комплексного оцінювання суб’єкта страхування. Остаточне рішення щодо умов страхування має прийматися з урахуванням результатів зовнішньої й експертної перевірки, технічного дослідження інформаційно-комунікаційної системи, документальних підтверджень, актуарних розрахунків та інших даних, передбачених процедурами страховика.

5.4. Висновки та рекомендації щодо практичного використання результатів оцінювання

Практична цінність апробованого підходу полягає у формуванні узгодженої логіки інформаційної взаємодії страхувальника, страховика, експерта та аудитора. Страхувальник отримує структурований профіль виявлених прогалин і

перелік рекомендованих заходів; страховик — стандартизовані дані для попереднього оцінювання ризику та визначення необхідного обсягу подальшої перевірки; експерт або аудитор — перелік відомостей і підтверджувальних матеріалів, які потребують перевірки. Повторне оцінювання дає змогу відстежувати зміну показників у часі, а за наявності документальних і технічних підтверджень — перевіряти фактичне виконання задекларованих заходів.

Таблиця 5.14 — Напрями практичного використання результатів пілотного оцінювання

Суб'єкт	**Практичне завдання**	**Використовуваний результат**	**Обмеження**
Страхувальник	Самооцінювання і підготовка до кіберстрахування	Доменний профіль, критичні прогалини, перелік рекомендованих заходів	Потрібні відповідальні особи, строки виконання та підтверджувальні матеріали
Андеррайтер	Попередня сегментація та визначення обсягу подальшої перевірки	CDMI, CDMI-UW, критичні прогалини, пояснення відповідей	Результат не є автоматичною відмовою у страхуванні або підставою для визначення тарифу
Страховик	Моніторинг профілів та підготовка до поновлення договору	Порівняння результатів первинного і повторного оцінювання, зміна доменних показників	Потрібні стандартизовані дані та забезпечення їх конфіденційності
Експерт/аудитор	Перевірка достовірності результатів самооцінювання	Перелік непідтверджених відомостей і необхідних підтверджувальних матеріалів	Результат залежить від повноти документальної та технічної перевірки
Керівництво	Визначення пріоритетності заходів із підвищення кіберстійкості	Розриви між поточними і цільовими значеннями показників	Фінансовий ефект потребує окремого обґрунтування

Джерело: запропоновано автором за результатами пілотного оцінювання.

Для страхувальників першочерговими є заходи, пов'язані з усуненням критичних прогалин: організація резервного копіювання та перевірки можливості відновлення даних, захист каналів комунікації, затвердження і тестування плану

реагування на кіберінциденти. Наступним кроком має бути усунення розриву між рівнем технологічного забезпечення та зрілістю управлінських процесів, зокрема формалізація ролей і відповідальності, порядку перегляду прав доступу, ведення реєстру інформаційних активів, навчання персоналу, класифікації даних і контролю виконання встановлених вимог.

Страховим компаніям рекомендовано застосовувати структурований опитувальник як перший рівень багатоступеневого оцінювання. Після автоматизованої перевірки відповіді за показниками з високим рівнем впливу мають підтверджуватися документами або результатами технічного дослідження. Виявлення критичної прогалини повинно ініціювати додатковий запит інформації, зовнішню чи експертну перевірку або визначення попередніх умов подальшого оцінювання, але не автоматичне остаточне рішення. Під час повторних циклів необхідно зберігати первинну відповідь, дату і зміст її зміни, підтверджувальні матеріали та відомості про особу, яка погодила зміну статусу.

Як приклад практичного застосування розглянуто анонімізований профіль страхувальника R05 із сектору охорони здоров'я. Його доменні значення становили: D1 — 60,71 бала; D2 — 52,78 бала; D3 — 39,29 бала, а значення CDMI — 51,11 бала. За прийнятою шкалою профіль відповідав встановленому рівню, однак містив критичну прогалину за показником Q17, що характеризував наявність плану реагування на кіберінциденти. Отже, агреговане значення не є достатньою підставою для безумовного прийняття ризику на страхування. Профіль може бути віднесений до категорії умовної прийнятності для подальшого оцінювання після усунення критичної прогалини та перевірки відповідних підтверджувальних матеріалів.

Для профілю R05 доцільно визначити такі попередні умови подальшого оцінювання: затвердити і протестувати план реагування на кіберінциденти; установити цільові строки відновлення; документувати порядок повідомлення про кіберінцидент; актуалізувати політику конфіденційності; підтвердити здійснення контролю за сторонніми постачальниками; надати матеріали, що

підтверджують резервне копіювання і тестове відновлення даних. Після виконання рекомендованих заходів проводиться повторне оцінювання, а зміна кожної відповіді має підтверджуватися документальними матеріалами або результатами технічного дослідження.

Ілюстративний сценарій використання результатів для коригування страхової премії. Одним із можливих напрямів практичного використання результатів оцінювання є їх урахування під час коригування базової страхової премії P_0, попередньо визначеної страховиком актуарними методами з урахуванням ліміту страхового покриття, франшизи, галузевої належності, обороту, історії збитків, ризикової експозиції та інших факторів [166–168]. Для демонстрації загального порядку такого використання скориговану страхову премію можна подати у вигляді:

$$P = P_0 \cdot (1 - d),$$

де

де P — скоригована страхова премія;

P_0 — базова страхова премія, визначена актуарними методами;

d — сценарний коефіцієнт коригування, додатне значення якого відповідає зниженню, а від'ємне — підвищенню базової страхової премії.

Наведене співвідношення використовується лише для ілюстрації можливого алгоритму врахування результатів оцінювання та не є розробленою або апробованою в дисертації актуарною моделлю. Питання Q28 характеризувало категорію загальних витрат на страхування, а не фактичну страхову премію за кіберстрахування. Тому одержане значення рангової кореляції $\rho = 0{,}692$ не дає підстав для статистичного визначення коефіцієнта d. Наведений сценарій є ілюстративним прикладом можливого використання результатів оцінювання. Діапазони коригування не є актуарно обґрунтованою тарифною шкалою, не використовувалися для встановлення страхових премій і потребують подальшого емпіричного та актуарного калібрування.

Таблиця 5.15 — Ілюстративний сценарій коригування базової страхової премії

CDMI, балів	Характеристика профілю	Сценарне коригування	Додаткова умова
90–100	Верхня частина оптимізованого рівня	Зниження на 20–25 %	Повна документальна, експертна і технічна перевірка
80–89,99	Верхня межа керованого та нижня частина оптимізованого рівня	Зниження на 15–20 %	Відсутність критичних прогалин
70–79,99	Верхня частина керованого рівня	Зниження на 10–15 %	Підтвердження ключових заходів кіберзахисту
60–69,99	Верхня межа встановленого та нижня частина керованого рівня	Зниження на 5–10 %	Усунення критичних прогалин і перевірка підтверджувальних матеріалів
50–59,99	Верхня частина встановленого рівня	Зниження на 0–5 %	Усунення критичних прогалин і перевірка підтверджувальних матеріалів
40–49,99	Верхня межа повторюваного та нижня частина встановленого рівня	Без коригування	Стандартні або спеціальні умови страхування
30–39,99	Верхня частина повторюваного рівня	Підвищення на 10–25 % або спеціальні умови	Розширена перевірка та перелік рекомендованих заходів
0–29,99	Початковий рівень або нижня частина повторюваного рівня	Коригування не визначається	Подальше оцінювання після впровадження мінімально необхідних заходів

Примітка. Наведені діапазони коригування є ілюстративними сценарними значеннями, сформованими для демонстрації можливого алгоритму використання результатів оцінювання. Вони не є актуарно обґрунтованими тарифними коефіцієнтами, не можуть використовуватися для визначення страхової премії без емпіричного калібрування та не підтверджені результатами проведеної пілотної апробації.
Джерело: запропоновано автором як ілюстративний сценарій.

Для профілю страхувальника R05 значення CDMI 51,11 бала відповідало б сценарному інтервалу зниження базової страхової премії від 0 до 5 %. Водночас наявність критичної прогалини за показником Q17 у межах запропонованого сценарію унеможливлює застосування такого коригування до моменту документованого усунення прогалини та перевірки відповідних підтверджувальних матеріалів. Цей приклад демонструє можливий алгоритм використання результатів оцінювання та підтверджує, що агреговане значення не повинно компенсувати відсутність критичного заходу кіберзахисту. Наведене сценарне коригування не є розрахованою страховою премією або актуарно обґрунтованою тарифною рекомендацією.

Подальша валідація та практичне впровадження запропонованого підходу передбачають три послідовні етапи. На першому етапі необхідно провести змістову валідацію питань, шкал, вагових коефіцієнтів і критичних умов із залученням фахівців у сферах кібербезпеки, страхування та актуарного аналізу. На другому етапі доцільно здійснити розширене контрольоване пілотування за участю страхувальників і страхових компаній, у межах якого відповіді мають супроводжуватися документальними або технічними підтвердженнями та зіставлятися з результатами незалежної перевірки. На третьому етапі необхідно розвинути дослідний вебзастосунок до рівня захищеного програмного модуля, інтегрувати його з інформаційними процесами андеррайтингу та провести статистичне й актуарне калібрування на достатньому масиві даних про договори кіберстрахування, кіберінциденти, страхові випадки та збитки.

Повні інструменти дослідження і деталізовані первинні результати доцільно подати в додатках: змістові питання анкети страхувальників із відповідями, використаними для розрахунку; графічні матеріали за результатами опитування десяти страхувальників; повний опитувальник страхових компаній зі 188 питаннями; результати первинного і повторного самооцінювання страхових компаній. У тексті розділу наведено таблиці, які безпосередньо відображають результати пілотної апробації та забезпечують простежуваність і відтворюваність розрахунків.

Таблиця 5.16 — Основні обмеження пілотної апробації та напрями їх усунення

Обмеження	**Наслідок**	**Необхідна дія**
Мала невипадкова вибірка страхувальників	Неможливість статистичного поширення результатів на генеральну сукупність	Розширення вибірки та її стратифікація за галузевою належністю, розміром і типом організації
Самооцінювальний характер даних страхувальників	Ризик соціально бажаних або неточних відповідей	Перевірка відповідей за документами, результатами інтерв'ю та технічного дослідження

Обмеження	Наслідок	Необхідна дія
Самооцінювальний характер даних страхових компаній	Неможливість ототожнення результатів із незалежно підтвердженим станом	Зовнішня й експертна перевірка, документальне підтвердження та технічне дослідження
Однакові вагові коефіцієнти контрольних позицій анкети страхових компаній	Однаковий внесок показників із різним рівнем критичності	Експертне та емпіричне калібрування вагових коефіцієнтів
Категоріальне кодування відповідей	Часткова втрата контексту та залежність результату від правил кодування	Керування версіями словника кодування, використання уточнювальних питань та аналізу чутливості
Відсутність достатнього масиву даних про кіберінциденти, страхові випадки і збитки	Неможливість обґрунтування прогностичної здатності показників і їх впливу на страхову премію	Накопичення емпіричних даних, статистична перевірка та актуарне калібрування
Відсутність повнофункціональної програмної реалізації	Обмеження масштабованості, керування доступом та інтеграції з інформаційними системами страховика	Розроблення захищеного програмного модуля, тестування та інтеграція з інформаційними процесами андеррайтингу

Джерело: систематизовано автором за результатами пілотної апробації.

З урахуванням наведених обмежень результати цього розділу коректно визначати як пілотну апробацію розроблених методичних та алгоритмічних положень на даних анкетного самооцінювання суб’єктів страхування. Одержані результати демонструють можливість кількісного оброблення структурованих анкетних даних, відтворюваність розрахункових процедур, простежуваність формування і зміни показників та підготовку структурованої інформації для подальшого комплексного оцінювання. Подальше практичне впровадження запропонованого підходу потребує розширеної валідації, розвитку дослідного вебзастосунку до рівня захищеної програмної системи, інтеграції з інформаційними процесами страховика та документального підтвердження результатів використання відповідними організаціями.

Висновки до розділу 5

1. Проведено пілотну апробацію розроблених методичних та алгоритмічних положень на двох масивах даних: десяти анонімізованих анкетах страхувальників і результатах первинного та повторного самооцінювання страхових компаній. Одержані результати використано для перевірки процедур збирання, перевірки, кодування, нормування й агрегування анкетних даних, формування часткових профілів цифрової зрілості та зрілості процесів кіберстрахування, а також аналізу зміни показників у часі.

2. Для оцінювання страхувальників сформовано структуру з 23 показників, об’єднаних у три домени з ваговими коефіцієнтами 0,30; 0,40 та 0,30. Якісні відповіді за п’ятибальною шкалою перетворено на нормовані оцінки в діапазоні від 0 до 100 балів. За результатами оброблення даних середнє значення CDMI становило 41,41 бала, медіана — 31,89 бала, а значення показника перебували в діапазоні від 12,62 до 84,84 бала. CDMI визначено як частковий показник анкетного самооцінювання, який не ототожнюється з інтегральним індексом RA&CIMM.

3. Найвище середнє значення одержано за доменом цифровізації та інформаційно-технологічної інфраструктури — 49,64 бала. Середні значення за доменом кіберзахисту й управління ризиками та доменом конфіденційності, управління даними і відповідності вимогам становили відповідно 37,82 та 37,98 бала. Це свідчить, що в межах досліджуваної вибірки відносно вищий рівень цифровізації не в усіх випадках супроводжувався відповідним рівнем організаційних, процедурних і контрольних механізмів кіберзахисту.

4. Поєднання CDMI з критичними контрольними умовами дало змогу сформувати попередні категорії для подальшого страхового оцінювання. Шість профілів потребували усунення критичних прогалин до проведення подальшого оцінювання, три профілі визначено як умовно прийнятні для подальшого

оцінювання після усунення відповідних прогалин, а один — як прийнятний для подальшого оцінювання з обов'язковою перевіркою підтверджувальних матеріалів. Сформовані категорії мають інформаційний характер і не є рішеннями щодо прийняття ризику на страхування або укладення договору.

5. За результатами контролю якості даних виявлено 16 випадків множинних відповідей у порядкових питаннях, чотири пропущені відповіді, п'ять відповідей «не застосовується» та три невизначені відповіді. Аналіз чутливості показав, що найбільша можлива зміна індивідуального результату залежно від способу кодування множинних відповідей становила 5,40 бала. Це підтвердило необхідність автоматизованої перевірки введених даних, використання версійованого словника кодування та окремого консервативного варіанта розрахунку CDMI-UW. Критичні контрольні умови при цьому перевіряються окремо від розрахунку CDMI-UW.

6. За результатами повторного самооцінювання значення показника СК1 збільшилося з 54,66 до 62,29 бала, а СК2 — з 50,42 до 60,17 бала. Приріст становив відповідно 7,63 та 9,75 бала. За прийнятою шкалою первинні значення показників відповідали встановленому рівню, а повторні — керованому. Одержані результати характеризують зміну часткових профілів анкетного самооцінювання і не підтверджують фактичного підвищення зрілості без зовнішньої й експертної перевірки, документального підтвердження та технічного дослідження інформаційно-комунікаційних систем.

7. Розроблені табличний прототип і дослідний вебзастосунок реалізують основні операції оброблення даних: збирання, зберігання, перевірку, кодування, нормування, групування, зважування й агрегування показників, аналіз чутливості, перевірку критичних контрольних умов, класифікацію результатів та формування рекомендацій. Забезпечено простежуваність переходу від первинної відповіді до доменного й узагальненого профілів, а також порівняння результатів послідовних циклів оцінювання. Табличний прототип і вебзастосунок доцільно

розглядати як дослідні реалізації окремих складових майбутньої інформаційної системи, а не як завершену програмну систему.

8. На прикладі анонімізованого профілю страхувальника R05 продемонстровано порядок переходу від доменних значень і критичних прогалин до формування попередньої категорії подальшого страхового оцінювання, визначення необхідних підтверджувальних матеріалів і проведення повторного оцінювання. Встановлено, що агреговане значення показника не повинно компенсувати відсутність критичного заходу кіберзахисту. Остаточне рішення щодо прийняття ризику на страхування має ґрунтуватися на результатах зовнішньої й експертної перевірки, документального підтвердження, технічного дослідження та актуарного аналізу.

9. Запропоновано ілюстративний сценарій можливого використання результатів оцінювання для коригування базової страхової премії. Наведені діапазони зниження або підвищення премії є сценарними значеннями, не становлять актуарно обґрунтованої тарифної шкали та потребують подальшого емпіричного й актуарного калібрування. Одержане значення рангової кореляції $\rho = 0{,}692$ характеризує зв’язок CDMI з категорією загальних витрат на страхування у межах досліджуваної вибірки і не підтверджує залежності між CDMI та страховою премією за кіберстрахування.

10. Подальший розвиток запропонованого підходу потребує розширення і стратифікації вибірки, змістової та емпіричної валідації питань, шкал, критичних умов і вагових коефіцієнтів, перевірки на достатньому масиві даних про договори кіберстрахування, кіберінциденти, страхові випадки і збитки, а також розвитку дослідного вебзастосунку до рівня захищеної програмної системи. Необхідними є керування доступом, зберігання версій і підтверджувальних матеріалів, журналювання операцій, інтеграція з інформаційними системами страховика та документоване пілотування у практичних процесах кіберстрахування.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне науково-прикладне завдання комп'ютерних наук, що полягає в розробленні комплексу взаємопов'язаних моделей, методів і алгоритмів збирання, представлення, передавання, зберігання, структуризації, формалізації, інтеграції, оброблення й аналізу різнорідних даних та організації доступу до них для підтримки прийняття рішень у процесах оцінювання й індексації операційних ризиків у кіберпросторі з метою їх страхування.

Основні наукові та практичні результати дослідження полягають у такому.

1. Проведено системний аналіз сучасного стану оцінювання ризиків інформаційної безпеки, кіберризиків та операційних ризиків у кіберпросторі. Встановлено, що реалізація кіберзагроз впливає не лише на конфіденційність, цілісність і доступність інформації, а й на виконання операційних процесів організації, безперервність надання послуг, доступність інформаційних ресурсів та виникнення фінансових збитків. Обґрунтовано необхідність розгляду кіберризику в контексті його впливу на операційну діяльність і використання результатів оцінювання кіберризиків у процесах кіберстрахування.

2. Уточнено місце кіберризику в системі операційних ризиків. Операційний кіберризик розглянуто як ризик виникнення негативних наслідків для операційних процесів організації внаслідок реалізації кіберзагроз, порушення функціонування інформаційно-комунікаційних систем або недостатньої результативності організаційних і технічних заходів інформаційної безпеки та кіберзахисту. Визначено взаємозв'язок між операційним ризиком, ризиком інформаційної безпеки та кіберризиком.

3. Встановлено, що оцінювання операційних ризиків у кіберпросторі потребує спільного оброблення кількісних, якісних, категоріальних, експертних і технічних показників. Сформовано систему базових параметрів, що охоплює

індикатори кіберінцидентів, кібератак, кіберзагроз і заходів кіберзахисту. Використання цієї системи забезпечує структуризацію та приведення різнорідних даних до вигляду, придатного для подальшого індексного оцінювання.

4. Удосконалено підхід до структуризації різнорідних показників оцінювання шляхом їх багаторівневого подання у вигляді індикаторів, піддоменів і доменів. Обґрунтовано використання базових індикаторів кібербезпеки для формування початкової множини показників і профілю стану об'єкта оцінювання. Запропонована структуризація забезпечує алгоритмічне оброблення показників та перехід від їх окремих значень до групових і узагальнених результатів оцінювання.

5. Розвинено індексний підхід до оцінювання стану кібербезпеки та операційних ризиків у кіберпросторі. Розроблено метод формування доменних підіндексів та інтегрального індексу, який передбачає нормування різнорідних показників, їх групування за визначеними доменами, зважування та подальше агрегування. Метод забезпечує кількісне подання результатів, порівняння об'єктів оцінювання та аналіз зміни показників за результатами повторного оцінювання.

6. Систематизовано та формалізовано процеси кіберстрахування як об'єкти алгоритмізації й автоматизації. Визначено інформаційні операції зі збирання, представлення, передавання, перевірки, зберігання, класифікації, оброблення, аналізу, агрегування та використання даних. Систематизовано інформаційні технології, що застосовуються або можуть застосовуватися у страхуванні та кіберстрахуванні, і розроблено трикомпонентну п'ятирівневу модель оцінювання рівня їх упровадження у процеси кіберстрахування.

7. Розвинено підхід до оцінювання зрілості процесів кіберстрахування на основі доменної декомпозиції показників і багаторівневого оцінювання. Формування доменних оцінок та їх подальше агрегування забезпечують перехід від окремих технологічних та організаційних характеристик до узагальненого

подання рівня зрілості процесів кіберстрахування та формування індексу зрілості кіберстрахування.

8. Розроблено модель оцінювання ризиків та зрілості процесів кіберстрахування RA&CIMM, яка поєднує оцінювання ризиків інформаційної безпеки, кіберризиків і зрілості процесів кіберстрахування. Структуру моделі сформовано на основі трьох взаємопов'язаних доменів: експертного оцінювання ризиків, мережевого оцінювання ризиків та оцінювання зрілості процесів кіберстрахування. RA&CIMM забезпечує структуроване представлення різнорідних показників, формування профілю ризиків і зрілості процесів кіберстрахування та створює основу для їх комплексного кількісного оцінювання.

9. Розроблено багаторівневу процедуру оцінювання ризиків і зрілості процесів кіберстрахування, яка охоплює самооцінювання, зовнішнє оцінювання, експертну перевірку та повторне оцінювання. Розроблено метод формування доменних підіндексів та інтегрального індексу RA&CIMM із використанням вагових коефіцієнтів. Початкові вагові характеристики складових моделі визначено на основі сформованого експертного профілю. Для подальшого формалізованого уточнення відносної пріоритетності критеріїв і вагових коефіцієнтів передбачено можливість застосування експертних методів, зокрема методу аналізу ієрархій. У межах дисертаційної роботи метод аналізу ієрархій не використовувався для визначення початкових вагових значень RA&CIMM.

10. Сформовано алгоритмічну основу інформаційної технології оцінювання й індексації операційних ризиків у кіберпросторі. Вона охоплює збирання і перевірку вхідних даних, їх формалізоване представлення, кодування, нормування, структуризацію, зважування й агрегування, формування часткових і доменних показників, обчислення інтегрального індексу, визначення профілю ризиків і зрілості процесів кіберстрахування та представлення результатів. Одержана інформація призначена для підтримки прийняття рішень у процесах кіберстрахування і не замінює експертного, технічного або актуарного рішення.

11. Проведено пілотну апробацію розроблених методичних та алгоритмічних положень на даних анкетного самооцінювання десяти страхувальників. Для кількісного оброблення даних сформовано композитний індекс цифрової зрілості CDMI за 23 показниками, об'єднаними у три домени. Середнє значення CDMI становило 41,41 бала, медіана — 31,89 бала, а значення показника перебували в діапазоні від 12,62 до 84,84 бала. Для консервативного варіанта обчислення сформовано показник CDMI-UW, у якому пропущені, невизначені та неоцінювані відповіді кодуються нульовим значенням. Критичні контрольні умови перевіряються окремо та використовуються разом із CDMI-UW під час формування попередньої категорії подальшого страхового оцінювання. CDMI та CDMI-UW є частковими показниками анкетного самооцінювання і не ототожнюються з інтегральним індексом RA&CIMM.

12. За результатами двох циклів самооцінювання страхових компаній встановлено зміну розрахункових показників: для СК1 — з 54,66 до 62,29 бала, тобто на 7,63 бала; для СК2 — з 50,42 до 60,17 бала, тобто на 9,75 бала. В обох випадках за прийнятою шкалою зафіксовано перехід від встановленого до керованого рівня. Одержані результати характеризують зміну часткових профілів анкетного самооцінювання і не підтверджують фактичного підвищення зрілості процесів кіберстрахування без зовнішньої й експертної перевірки, документального підтвердження та технічного дослідження інформаційно-комунікаційних систем.

13. Пілотна апробація продемонструвала можливість кількісного оброблення структурованих анкетних даних, відтворюваність розрахункових процедур, порівняння результатів повторного оцінювання та формування структурованої інформації для подальшого комплексного оцінювання. Окремі процедури реалізовано із застосуванням електронних опитувальників, структурованих розрахункових таблиць і дослідного вебзастосунку, що забезпечує збирання та зберігання відповідей, обчислення доменних і узагальнених показників, формування рекомендацій та порівняння результатів

послідовних циклів оцінювання. Обмежений обсяг вибірки, самооцінювальний характер вихідних даних, рівновагове оцінювання окремих контрольних позицій та відсутність достатнього масиву даних про договори кіберстрахування, кіберінциденти, страхові випадки і збитки зумовлюють необхідність подальшої документальної, експертної, технічної, емпіричної та актуарної перевірки розробленого підходу.

Таким чином, у дисертаційній роботі розроблено комплекс взаємопов'язаних моделей, методів і алгоритмів збирання, представлення, передавання, зберігання, структуризації, формалізації, інтеграції, оброблення й аналізу різнорідних даних та організації доступу до них. Одержані результати забезпечують формування доменних підіндексів та інтегрального індексу, профілю ризиків і зрілості процесів кіберстрахування, а також структурованої інформації для підтримки прийняття рішень у процесах оцінювання й індексації операційних ризиків у кіберпросторі з метою їх страхування.

Наукова новизна одержаних результатів полягає в розробленні та розвитку методологічних основ оцінювання й індексації операційних ризиків у кіберпросторі для інформаційної підтримки прийняття рішень у процесах кіберстрахування. Розроблено модель оцінювання ризиків та зрілості процесів кіберстрахування RA&CIMM і метод формування доменних підіндексів та інтегрального індексу; удосконалено підхід до структуризації різнорідних показників оцінювання на основі їх подання у вигляді ієрархічної системи доменів, піддоменів та індикаторів; набули подальшого розвитку підходи до систематизації, формалізації й автоматизації процесів кіберстрахування та оцінювання рівня їх зрілості.

Практичне значення одержаних результатів полягає в можливості використання розроблених моделей, методів, алгоритмів, системи показників, структурованих опитувальників, доменних профілів та індексних оцінок для оцінювання й індексації операційних ризиків у кіберпросторі, оцінювання кіберризиків і зрілості процесів кіберстрахування, а також формування

структурованої інформації для підтримки прийняття рішень. Практичну перевірку окремих методичних та алгоритмічних положень здійснено шляхом їх реалізації у формі структурованих опитувальників, процедур кодування і контролю якості даних, алгоритмів формування індексних оцінок, структурованих розрахункових таблиць і дослідного вебзастосунку.

Результати дисертаційного дослідження формують методологічну та інформаційну основу для подальшого розвитку та повномасштабної програмної реалізації RA&CIMM. Подальші дослідження доцільно спрямувати на розширення практичної апробації моделі у страхових компаніях і серед потенційних страхувальників, формування репрезентативної бази емпіричних даних, верифікацію шкал і вагових характеристик, розроблення повнофункціональної захищеної інформаційної системи, автоматизоване отримання технічних показників із систем моніторингу та кіберзахисту, розширення мережевого домену, а також дослідження можливостей автоматизованого обміну даними між страховими та кібербезпековими інформаційними системами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

2. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

3. National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) 29. 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29

4. Rangu C. M., Badea L., Scheau M. C., Găbudeanu L., Panait I., Radu V. Cyber insurance risk analysis framework considerations. The Journal of Risk Finance. 2024. Vol. 25, No. 2. P. 224–252. DOI: https://doi.org/10.1108/JRF-10-2023-0245

5. International Association of Insurance Supervisors (IAIS). Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development. 2020. URL: https://www.iais.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf

6. Худинцев М. М., Жилін А. В., Давидюк А. В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / каталог) : монографія. Київ : Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, 2021. 240 с. ISBN 978-966-136-887-2. URL: https://www.researchgate.net/publication/360450188_Svitovi_indeksi_kiberbezpeki_oglad_ta_metodiki_formuvanna_Globalnij_zvit_Katalog

7. Мармоза А. Т. Теорія статистики. 2-ге вид., перероб. і допов. Київ : Центр учбової літератури, 2013. 592 с. URL: https://fpk.in.ua/images/biblioteka/3fmb_finan/Teoriya-statystyky-Marmoza-A.T.pdf

8. The Cyber Resilience Index: Advancing Organizational Cyber Resilience, White Paper, World Economic Forum, July 2022, 29 p. URL: https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf

9. Худинцев М.М., Хоменко О.А. Застосування індексів кібербезпеки для оцінки стану інформаційної безпеки об'єктів критичної інфраструктури в умовах військового часу. Актуальні проблеми управління інформаційною безпекою держави : збірник матеріалів XIV Всеукраїнської науково-практичної конференції. Національна академія Служби безпеки України. Інститут модернізації змісту освіти Міністерства освіти і науки України (м. Київ, 30 березня 2023 року). Київ, 2023. с. 341–344. URL: https://nasbu.edu.ua/uploads/p_57_92088934.pdf

10. Худинцев М.М., Хоменко О.А. Статистичний підхід для обробки даних та формування індексів про кіберінциденти, кібератаки, кіберзагрози та заходи протидії. Кібербезпека енергетики : матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ, 31 травня 2023 року). Київ, 2023. с. 100–104. URL: https://ipme.kiev.ua/wp-content/uploads/2023/06/1-Матеріали-КБЕ-2023.pdf

11. Худинцев М.М., Хоменко О.А. Методологічні засади індексу кіберрезильєнтності критичної інфраструктури. Резильєнтність критичної інфраструктури – 2023 : збірник матеріалів науково-практичної конференції. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ, 21 червня 2023 року). Київ, 2023. с. 52–55. URL: https://ipme.kiev.ua/wp-content/uploads/2023/06/Mat-Critical-Infrastructure-Resilience-–-2023.pdf

12. ISO/IEC 27102:2019. Information security management — Guidelines for cyber-insurance. 1st ed. International Organization for Standardization, 2019. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27102:ed-1:v1:en

13. Худинцев М. М., Хоменко О. А. Автоматизація стандартизованих процесів кіберстрахування. Екологічна безпека та природокористування. 2025. Т. 54, № 2. С. 143–153. DOI: https://doi.org/10.32347/2411-4049.2025.2.143-153

14. Про прийняття національних стандартів, змін, поправок до них та скасування національних стандартів : Наказ ДП «УкрНДНЦ» від 15.06.2023 № 135. ДСТУ ISO/IEC 27102:2023. URL: https://zakon.rada.gov.ua/rada/show/v0135774-23#Text

15. Ellili N., Nobanee H., Alsaiari L., Shanti H., Hillebrand B., Hassanain N., Elfout L. The Applications of Big Data in the Insurance Industry: A Bibliometric and Systematic Review of Relevant Literature. The Journal of Finance and Data Science. 2023. Vol. 9. Article 100102. DOI: https://doi.org/10.1016/j.jfds.2023.100102

16. International Association of Insurance Supervisors (IAIS). Issues Paper on the Use of Big Data Analytics in Insurance. 2020. 41 p. URL: https://www.iais.org/uploads/2022/01/200319-Issues-Paper-on-Use-of-Big-Data-Analytics-in-Insurance-FINAL.pdf

17. European Union Agency for Cybersecurity (ENISA). Cyber Insurance – Models and Methods and the Use of AI. ENISA Research and Innovation Brief. 2024. URL: https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai

18. Farao A., Paparis G., Panda S., Panaousis E. A., Zarras A., Xenakis C. A Cyber Insurance Architecture with Smart Contracts and Self-Sovereign Identity on Top of Blockchain. International Journal of Information Security. 2024. Vol. 23. P. 347–371. DOI: https://doi.org/10.1007/s10207-023-00744-x

19. Худинцев М. М., Хоменко О. А. Інформаційні технології кіберстрахування. Електронне моделювання. 2026. Т. 48, № 1. С. 33–50. DOI: https://doi.org/10.15407/emodel.48.01.033

20. European Union Agency for Cybersecurity (ENISA). Cyber Insurance: Recent Advances, Good Practices and Challenges. 2016. URL:

https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges

21. Рамський А. Ю., Арабаджи К. В. Кіберстрахування в банківському секторі: ідентифікація ризиків та інструменти підтримки безпеки. Науковий вісник Міжнародної асоціації науковців. Серія: економіка, управління, безпека, технології. 2023. Т. 2, № 2. URL: https://man.org.ua/nv/index.php/about/article/view/49/52

22. Ксьонжик І., Жовта Н., Павліна А. Страхування ризиків кібербезпеки діяльності суб'єктів господарювання в сучасному інформаційному просторі. Економіка та суспільство. 2021. № 34. DOI: https://doi.org/10.32782/2524-0072/2021-34-90

23. Howden. Cyber Insurance: A Hard Reset 2.0. 2022. 38 p. URL: https://www.howdengroup.com/sites/corporate.howdenprod.com/files/2022-06/howden-cyber-insurance-a-hard-reset-2.0-single-page-final.pdf

24. Farley J. 2023 U.S. Cyber Market Conditions Outlook Report. Gallagher. 2023. 5 p. URL: https://www.ajg.com/-/media/files/gallagher/us/2023-us-cyber-market-conditions-outlook-report.pdf

25. Hiscox. Hiscox Cyber Readiness Report 2021: Don't let cyber be a game of chance. 2021. URL: https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber%20Readiness%20Report%202021.pdf

26. Lander & Rogers. CyberSight 360: Cyber Insurance Trends Shaping 2025 and Beyond. 2025. URL: https://www.landers.com.au/legal-insights-news/cyber-insurance-trends-shaping-2025-and-beyond

27. Buckman B. 2025 Cyber Insurance Trends Report. Huntress. 2025. URL: https://www.huntress.com/blog/cyber-insurance-trends

28. Adam M., Emura K., Ashworth S., Polizu C., Kolli S. Cyber Insurance Market Outlook 2025: Cycle Management Will Be Key To Sustaining Profits. S&P Global Ratings. 2024. URL:

https://www.spglobal.com/ratings/en/research/articles/241127-cyber-insurance-market-outlook-2025-cycle-management-will-be-key-to-sustaining-profits-13323968

29. Munich Re. Cyber Insurance: Risks and Trends 2026. 25 March 2026. URL: https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2026.html

30. Silverfort. The New Cyber Insurance Requirements: What to Know & How to Comply. 2025. URL: https://www.silverfort.com/wp-content/uploads/2025/02/ebook-cyber-insurance-identity-security.pdf

31. Federation of European Risk Management Associations (FERMA). Demystifying Cyber Insurance: Today's Trends & Tomorrow's Challenges. 6 October 2025. URL: https://ferma.eu/wp-content/uploads/2025/10/Demystifying-Cyber-Insurance-todays-trends-tomorrows-challenges.pdf

32. Лащик І., Кондрат І., Віблий П., Білець В. Страховий ринок України: сучасний стан та перспективи розвитку. Галицький економічний вісник. 2020. № 5 (66). С. 105–112. URL: https://galicianvisnyk.tntu.edu.ua/pdf/66/894.pdf

33. Марина А. С., Пеценко М. В. Страховий ринок України в умовах війни. Цифрова економіка та економічна безпека. 2023. № 5 (05). С. 44–51. DOI: https://doi.org/10.32782/dees.5-7

34. Корман, І., Семенда, О., & Макушок, О. (2024). Маркетингове дослідження українського ринку страхових послуг. Київський економічний науковий журнал, (4), С. 119-126. DOI: https://doi.org/10.32782/2786-765X/2024-4-17

35. European Business Association. Український ринок кібербезпеки зріс у чотири рази за вісім років. 2024. URL: https://eba.com.ua/ukrayinskyj-rynok-kiberbezpeky-zris-u-chotyry-razy-za-visim-rokiv/

36. Жарікова А. Кількість кібератак на енергетичну інфраструктуру з початку війни зросла на третину – Міненерго. Економічна правда. 21.11.2022. URL: https://www.epravda.com.ua/news/2022/11/21/694084/

37. Худинцев М. М., Хоменко О. А., Клименков О. А. Методологічні основи оцінювання ризиків кіберстрахування. Екологічна безпека та природокористування. 2026. Т. 58, № 2. С. 251–261. DOI: https://doi.org/10.32347/2411-4049.2026.2.251-261

38. Розробка концептуальних засад і науково-методичної бази оцінки стану кібербезпеки та рівня захищеності інформаційних активів та ресурсів суб'єктів забезпечення кібербезпеки України : НДДКР, державний реєстраційний № 0121U112396. ГО «Міжнародний університет кібербезпеки». 2021–2024.

39. U.S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2). Version 2.1. 2022. URL: https://c2m2.doe.gov/C2M2%20Version%202.1%20June%202022.pdf

40. U.S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2) Self-Evaluation Report. Generated by the C2M2 HTML-Based Tool, Version 2.1, 30 August 2026. 167 p. Official C2M2 resources. URL: https://energy.gov/C2M2

41. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» : Указ Президента України від 01.02.2022 № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text

42. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text

43. Jones J., Freund J. Measuring and Managing Information Risk: A FAIR Approach. 2nd ed. Butterworth-Heinemann, 2025. DOI: https://doi.org/10.1016/C2022-0-02439-9

44. Про основні засади забезпечення кібербезпеки України (2017). Верховна Рада України. Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

45. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

46. Потій О., Семенченко А., Дубов Д., Бакалинський О., Мялковський Д. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. Захист інформації. 2021. Т. 23, № 1. С. 47–60. URL: https://jrnl.kai.edu.ua/index.php/ZI/article/view/15434

47. Boyarchuk R., Khudyntsev M., Lebid O., Trofymchuk O. Organizational and Technical Model of National Cybersecurity and Cyber Protection. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS'2021), Kyiv, Ukraine. CEUR Workshop Proceedings. 2021. Vol. 2923. P. 37–46. URL: https://ceur-ws.org/Vol-2923/paper5.pdf

48. Оцінка стійкості енергетичної інфраструктури України : аналітичний звіт / Павленко О., Антоненко А., Ніцович Р., Євтушок С., Суходоля О. Київ : ГО «Діксі Груп», 2022. 72 с. URL: https://dixigroup.org/wp-content/uploads/2022/05/dixi-energy-resilience-str.pdf

49. Кібербезпека енергетики : матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, 27 травня 2022 р. Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2022. 128 с. URL: https://ipme.kiev.ua/wp-content/uploads/2022/05/Матеріали-КБЕ-2022.pdf

50. Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України. Кібербезпека та стійкість об'єктів енергетики в суспільстві та державі в нормальних, критичних та аварійних умовах. ELECTRON Project. 2022. URL: https://electron-project.eu/blog/cybersecurity-and-sustainability-of-energy-sector-facilities-in-society-and-the-state-in-normal-critical-and-emergency-circumstances/

51. Евенсен Д., Совакул Б., Далтон Н., Глебова К. Енергетична безпека, зміна клімату та майбутня відбудова України. Інститут глобального сталого розвитку Бостонського університету. 2022. 20 с. URL:

https://www.bu.edu/igs/files/2022/10/Energy-Security-Climate-Change-and-the-Future-of-Ukraine-Reconstruction_FINAL_translation.pdf

52. Сафаров Ф., Владіміров Є., Бракко С., Харковина О., Дзядек Д. Кібербезпека в енергетичному секторі: які виклики стоять перед об'єктами критичної інфраструктури України? Energy Security Forum: Післявоєнне відновлення енергетичного сектору України, 21–25.11.2022, Київ. 2022. URL: https://old.saee.gov.ua/uk/news/4628

53. Худинцев М. М. Концептуальні положення забезпечення кібербезпеки енергетичної галузі України. Електронне моделювання. 2023. Т. 45, № 1. С. 80–97. URL: https://www.emodel.org.ua/images/em/45-1/45-1-6.pdf

54. Гулак Г. М., Скітер І. С., Гулак Є. Г. Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об’єктів ядерної енергетики. Кібербезпека: освіта, наука, техніка. 2021. № 4 (12). С. 172–186. DOI: https://doi.org/10.28925/2663-4023.2021.12.172186

55. Кібербезпека енергетики : запрошення, програма та матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, 28 травня 2021 р. Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2021. 61 с. URL: https://ipme.kiev.ua/wp-content/uploads/2021/05/KBE-2021m.pdf

56. Organization for Security and Co-operation in Europe (OSCE). Cyber Incident Classification: A Report on Emerging Practices within the OSCE Region. 2022. URL: https://www.osce.org/files/f/documents/6/5/530293.pdf

57. European Telecommunications Standards Institute (ETSI). ETSI GS ISI 001-1 V1.1.2 (2015-06). Information Security Indicators (ISI); Indicators (INC); Part 1: A Full Set of Operational Indicators for Organizations to Use to Benchmark Their Security Posture. 2015. URL: https://www.etsi.org/deliver/etsi_gs/isi/001_099/00101/

58. ISO/IEC 27004:2016. Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation. 2nd ed. International Organization for Standardization, 2016. URL:

https://www.iso.org/standard/64120.html

59. FAIR Institute. Factor Analysis of Information Risk (FAIR) Standard. Version 3.0. 2025. URL: https://www.fairinstitute.org/hubfs/Standards%20Artifacts/Factor%20Analysis%20of%20Information%20Risk%20%28FAIR%29%20Standard%20v3.0%20%28January%202025%29.pdf

60. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. Київ : Мінекономрозвитку України, 2015. URL: https://wiki.nazk.gov.ua/wp-content/uploads/2020/10/UA-dstu-31010.pdf

61. Про затвердження Положення про вимоги до системи управління страховика : Постанова Правління Національного банку України від 27.12.2023 № 194. URL: https://zakon.rada.gov.ua/laws/show/v0194500-23#Text

62. Pratt S., Kiran S. NIST Cyber Risk Scoring (CRS) – Program Overview. National Institute of Standards and Technology, 2021. URL: https://csrc.nist.gov/presentations/2021/nist-cyber-risk-scoring-crs-program-overview

63. Bodeau D., Graubart R., McQuaid R., Woodill J. Jr. Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. MITRE, 2018. URL: https://www.mitre.org/news-insights/publication/cyber-resiliency-metrics-measures-effectiveness-and-scoring

64. Турчинов О. В., Худинцев М. М., Клименков О. А., Хоменко О. А., Палажченко І. Л. Мережева та економічна складова фінансових індексів кібербезпеки. Екологічна безпека та природокористування. 2025. Т. 56, № 4. С. 102–113. DOI: https://doi.org/10.32347/2411-4049.2025.4.102-113

65. Eling M., Ibragimov R., Ning D. Time Dynamics of Cyber Risk. 2023. 64 p. DOI: https://doi.org/10.2139/ssrn.4497621

66. The SGMM Team. Smart Grid Maturity Model, Version 1.2: Model Definition. CMU/SEI-2011-TR-025. Software Engineering Institute, Carnegie Mellon University, 2011. DOI: https://doi.org/10.1184/R1/6583835.v1

67. Худинцев М.М., Палажченко І.Л., Хоменко О.А. Оцінка стану кіберзахисту з використанням базових індикаторів кібербезпеки. Інформаційно-комунікаційні технології для перемоги та відновлення : матеріали XXIV Міжнародної науково-практичної конференції Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України (м. Київ, 11–12 листопада 2025 року). Київ, 2025. с. 61–63. URL: https://itgip.org/wp-content/uploads/2025/11/1_zbirka_2025_dlja-sajtu.pdf

68. Худинцев М.М., Хоменко О.А. Тренди та інформаційні технології кіберстрахування. Кібербезпека енергетики : матеріали науково-практичної конференції. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ, 29 травня 2024 року). Київ, 2024. с. 56–57. URL: https://ipme.kiev.ua/wp-content/uploads/2024/06/Матеріали-КБЕ-2024.pdf

69. Хоменко О. А., Худинцев М. М. Інформаційні технології страхування та кіберстрахування. Безпека енергетики в епоху цифрової трансформації : матеріали VII науково-практичної конференції. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ, 20 листопада 2025 року). Київ, 2025. с. 91–92. URL: https://ipme.kiev.ua/wp-content/uploads/2026/01/Матеріали-конференції-БЕЕЦТ-2025.pdf

70. Voo J., Hemani I., Cassidy D. National Cyber Power Index 2022. Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022. URL: https://www.belfercenter.org/publication/national-cyber-power-index-2022

71. MSCI Inc. MSCI Cybersecurity Index Methodology. 2018. URL: https://www.msci.com/eqb/methodology/meth_docs/MSCI_CyberSecurity_Index_Methodology.pdf

72. Evolve ETFs. Evolve Cyber Security Index Fund (CYBR): Fact Sheet. 2020. URL: https://evolveetfs.com/wp-content/uploads/2020/03/CYBR-FactSheet-February-28-2020.pdf

73. Foxberry Ltd. Cybersecurity & Data Privacy Thematic Index. URL:

https://www.foxberry.com/indices/thematics/cybersecurity_data_privacy_pr

74. INDXX. INDXX Cybersecurity Index. URL: https://www.indxx.com/index/indxx-cybersecurity-index

75. S&P Dow Jones Indices. S&P Kensho Cyber Security Index. URL: https://www.spglobal.com/spdji/en/indices/equity/sp-kensho-cyber-security-index/

76. Nasdaq OMX. NASDAQ Cybersecurity Index (NQCYBRT): Fact Sheet. URL: https://indexes.nasdaqomx.com/docs/FS_NQCYBRT.pdf

77. Nasdaq OMX. NASDAQ Cybersecurity Index (NQCYBR): Methodology. URL: https://indexes.nasdaqomx.com/docs/Methodology_NQCYBR.pdf

78. Solactive AG. Solactive Cybersecurity Index: Fact Sheet (DE000SLA3UE7). URL: https://www.solactive.com/wp-content/uploads/solactiveip/en/Factsheet_DE000SLA3UE7.pdf

79. World Bank Group. GIIF Achievements in ACP Countries: 2010–2015. Global Index Insurance Facility. 2016. 50 p. URL: https://documents1.worldbank.org/curated/en/482761490702615329/pdf/113713-WP-ENGLISH-GIIF-ACP-Report-Eng-Web-PUBLIC.pdf

80. Branzei R., Dimitrov D., Tijs S. Models in Cooperative Game Theory: Crisp, Fuzzy, and Multi-Choice Games. Lecture Notes in Economics and Mathematical Systems. Vol. 556. Berlin, Heidelberg : Springer, 2005. DOI: https://doi.org/10.1007/3-540-28509-1

81. Горда С. Є. Методи ресурсного теоретико-ігрового аналізу процесів регіонального розвитку : автореф. дис. на здобуття наук. ступеня канд. техн. наук. Київ : Інститут телекомунікацій і глобального інформаційного простору НАН України, 2018. URL: https://itgip.org/wp-content/uploads/2019/01/a_regorda-1111.pdf

82. McGregor R., Reaiche C., Boyle S., Corral de Zubielqui G. Cyberspace and Personal Cyber Insurance: A Systematic Review. Journal of Computer Information Systems. 2024. Vol. 64, No. 1. P. 157–171. DOI: https://doi.org/10.1080/08874417.2023.2185551

83. Franke U. The cyber insurance market in Sweden. Computers & Security. 2017. Vol. 68. P. 130–144. DOI: https://doi.org/10.1016/j.cose.2017.04.010

84. Aziz B., Suhardi, Kurnia. A systematic literature review of cyber insurance challenges. 2020 International Conference on Information Technology Systems and Innovation (ICITSI). 2020. P. 357–363. DOI: https://doi.org/10.1109/ICITSI50517.2020.9264966

85. Dambra S., Bilge L., Balzarotti D. SoK: Cyber-Insurance? Technical Challenges and a System Security Roadmap. 2020 IEEE Symposium on Security and Privacy (SP). 2020. P. 1367–1383. DOI: https://doi.org/10.1109/SP40000.2020.00063

86. Adriko R., Nurse J. R. C. Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review. Information & Computer Security. 2024. Vol. 32, No. 5. P. 691–710. DOI: https://doi.org/10.1108/ICS-01-2024-0025

87. Bace B., Dubois E., Tatar U. Resilience against Catastrophic Cyber Incidents: A Multistakeholder Analysis of Cyber Insurance. Electronics. 2024. Vol. 13, No. 14. Article 2768. DOI: https://doi.org/10.3390/electronics13142768

88. 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. Mapping cyber insurance: a taxonomical study using bibliometric visualization and systematic analysis. Global Knowledge, Memory and Communication. 2023. Vol. 74, No. 3/4. P. 1111–1138. DOI: https://doi.org/10.1108/GKMC-03-2023-0082

89. European Insurance and Occupational Pensions Authority (EIOPA). Cyber Risk for Insurers – Challenges and Opportunities. 2019. URL: https://www.eiopa.europa.eu/document/download/61701869-eab9-49c7-a9ec-14d0b810f755_en?filename=Cyber%20Risk%20for%20Insurers%20-%20Challenges%20and%20Opportunities.pdf

90. Organisation for Economic Co-operation and Development (OECD). Enhancing the Role of Insurance in Cyber Risk Management. OECD Publishing, Paris. 2017. DOI: https://doi.org/10.1787/9789264282148-en

91. American International Group, Inc. CyberMatics®. AIG. URL: https://www.aig.com/home/risk-solutions/business/cyber/cybermatics

92. Келлі М., Такер Дж. Future Risk. Allianz Insurance plc. 20 січня 2021 р. URL: https://www.allianz.co.uk/news-and-insight/insight-and-expertise/future-risk.html

93. Воттерс Е. 50 найпопулярніших статистичних даних, цифр і фактів з кібербезпеки. Computing Technology Industry Association (CompTIA). 27 Jan. 2023. URL: https://lecbyo.files.cmp.optimizely.com/download/9db2ff5c9e2711f08d21221c26c50bba

94. Розроблення переліку, методики оброблення для публікації статистичних даних про кіберінциденти/кібератаки : НДДКР, державний реєстраційний № 0123U102272. Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України. 2023.

95. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06.10.2021 № 601. URL: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601

96. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.05.2023 № 463. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami

97. Про затвердження Вимог з кібербезпеки паливно-енергетичного сектору критичної інфраструктури : Наказ Міністерства енергетики України від 15.12.2022 № 417. URL: https://zakon.rada.gov.ua/laws/show/z0249-23#Text

98. Порядок огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури : Наказ Міністерства енергетики України від 16.01.2023. URL: https://mev.gov.ua/sites/default/files/2023-01/%D0%9D%D0%B0%D0%BA%D0%B0%D0%B7%20%D0%9F%D0%BE%D1%80%D1%8F%D0%B4%D0%BE%D0%BA%20%281%29.pdf

99. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Кабінету Міністрів України від 11.11.2020 № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

100. Про схвалення Концепції впровадження "розумних мереж" в Україні до 2035 року : Розпорядження Кабінету Міністрів України від 14.10.2022 № 908-р. URL: https://zakon.rada.gov.ua/laws/show/908-2022-%D1%80#Text

101. Суходоля О. М., Харазішвілі Ю. М., Бобро Д. Г., Сменковський А. Ю., Рябцев Г. Л., Завгородня С. П. Енергетична безпека України: методологія системного аналізу та стратегічного планування : аналітична доповідь. Київ : НІСД, 2020. 178 с. URL: https://niss.gov.ua/sites/default/files/2020-12/sukhodolia_energy_security_sayt-1.pdf

102. Суходоля О. М., Харазішвілі Ю. М., Бобро Д. Г., Рябцев Г. Л., Завгородня С. П. Визначення рівня енергетичної безпеки України : аналітична доповідь / за заг. ред. О. М. Суходолі. Київ : НІСД, 2021. 71 с. URL: https://niss.gov.ua/sites/default/files/2022-06/analytrep_02_2022.pdf

103. Клапків Ю. М. Ринок страхових послуг: концептуальні засади, технічні інновації та перспективи розвитку : монографія. Тернопіль : ТНЕУ, 2020. 568 с. URL: https://www.researchgate.net/publication/340461341_Rinok_strahovih_poslug_konceptualni_zasadi_tehnicni_innovacii_ta_perspektivi_rozvitku

104. Williams C. A., Heins R. M. Risk Management and Insurance. 6th ed. New York : McGraw-Hill, 1989. 836 p. URL:

https://documentacion.fundacionmapfre.org/documentacion/publico/es/bib/11723.do

105. Волосович С. В. Страхування ризиків кредитної сфери : монографія. Київ : КНТЕУ, 2013. 388 с. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=nX9ooDIAAAAJ&citation_for_view=nX9ooDIAAAAJ:08ZZubdj9fEC

106. Marotta A., Martinelli F., Nanni S., Orlando A., Yautsiukhin A. Cyber-insurance survey. Computer Science Review. 2017. Vol. 24. P. 35–61. DOI: https://doi.org/10.1016/j.cosrev.2017.01.001

107. Romanosky S., Ablon L., Kuehn A., Jones T. Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk? Journal of Cybersecurity. 2019. Vol. 5, No. 1. Article tyz002. DOI: https://doi.org/10.1093/cybsec/tyz002

108. Böhme R., Schwartz G. Modeling Cyber-Insurance: Towards a Unifying Framework. Workshop on the Economics of Information Security (WEIS), Cambridge, MA, 2010. URL: https://cyber.harvard.edu/cybersecurity/Modeling_Cyber-Insurance

109. Пікус Р. В., Бабенко Ю. Л. Кіберстрахування: нові можливості для страхового ринку України. Економіка та держава. 2022. № 2. С. 134–140. DOI: https://doi.org/10.32702/2306-6806.2022.2.134

110. Odell L. A., Fauntleroy J. C., Wagner R. R. Cyber Insurance – Managing Cyber Risk. Alexandria, VA : Institute for Defense Analyses, 2015. IDA Non-Standard NS D-5481. URL: https://www.ida.org/assets/2026/06/18091058/D-5481.pdf

111. National Cyber Security Centre (NCSC). Cyber Essentials Resources. 2025. URL: https://www.ncsc.gov.uk/cyberessentials/resources#section_3

112. European Union Agency for Cybersecurity (ENISA). Demand Side of Cyber Insurance in the EU: Market Dynamics and Strategic Considerations. 2023. URL: https://www.enisa.europa.eu/sites/default/files/publications/Demand%20Side%20of%20Cyber%20Insurance%20in%20the%20EU.pdf

113. Волошинський Ю. 6 головних технологічних трендів у страховій галузі на 2024 рік. 2023. URL: https://our-thinking.nashtechglobal.com/insights/new-technology-in-the-insurance-industry

114. Цивільний кодекс України : Закон України від 16 січня 2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

115. Про страхування : Закон України від 18 листопада 2021 р. № 1909-IX. URL: https://zakon.rada.gov.ua/laws/show/1909-20#Text

116. Про фінансові послуги та фінансові компанії : Закон України від 14 грудня 2021 р. № 1953-IX. URL: https://zakon.rada.gov.ua/laws/show/1953-20#Text

117. Про затвердження Положення про авторизацію надавачів фінансових послуг та умови здійснення ними діяльності з надання фінансових послуг : Постанова Правління Національного банку України від 29.12.2023 № 199. URL: https://zakon.rada.gov.ua/laws/show/v0199500-23#Text

118. 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 Національного банку України від 25.12.2023 № 183. URL: https://zakon.rada.gov.ua/laws/show/v0183500-23#Text

119. Про затвердження Положення про встановлення критеріїв, за якими оцінюється ступінь ризику від здійснення діяльності надавачами фінансових послуг, їх суспільна важливість, на підставі яких визначається періодичність проведення планових інспекційних перевірок, та порядку їх застосування : постанова Правління Національного банку України від 8 листопада 2023 р. № 143. URL: https://zakon.rada.gov.ua/laws/show/v0143500-23#Text

120. Про затвердження Положення про характеристики та класифікаційні ознаки класів страхування, ризики у межах класів страхування, переліки ризиків у межах класів страхування, а також особливості здійснення діяльності із страхування та укладання договорів за класами страхування : постанова Правління Національного банку України від 25 грудня 2023 р. № 182. URL: https://zakon.rada.gov.ua/laws/show/v0182500-23#Text

121. Про затвердження Положення про порядок обліку страховиком договорів, пов’язаних зі здійсненням діяльності із страхування, та вимоги до

захисту інформації страховика : постанова Правління Національного банку України від 29 грудня 2023 р. № 204. URL: https://zakon.rada.gov.ua/laws/show/v0204500-23#Text

122. Federal Trade Commission (FTC). Cyber Insurance. 2024. URL: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

123. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. 2019. L 151. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

124. International Association of Insurance Supervisors (IAIS). Issues Paper on Insurance Sector Operational Resilience. May 2023. 28 p. URL: https://www.iais.org/uploads/2023/05/Issues-Paper-on-Insurance-Sector-Operational-Resilience.pdf

125. Cybersecurity and Infrastructure Security Agency (CISA). Best Practices for MITRE ATT&CK® Mapping. 2021. URL: https://www.cisa.gov/sites/default/files/2023-01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf

126. Atzori L., Iera A., Morabito G. The Internet of Things: A Survey. Computer Networks. 2010. Vol. 54, No. 15. P. 2787–2805. DOI: https://doi.org/10.1016/j.comnet.2010.05.010

127. Privacy + Security Academy. Cyber Liability Insurance Buying Guide 2021. 2021. URL: https://www.privacysecurityacademy.com/wp-content/uploads/2024/05/Cyber-Liability-Insurance-Buying-Guide-2021.pdf

128. Prudential Regulation Authority. Cyber Insurance Underwriting Risk : Consultation Paper CP39/16. Bank of England. 2016. URL: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2016/cp3916

129. Professional Risk Underwriting Pty Ltd. ProRisk Cyber & Privacy Liability Insurance Policy v04.21. 2021. URL: https://www.prorisk.com.au/siteassets/documents/policy-wordings/prorisk-cyber-privacy-liability-insurance-policy-v04.21.pdf

130. Royal & Sun Alliance Insurance plc. Cyber Risk Insurance Policy. 2018. URL: https://static.rsagroup.com/rsa/commercial-insurance-products/cyber/cyber-risk-insurance-policy-wording.pdf

131. Woods D., Agrafiotis I., Nurse J. R. C., Creese S. Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms. Journal of Internet Services and Applications. 2017. Vol. 8. Article 8. DOI: https://doi.org/10.1186/s13174-017-0059-y

132. Pal R., Golubchik L., Psounis K., Hui P. Embracing and Controlling Risk Dependency in Cyber-Insurance Policy Underwriting. Journal of Cybersecurity. 2019. Vol. 5, No. 1. Article tyz010. DOI: https://doi.org/10.1093/cybsec/tyz010

133. European Insurance and Occupational Pensions Authority (EIOPA). Methodological Principles of Insurance Stress Testing – Cyber Component. 2023. URL: https://www.eiopa.europa.eu/publications/methodological-principles-insurance-stress-testing-cyber-component_en

134. Bogomolniy O. Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk. SANS Institute, 2017. URL: https://www.sans.org/white-papers/37572

135. Paragioudakis A., Komninos N., Smyrlis M., Spanoudakis G., Kloukinas C. Risk Management for Cyber Insurance: A Survey for Data-Driven Approaches with the Use of AI. International Journal of Information Security. 2026. Vol. 25. Article 112. DOI: https://doi.org/10.1007/s10207-026-01275-5

136. International Organization for Standardization. ISO 31000:2018. Risk management — Guidelines. 2nd ed. Geneva: ISO, 2018. 16 p. URL: https://www.iso.org/standard/65694.html

137. Гудзь О. Є. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. Економіка. Менеджмент. Бізнес. 2019. № 3 (29). С. 4–12. DOI: https://doi.org/10.31673/2415-8089.2019.030412

138. Нагайчук Н. Г., Третяк Н. М., Ткаленко О. О. Страхування в системі управління кіберризиками підприємства в умовах цифрової економіки. Фінансовий простір. 2019. № 1 (33). С. 97–111. DOI: https://doi.org/10.18371/fp.1(33).2019.177102

139. Селіверстова Л. С., Трухан Д. А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. Економіка та держава. 2020. № 1. С. 23–26. DOI: https://doi.org/10.32702/2306-6806.2020.1.23

140. Дубина М. В., Середюк І. О., Білоус Н. В. Роль кіберстрахування в системі ризик-менеджменту банківських установ. Проблеми і перспективи економіки та управління. 2020. № 1 (21). С. 183–196. DOI: https://doi.org/10.25140/2411-5215-2020-1(21)-183-196

141. Kumar S., Loo L., Kocian L. Blockchain Applications in Cyber Liability Insurance. International Journal on Cybernetics & Informatics (IJCI). 2024. Vol. 13, No. 5. P. 119–139. URL: https://ijcionline.com/paper/13/13524ijci08.pdf

142. Vakilinia I., Sengupta S. A Coalitional Cyber-Insurance Framework for a Common Platform. IEEE Transactions on Information Forensics and Security. 2019. Vol. 14, No. 6. P. 1526–1538. DOI: https://doi.org/10.1109/TIFS.2018.2881694

143. Lepoint T., Ciocarlie G. F., Eldefrawy K. BlockCIS — A Blockchain-Based Cyber Insurance System. 2018 IEEE International Conference on Cloud Engineering (IC2E). Orlando, FL, USA: IEEE, 2018. P. 378–384. DOI: https://doi.org/10.1109/IC2E.2018.00072

144. Armstrong D., Steward T., Thakerar S. Cyber Risks and Insurance: The Legal Principles. London: Bloomsbury Professional, 2021. 232 p. ISBN 978-1-5265-1413-4. URL: https://www.bloomsbury.com/uk/cyber-risks-and-insurance-the-legal-principles-9781526514134/

145. Turban E., Outland J., King D., Lee J. K., Liang T.-P., Turban D. C. Electronic Commerce 2018: A Managerial and Social Networks Perspective. 9th ed. Cham: Springer, 2018. 653 p. DOI: https://doi.org/10.1007/978-3-319-58715-8

146. Farkas S., Lopez O., Thomas M. Cyber Claim Analysis Using Generalized Pareto Regression Trees with Applications to Insurance. Insurance: Mathematics and Economics. 2021. Vol. 98. P. 92–105. DOI: https://doi.org/10.1016/j.insmatheco.2021.02.009

147. Eling M., Wirfs J. H. Modelling and Management of Cyber Risk. International Actuarial Association Life Section Colloquium, Oslo, 7–10 June 2015. 2015. URL: https://actuaries.org/app/uploads/2025/07/IAALS-WirfsEling_Papers_Oslo2015.pdf

148. Security Risk Models for Cyber Insurance / eds. D. Rios Insua, C. Baylon, J. Vila. 1st ed. New York : Chapman and Hall/CRC, 2020. 172 p. DOI: https://doi.org/10.1201/9780429329487

149. Awiszus K., Penner I., Svindland G., Voß A., Weber S. Modeling and Pricing Cyber Insurance: Idiosyncratic, Systematic, and Systemic Risks. European Actuarial Journal. 2023. Vol. 13. P. 1–53. DOI: https://doi.org/10.1007/s13385-023-00341-9

150. Munich Re. Global Cyber Risk and Insurance Survey 2024. 2024. URL: https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey.html

151. Fortune Business Insights. Cyber Insurance Market Size, Share & Industry Trends Analysis, By Insurance Type (Standalone and Tailored), By Coverage Type (First-party and Liability Coverage), By Enterprise Size (SMEs and Large Enterprise), By End-user (Healthcare, Retail, BFSI, IT & Telecom, Manufacturing, and Others), and Regional Forecast, 2026–2034. 2026. URL: https://www.fortunebusinessinsights.com/cyber

152. Tsohou A., Diamantopoulou V., Gritzalis S., Lambrinoudakis C. Cyber Insurance: State of the Art, Trends and Future Directions. International Journal of Information Security. 2023. DOI: https://doi.org/10.1007/s10207-023-00660-8

153. International Association of Insurance Supervisors, Financial Stability Institute. Cyber Insurance Unpacked: The Corporate Digital Safety Net. FSI Insights on Policy Implementation. 2026. URL: https://www.iais.org/uploads/2026/06/FSI-IAIS-Insights-Cyber-insurance-unpacked-the-corporate-digital-safety-net.pdf

154. Kagermann H., Wahlster W., Helbig J. Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0: Final Report of the Industrie 4.0 Working Group. Frankfurt/Main: acatech — National Academy of Science and Engineering, 2013. URL: https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/

155. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг : Постанова Правління Національного банку України від 09.12.2025 № 143. URL: https://zakon.rada.gov.ua/laws/show/v0143500-25#Text

156. Про затвердження Інструкції з оцінки 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 Національного банку України від 05.04.2024 № 38. URL: https://zakon.rada.gov.ua/laws/show/v0038500-24/ed20240405#n35

157. Про затвердження Положення про вимоги до системи управління кредитною спілкою : Постанова Правління Національного банку України від 02.02.2024 № 15. URL: https://zakon.rada.gov.ua/laws/show/v0015500-24/ed20240202#n63

158. Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

159. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Кабінету Міністрів України від 29.12.2021 № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

160. Khudyntsev M., Lebid O., Bychenok M., Zhylin A., Davydiuk A. Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. Information and Communication Technologies and Sustainable Development. ICT&SD 2022 / eds. S. Dovgyi, O. Trofymchuk, V. Ustimenko, L. Globa. Lecture Notes in Networks and Systems. Springer, Cham. 2023. Vol. 809. DOI: https://doi.org/10.1007/978-3-031-46880-3_17

161. Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури : Постанова Кабінету Міністрів України від 24.03.2023 № 257. URL: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text

162. Saaty T. L. Theory of the Analytic Hierarchy Process. Part 2.1. System Research and Information Technologies. 2003. No. 1. P. 48–72. URL: https://journal.iasa.kpi.ua/article/view/175311

163. Saaty T. L. A Scaling Method for Priorities in Hierarchical Structures. Journal of Mathematical Psychology. 1977. Vol. 15, No. 3. P. 234–281. DOI: https://doi.org/10.1016/0022-2496(77)90033-5

164. Dalkey N., Helmer O. An Experimental Application of the Delphi Method to the Use of Experts. Management Science. 1963. Vol. 9, No. 3. P. 458–467. DOI: https://doi.org/10.1287/mnsc.9.3.458

165. Худинцев М. М., Хоменко О. А. Оцінки рівня цифрової зрілості страховиків України [Questionnaire]. Google Forms. 2026. URL: https://docs.google.com/forms/d/e/1FAIpQLSeX_nBDb8fBtc73wbouZ-wCBZS5cwUF7Llxk3VKOy62Kjvzgg/viewform

166. Biener C., Eling M., Wirfs J. H. Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance – Issues and Practice. 2015. Vol. 40, No. 1. P. 131–158. DOI: https://doi.org/10.1057/gpp.2014.19

167. American Academy of Actuaries. Cyber Risk Reinsurance Issues. Cyber Risk Toolkit. 2023. URL: https://www.actuary.org/wp-content/uploads/2025/05/6Reinsurance.pdf

168. Tatar U., Keskin O., Bahsi H., Pinto C. A. Quantification of Cyber Risk for Actuaries: An Economic-Functional Approach. Society of Actuaries, 2020. 84 p. URL:https://www.soa.org/globalassets/assets/files/resources/research-report/2020/quantification-cyber-risk.pdf

Додаток А. Методика пілотного розрахунку композитного індексу цифрової зрілості CDMI

Статус: пілотна операціоналізація даних десяти анкет страхувальників; результат не є остаточним страховим або актуарним рішенням

А.1 Логіка оброблення даних

Таблиця А.1 - Послідовність оброблення даних

Етап	Операція	Зміст
1	Збирання	Отримання відповідей на 30 запитань анкети та фіксація часових позначок.
2	Структуризація	Розподілення Q1-Q30 за доменами та функціональними ролями.
3	Кодування	Перетворення якісних відповідей на нормовані оцінки 0, 25, 50, 75 або 100 балів.
4	Контроль якості	Окреме позначення пропусків, множинного вибору, відповідей «не застосовується» та невизначених відповідей.
5	Агрегування	Розрахунок доменних підіндексів D1-D3, CDMI та консервативного індексу CDMI-UW.
6	Підтримка рішення	Визначення рівня зрілості, критичних прогалин і формування рекомендацій щодо подальшого оцінювання.

А.2 Параметри індексу зрілості

Таблиця А.2 - Структура доменів і склад оцінюваних показників

Код	Домен або роль	Вага	Кількість	Питання
D1	Цифровізація та IT-інфраструктура	0,30	7	Q1, Q3-Q8
D2	Кіберзахист і управління ризиками	0,40	9	Q9-Q17
D3	Конфіденційність, дані та відповідність	0,30	7	Q18-Q24
-	Контекстні, контрольні та профільні питання	-	7	Q2, Q25-Q30

Питання Q2 характеризує технологічний контекст; Q25 використовується для контрольного самооцінювання; Q26-Q30 формують профіль респондента. Ці питання не включаються до розрахунку CDMI. Питання Q12, Q13 і Q17 перевіряються як критичні контрольні умови окремо від інтегрального індексу.

А.3 Правила оброблення даних

Таблиця А.3 - Спеціальні правила оброблення відповідей

Умова	Правило
Оцінка відповіді	Якісні відповіді перетворюються на 0, 25, 50, 75 або 100 балів.
Домен	Значення домену визначається як середнє доступних оцінок у відповідному домені.
Індекс	CDMI формується з урахуванням ваг доменів D1, D2 і D3.

Умова	Правило
Множинний вибір	Основний сценарій використовує мінімальний розпізнаний бал; додатково розраховано середній і максимальний сценарії.
Пропуск / N/A	Для дослідницького CDMI не включається до середнього; повнота показується окремо.
Консервативне кодування CDMI-UW	Для консервативного андеррайтингового скринінгу пропуск або неоцінюване значення дорівнює нулю.
Критична контрольна умова	Q12, Q13 або Q17 нижче 50 балів означає критичну прогалину незалежно від середнього значення.
Межа рішення	Індекс підтримує андеррайтинг, але не замінює оцінку експозиції, збитковості, ліміту, франшизи та технічну верифікацію.

А.4 Шкала інтерпретації рівня зрілості

Таблиця А.4 - Інтерпретація значень CDMI

Діапазон, балів	Рівень	Зміст
Від 0 до 20 включно	Початковий (хаотичний)	Процеси відсутні або виконуються несистемно.
Понад 20 до 40 включно	Повторюваний	Окремі практики повторюються, але їх формалізація є неповною.
Понад 40 до 60 включно	Встановлений	Основні процеси формалізовані та документовані.
Понад 60 до 80 включно	Керований	Процеси вимірюються, контролюються та переглядаються.
Понад 80 до 100 включно	Оптимізований	Здійснюється постійне вдосконалення процесів на основі даних.

А.5 Структура опитувальника

Таблиця А.5 - Розподіл запитань за доменами та функціональними ролями

Код і домен	Роль	Показник	Формулювання питання
Q1 D1	Індекс	Автоматизація бізнес-процесів	Який рівень автоматизації основних бізнес-процесів Вашої організації?
Q2 D1	Контекст	Використовувані інформаційні технології	Які інформаційні технології Ваша компанія активно використовує?
Q3 D1	Індекс	IT-стратегія / цифрова трансформація	Чи має компанія затверджену IT-стратегію або план цифрової трансформації?
Q4 D1	Індекс	Оновлення IT-інфраструктури	Як часто оновлюється IT-інфраструктура (сервери, ПЗ, обладнання)?
Q5 D1	Індекс	Безпечне використання хмарних сервісів	Чи використовує компанія хмарні сервіси відповідно до політик безпеки (ISO/IEC 27017:2015)?
Q6 D1	Індекс	Цифрові навички персоналу	Який рівень цифрових навичок персоналу (за самооцінкою)?

Код і домен	Роль	Показник	Формулювання питання
Q7 D1	Індекс	Інтеграція із зовнішніми API	Чи інтегровані Ваші системи з зовнішніми API, у т.ч. державними платформами та реєстрами (Дія, податкова, банки, інше, зазначте за можливістю з якими)?
Q8 D1	Індекс	Автоматизація документообігу	Який рівень автоматизації документообігу?
Q9 D2	Індекс	Політики інформаційної безпеки	Чи впроваджено політику (політики) інформаційної безпеки у вашій організації?
Q10 D2	Індекс	Відповідальність за кібербезпеку	Чи є призначений відповідальний за кібербезпеку (CISO, CDTO, IT-безпека, ІБ, захист інформації - зазначте)?
Q11 D2	Індекс	Аудит / тестування на проникнення	Як часто проводиться аудит або тестування на проникнення (PenTest)?
Q12 D2	Індекс	Політика резервного копіювання	Чи є політика резервного копіювання даних (backup) відповідно до ISO/IEC 27002:2022 або іншого документу (зазначте якого)?
Q13 D2	Індекс	Захист комунікаційних каналів	Як захищено Ваші комунікаційні канали (VPN, шифрування, MFA)?
Q14 D2	Індекс	Навчання з кібергігієни	Чи навчаються співробітники основам кібергігієни (ENISA Cybersecurity Training Framework, 2023 або інше)?
Q15 D2	Індекс	Спроможність до відновлення	Як швидко компанія здатна відновити діяльність після кіберінциденту (якщо була така практика)?
Q16 D2	Індекс	Оцінювання фінансового впливу	Чи оцінюєте Ви фінансовий вплив кіберінцидентів?
Q17 D2	Індекс	План реагування на кіберінциденти	Чи має компанія план реагування на кіберінциденти (Incident Response Plan, ISO/IEC 27035:2023 або інше - зазначте)?
Q18 D3	Індекс	Захист персональних даних	Чи дотримується Ваша компанія Закону України «Про захист персональних даних» №2297-VI?
Q19 D3	Індекс	Політика конфіденційності / GDPR	Чи впроваджено політику конфіденційності відповідно до GDPR (Regulation (EU) 2016/679)?
Q20 D3	Індекс	Оцінювання відповідності стандартам	Чи проводиться оцінка відповідності стандартам кібербезпеки (ISO/IEC 27001, NIST CSF, ENISA, інше - зазначте)?
Q21 D3	Індекс	Актуалізація політик ІБ	Якщо існують, як часто оновлюються політики інформаційної безпеки?

Код і домен	Роль	Показник	Формулювання питання
Q22 D3	Індекс	Перевірка сторонніх IT-провайдерів	Чи залучає Ваша компанія сторонніх провайдерів IT-послуг і чи перевіряє їхню безпеку (вимога ISO/IEC 27036-3:2021)?
Q23 D3	Індекс	Кібервправи / симуляції інцидентів	Чи має компанія досвід участі у кібервправах або симуляціях інцидентів?
Q24 D3	Індекс	Наявність страхового покриття кіберризиків	Чи має компанія страховий поліс щодо кіберризиків?
Q25 D3	Контроль	Загальна самооцінка зрілості	Як би Ви оцінили загальний рівень зрілості Вашої компанії у сфері цифровізації та кіберзахисту (за моделлю ENISA Cyber Maturity, 2022)?
Q26 Профіль	Профіль	Сектор діяльності	До якої сфери (якого сектору) належить Ваша компанія?
Q27 Профіль	Профіль	Кількість працівників	Який розмір компанії за кількістю працівників?
Q28 Профіль	Профіль	Річні витрати на страхування	Яку суму в рік ви витрачаєте на страхування?
Q29 Профіль	Профіль	Тривалість роботи на ринку	Скільки років компанія працює на ринку?
Q30 Профіль	Профіль	Самовизначений розмір компанії	Як ви визначаєте розмір своєї компанії?

А.6 Загальна схема кодування відповідей

Таблиця А.6 - Уніфікована шкала кодування

Рівень	Бал	Якісна інтерпретація
Рівень 1	0	Контроль відсутній, стан невідомий або критично низький.
Рівень 2	25	Захід заплановано або реалізовано мінімально чи фрагментарно.
Рівень 3	50	Контроль упроваджено частково.
Рівень 4	75	Контроль переважно впроваджено, але він потребує вдосконалення.
Рівень 5	100	Контроль повністю й стабільно впроваджено.

Додаток Б. Акти про впровадження результатів дисертаційного дослідження

ГАРДІАН
СТРАХОВА КОМПАНІЯ

Товариство з додатковою відповідальністю «СТРАХОВА КОМПАНІЯ «ГАРДІАН»
01032, м. Київ, вул. Саксаганського, буд. 96 , тел. +38 044 333 37 10,
office@grdn.com.ua, www.grdn.com.ua
ЄДРПОУ 35417298

АКТ
про впровадження результатів дисертаційного дослідження
22 вересня 2026 року

Цей акт складено на підтвердження практичного використання Товариством з додатковою відповідальністю «Страхова компанія «ГАРДІАН»» окремих результатів дисертаційного дослідження Хоменка О. А. на тему «Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)».

Відповідальні фахівці компанії ознайомилися із запропонованим підходом до оцінювання кіберризиків і зрілості процесів кіберстрахування, структурою показників, послідовністю самооцінювання та порядком формування узагальненого профілю.

У межах пілотної апробації проведено первинне та повторне самооцінювання. За результатами кожного циклу сформовано відповідний профіль і рекомендації щодо вдосконалення організаційних, управлінських та інформаційно-технологічних процесів. Порівняння послідовних результатів дало змогу простежити зміни окремих складових профілю та визначити напрями подальшої роботи без розкриття внутрішньої інформації компанії.

Під час вивчення метаріалів, були представлені пропозиції щодо оцінювання рівня цифрової зрілості страхувальника і загальною логікою їх використання в дослідному вебінтерфейсі. Ці матеріали можуть надалі застосовуватися для структурованого отримання й оброблення інформації про відповідні процеси страхувальника, формування узагальненого профілю та підготовки рекомендацій.

Практичне використання запропонованого підходу підтвердило можливість його застосування для структурованого самооцінювання та порівняння результатів послідовних циклів. Матеріали щодо оцінювання страхувальника можуть використовуватися як додаткове інформаційно-аналітичне джерело під час попереднього розгляду кіберризиків і визначення обсягу подальшої перевірки.

Результати оцінювання мають інформаційно-аналітичний і рекомендаційний характер. Вони не є результатами незалежного аудиту кібербезпеки, зовнішньої чи експертної перевірки, технічного дослідження інформаційно-комунікаційних систем або актуарного оцінювання, не замінюють професійного рішення уповноважених осіб страховика та не створюють для сторін фінансових, страхових чи інших юридичних зобов'язань.

Цей акт підтверджує практичне використання окремих результатів дисертаційного дослідження та може бути долучений до матеріалів дисертаційної роботи.

Генеральний директор
ПрАТ «СК «ГАРДІАН» **Тетяна ЩУЧЬЄВА**

EXPRESS
СТРАХУВАННЯ
ДЛЯ ВАШОЇ ВПЕВНЕНОСТІ

УКРАВТО
ГРУП

АКТ
про впровадження результатів дисертаційного дослідження

Результати дисертаційного дослідження Хоменка Олексія Антоновича на тему «Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)» використано у роботі Товариства з додатковою відповідальністю «ЕКСПРЕС СТРАХУВАННЯ» під час пілотної апробації окремих процедур оцінювання зрілості процесів кіберстрахування.

У межах апробації проведено первинне та повторне самооцінювання із застосуванням запропонованої структури показників і правил оброблення анкетних даних. За результатами послідовних циклів сформовано узагальнені профілі та рекомендації щодо подальшого вдосконалення відповідних процесів.

Під час практичного використання опрацьовано такі складові:

– структуру показників оцінювання зрілості процесів кіберстрахування;

– порядок збирання, перевірки, кодування, нормування та агрегування анкетних даних;

– формування профілю оцінювання та його подання за окремими напрямами;

– зіставлення результатів первинного і повторного самооцінювання;

– формування рекомендацій за результатами оцінювання.

Представники компанії також ознайомилися з методичними матеріалами та можливостями дослідного вебінтерфейсу, призначеними для оцінювання рівня цифрової зрілості страхувальників. Запропонований підхід може надалі використовуватися для структурованого збирання й узагальнення відомостей про організаційні, управлінські та інформаційно-технологічні характеристики страхувальника, формування його профілю та визначення напрямів, що потребують додаткового аналізу.

Сформована інформація може розглядатися як допоміжна інформаційно-аналітична основа під час попереднього оцінювання кіберризиків страхувальника та визначення необхідності подальшої документальної, експертної або технічної перевірки. Вона не є самостійною підставою для прийняття ризику на страхування, встановлення умов договору, розрахунку страхової премії, франшизи або ліміту відповідальності.

Одержані результати мають інформаційно-аналітичний і рекомендаційний характер, не замінюють незалежного аудиту, зовнішньої та експертної перевірки, документального підтвердження, технічного дослідження інформаційно-комунікаційних систем, актуарних розрахунків або професійного рішення уповноважених осіб страховика та не створюють для сторін фінансових чи інших юридичних зобов'язань.

Цей акт підтверджує практичне використання окремих результатів дисертаційного дослідження та може бути долучений до матеріалів дисертаційної роботи.

Заступник директора
ТДВ «ЕКСПРЕС СТРАХУВАННЯ» **Шпак О. О.**

М П

«07» вересня 2026 року

04073, м. Київ, Україна
пр. Бандери Степана, 22
0 800 502 300
073 073 88 17
info@express-group.com.ua
www.express-insurance.com.ua

Вих. № 3692
24" 09 2026р.

ARX
A FAIRFAX COMPANY

АКТ
про впровадження результатів дисертаційного дослідження

Результати дисертаційного дослідження Хоменка Олексія Антоновича на тему «Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)» використано у діяльності Приватного акціонерного товариства «Страхова компанія «АРКС» під час апробації окремих процедур оцінювання зрілості процесів кіберстрахування.

У межах апробації представники компанії ознайомилися з методичними матеріалами дослідження, структурою анкети самооцінювання та підходами до узагальнення отриманих відомостей. За результатами опрацювання матеріалів сформовано рекомендації щодо подальшого вдосконалення відповідних процесів.

Окремо розглянуто можливості дослідного вебінтерфейсу для оцінювання рівня цифрової зрілості страхувальників. Запропонований підхід може надалі використовуватися як допоміжний інструмент для структурованого збирання й узагальнення інформації, формування профілю страхувальника та підготовки рекомендацій.

Матеріали оцінювання можуть слугувати додатковою інформаційно-аналітичною основою під час попереднього розгляду кіберризиків та визначення потреби у подальшій документальній, експертній або технічній перевірці.

Одержані результати мають інформаційно-аналітичний і рекомендаційний характер. Вони не замінюють незалежного аудиту, технічного дослідження, актуарних розрахунків або професійного рішення уповноважених осіб страховика, не є самостійною підставою для визначення умов страхування та не створюють для сторін фінансових чи інших юридичних зобов'язань.

Цей акт підтверджує практичну апробацію та використання окремих результатів дисертаційного дослідження і може бути долучений до матеріалів дисертаційної роботи.

«25» серпня 2026 року

ПрАТ «СК «АРКС»
Директор Департаменту
по роботі з клієнтами КРД
Лук'янова Лілія Юріївна

АКТ

про практичне використання результатів дисертаційного дослідження «Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)» Хоменка Олексія Антоновича

Цим актом підтверджується, що ТОВ «СБ МАЛАКУТ» ознайомилося з методичними та практичними результатами дисертаційного дослідження Хоменка Олексія Антоновича, присвяченого інформаційній технології оцінювання кіберризиків і зрілості процесів кіберстрахування.

Представники ТОВ «СБ МАЛАКУТ» пройшли апробаційне оцінювання за анкетою, призначеною для професійних учасників страхового ринку, та ознайомилися з можливостями розробленого дослідного вебзастосунку. За результатами оцінювання сформовано профіль рівня зрілості, визначено напрями подальшого вдосконалення відповідних процесів та надано рекомендації.

Окремі положення запропонованої методики використано ТОВ «СБ МАЛАКУТ» для структурування інформації про кіберризики, попереднього оцінювання готовності клієнтів до кіберстрахування та підготовки рекомендацій щодо підвищення рівня їхньої цифрової зрілості.

Практична цінність результатів дисертаційного дослідження полягає в можливості їх використання страховим брокером під час консультування клієнтів, підготовки матеріалів для взаємодії зі страховиками та формування пропозицій щодо послуги оцінювання кіберризиків і зрілості процесів кіберстрахування.

Результати дисертаційного дослідження використано ТОВ «СБ МАЛАКУТ» під час структурування консультаційних матеріалів для клієнтів, попереднього оцінювання їхньої готовності до кіберстрахування та підготовки матеріалів для взаємодії зі страховиками.

Цей акт підтверджує практичне використання окремих результатів дисертаційного дослідження у діяльності ТОВ «СБ МАЛАКУТ».

Директор ТОВ «СБ МАЛАКУТ»

м.п.

«10» серпня 2026 року

м. Київ

Громадська організація
МІЖНАРОДНИЙ
УНІВЕРСИТЕТ КІБЕРБЕЗПЕКИ

Non-government organization
INTERNATIONAL
CYBERSECURITY UNIVERSITY

03115, м. Київ, вул. Депутатська, 6, оф. 171
тел. +38 044 5371085 / info@icu-ng.org / код ЄДРПОУ 42933925

15.09.2026 р. вих. № 20260915-1

АКТ ВПРОВАДЖЕННЯ
результатів дисертаційного дослідження
ХОМЕНКА Олексія Антоновича
на тему «Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)»

Впроваджено в рамках науково-дослідної роботи «Розробка концептуальних засад і науково-методичної бази оцінювання стану кібербезпеки та рівня захищеності інформаційних активів та ресурсів суб'єктів забезпечення кібербезпеки України» (Реєстраційна картка НДДКР 0121U112396, дата реєстрації: 29-07-2021).

1. Загальні відомості

Цим актом засвідчується, що результати дисертаційного дослідження Хоменка О.А. на тему «Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)», поданого на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», впроваджено в рамках виконання науково-дослідної роботи «Розробка концептуальних засад і науково-методичної бази оцінювання стану кібербезпеки та рівня захищеності інформаційних активів та ресурсів суб'єктів забезпечення кібербезпеки України» (Реєстраційна картка НДДКР 0121U112396, дата реєстрації: 29-07-2021), що виконувалася Громадською організацією «Міжнародний університет кібербезпеки» у 2021–2024 роках.

2. Об'єкт впровадження

Об'єктом впровадження є науково-методичні результати дисертаційного дослідження, зокрема:

- система базисних параметрів для статистичного опису стану кібербезпеки (індикатори кіберінцидентів, кібератак, кіберзагроз та заходи кіберзахисту);
- модель структуризації різнорідних показників оцінки стану кібербезпеки на основі доменної декомпозиції;
- метод формування групових, доменних та інтегральних індексних оцінок;
- підхід до використання базових індикаторів кібербезпеки (індикаторів кібергігієни) для скорочення початкової множини показників;
- модель оцінки ризиків та зрілості кіберстрахування (RA&CIMM);
- інформаційна технологія оцінки та індексації операційних ризиків у кіберпросторі.

3. Форма впровадження

Результати дослідження впроваджено у вигляді:

- науково-методичних рекомендацій щодо оцінювання стану кібербезпеки та рівня захищеності інформаційних активів і ресурсів суб'єктів забезпечення кібербезпеки України;
- структурованих опитувальників для самооцінювання стану кіберзахисту;
- розрахункових модулів для визначення інтегральних індексів кібербезпеки;
- рекомендацій щодо формування профілів захищеності та зрілості;
- пропозицій щодо впровадження індексного підходу в систему моніторингу кібербезпеки.

4. Сфера використання

Результати впроваджено в таких напрямах виконання НДР:

- формування системи показників і індикаторів для оцінювання стану кібербезпеки;
- застосування індексного підходу до оцінювання стану кібербезпеки;
- оцінювання рівня захищеності інформаційних активів і ресурсів;
- розроблення моделей оцінки стану кіберзахисту з використанням базових індикаторів;
- формування профілів захищеності та зрілості суб'єктів забезпечення кібербезпеки;
- підготовки науково-методичної бази для подальших досліджень у сфері кіберстрахування.

5. Практичні результати впровадження

У результаті впровадження отримано такі практичні результати:

1. Сформовано систему базисних параметрів для статистичного опису кіберінцидентів, кібератак, кіберзагроз та заходів кіберзахисту.
2. Розроблено та апробовано модель структуризації різнорідних показників оцінки стану кібербезпеки на основі доменної декомпозиції.
3. Запропоновано метод формування групових, доменних та інтегральних індексних оцінок для агрегування різнорідних показників.
4. Обґрунтовано доцільність використання базових індикаторів кібербезпеки (індикаторів кібергігієни) для скорочення початкової множини показників та спрощення процедур моніторингу.
5. Розроблено рекомендації щодо формування профілів захищеності та зрілості суб'єктів забезпечення кібербезпеки.
6. Підготовлено науково-методичну базу для подальших досліджень у сфері оцінки кіберризиків та кіберстрахування.

6. Науковий та практичний ефект

Впровадження результатів дисертаційного дослідження дозволило:

- підвищити науковий рівень виконання НДР шляхом застосування сучасних методів індексного оцінювання;
- сформувати системний підхід до оцінювання стану кібербезпеки та рівня захищеності інформаційних активів;
- створити науково-методичну основу для розроблення моделей оцінки зрілості кібербезпеки;

- підготувати рекомендації щодо впровадження індексного підходу в систему моніторингу кібербезпеки;
- забезпечити наукову новизну та практичну цінність результатів НДР.

7. Висновок

Результати дисертаційного дослідження Хоменка О.А. на тему «Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)» мають наукову та практичну цінність, пройшли апробацію та впроваджені в рамках виконання науково-дослідної роботи «Розробка концептуальних засад і науково-методичної бази оцінювання стану кібербезпеки та рівня захищеності інформаційних активів та ресурсів суб'єктів забезпечення кібербезпеки України» (Реєстраційна картка НДДКР 0121U112396).

Запропоновані моделі, методи та алгоритми дозволяють підвищити ефективність оцінювання стану кібербезпеки та створити науково-методичну основу для подальших досліджень у сфері кіберстрахування.

Акт складено для пред'явлення в спеціалізовану вчену раду за місцем захисту дисертації.

Голова Правління
ГО «Міжнародний університет кібербезпеки»

/Роман БОЯРЧУК/

Член Правління
ГО «Міжнародний університет кібербезпеки»

/Вячеслав КРАВЧУК/

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«ЕС.ЕС.АЙ. ІНТЕРНЕШНЛ»
Україна, 04073, м. Київ, проспект Степана Бандери, 9

АКТ

про практичне використання результатів дисертаційного дослідження Хоменка Олексія Антоновича

Цим актом підтверджується, що ТОВ «ЕС.ЕС.АЙ.ІНТЕРНЕШНЛ» здійснило практичне тестування дослідного вебзастосунку, створеного за результатами дисертаційного дослідження Хоменка Олексія Анатолійовича на тему «Методологічні основи оцінки та індексації ризиків для страхування операційних ризиків у кіберпросторі (кіберстрахування)».

Під час тестування представником товариства заповнено електронну анкету та внесено відомості про інформаційно-технологічну інфраструктуру, застосовувані заходи кіберзахисту, управління даними й організаційні процедури.

За результатами автоматизованого оброблення введених даних сформовано індивідуальний профіль цифрової зрілості товариства, до якого увійшли узагальнена й доменні оцінки, визначений рівень зрілості та рекомендації щодо подальшого вдосконалення відповідних процесів.

Одержані результати та сформовані вебзастосунком https://digitalmaturity.org.ua/ рекомендації враховано під час планування подальших організаційних і технічних заходів із підвищення рівня цифрової зрілості та кіберстійкості товариства.

Результати оцінювання мають інформаційний і рекомендаційний характер та не є результатами незалежного аудиту, сертифікації або технічного дослідження інформаційно-комунікаційних систем товариства.

Цей акт підтверджує виключно факт практичного тестування дослідного вебзастосунку та ознайомлення товариства з одержаними результатами і рекомендаціями.

Директор
ТОВ «ЕС.ЕС.АЙ.ІНТЕРНЕШНЛ»

Ігор ДАНАТОВ

м. п.

«28» серпня 2025 року