МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Кваліфікаційна наукова
праця на правах рукопису

СИДОРЕНКО СЕРГІЙ ЮРІЙОВИЧ

УДК 004.056.53:004.75 (043.3)

ДИСЕРТАЦІЯ

МЕТОДИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

122 «Комп’ютерні науки»

12 «Інформаційні технології»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.


_____ С.Ю. Сидоренко

Науковий керівник:
Фесенко Андрій Олексійович
кандидат технічних наук, доцент

Київ – 2026

АНОТАЦІЯ

Сидоренко С.Ю. Методи оцінювання ефективності та захищеності інформаційно-комунікаційних систем критичної інфраструктури держави. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки». – Національний університет «Київський авіаційний інститут», м. Київ, 2026.

Дисертаційна робота присвячена дослідженню методів оцінювання ефективності функціонування та захищеності інформаційно-комунікаційних систем (ІКС) критичної інфраструктури (КІ), а саме – методу оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур, методу оцінювання впливу інцидентів на рівень захищеності ІКС та методу підвищення рівня захищеності критичних інформаційних систем (КІС) КІ.

Проведено аналіз сучасних підходів до оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур. Встановлено, що існуючі методи базуються на використанні інструментарію теорії надійності, ризик-аналізу, оптимізації та стохастичного моделювання. Водночас більшість із них враховує взаємозалежності між ОКІ лише частково або в межах окремих моделей, що не забезпечує комплексного урахування динаміки функціонування систем та обмежує можливості обґрунтованого розподілу ресурсів. Аналіз підходів до оцінювання впливу інцидентів на рівень захищеності ІКС показав, що існуючі рішення переважно орієнтовані на оцінювання ризиків, пріоритизацію інцидентів або визначення окремих показників їх впливу. При цьому встановлено

відсутність формалізованого взаємозв’язку між характеристиками інцидентів та параметрами стану системи, а також обмеженість інтегрованого врахування їх впливу на узагальнений рівень захищеності. У ході аналізу підходів до підвищення рівня захищеності КІС встановлено, що сучасні дослідження зосереджені на окремих складових, зокрема оцінюванні ризику, надійності та стійкості систем, часто в рамках концепції 3R. Разом із тим виявлено, що існуючі підходи не забезпечують комплексного врахування взаємозв’язків між зазначеними характеристиками, а також недостатньо орієнтовані на оптимізацію стратегій забезпечення захищеності в умовах обмежених ресурсів. Проведений аналіз дозволив сформулювати завдання дисертаційного дослідження щодо розроблення та вдосконалення відповідних методів оцінювання та підвищення захищеності інформаційно-комунікаційних систем критичної інфраструктури держави.

Удосконалено метод оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур, за рахунок використання графового подання взаємозалежностей об’єктів, марківських і напівмарківських процесів моделювання станів, забезпечує оцінювання ймовірнісних характеристик функціонування системи та обґрунтування розподілу інвестицій у забезпечення безпеки об’єктів критичної інфраструктури. Крім того, сформовано практичні рекомендації щодо раціонального розподілу інвестицій та ресурсів з урахуванням наявних обмежень. Отримані результати експериментального дослідження показали, що значення ймовірності забезпечення заданого рівня ефективності варіюється в межах P_{sat}=0.39–0.78 залежно від структури взаємозв’язків та рівня резервування, при цьому приріст показника становить ΔP=0.16–0.22.

Удосконалено метод оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем критичної інфраструктури, який за рахунок формалізації взаємозв’язку між

характеристиками інцидентів та параметрами стану системи, а також використання вагових коефіцієнтів їх впливу, дозволяє кількісно враховувати вплив інцидентів на інтегральний показник захищеності та оцінювати загальний стан функціонування системи. На основі розробленого методу сформовано методику оцінювання впливу інцидентів, що дозволяє враховувати їх наслідки при прийнятті рішень щодо управління функціонуванням інформаційно-комунікаційних систем. Отримані результати експериментального дослідження показали, що застосування методу дозволяє кількісно оцінювати вплив інцидентів на рівень захищеності ІКС, що підтверджується зміною інтегрального показника від $S(t)=0.17$ у несприятливих умовах до $S(t)=0.441$ в умовах зниження негативного впливу інцидентів на функціонування системи.

Отримав подальшого розвитку метод підвищення рівня захищеності КІС, який завдяки формалізації взаємозв’язків між ризиком, надійністю та стійкістю, використанню інтегрального показника рівня захищеності та врахуванню технічних і організаційних факторів, дає можливість здійснювати комплексне оцінювання стану системи, прогнозування впливу загроз і оптимізацію стратегій підвищення стійкості в умовах обмежених ресурсів. Розроблено програмне забезпечення, яке забезпечує комплексне оцінювання стану інформаційно-комунікаційних систем, прогнозування впливу загроз, а також сформовано практичні рекомендації щодо вибору раціональної сукупності організаційних і технічних заходів функціонування об’єктів критичної інформаційної інфраструктури. Отримані результати експериментального дослідження показали, що застосування методу забезпечує підвищення рівня захищеності КІС транспортного сектору на 17–26%, що підтверджує ефективність методу та обґрунтованість обраних стратегій підвищення захищеності.

На основі запропонованих методик та розробленого спеціалізованого програмного забезпечення проведено експериментальне дослідження та верифіковано розроблені у роботі методи. Результати дисертації впроваджені і використовуються у діяльності ТОВ «AxxonSoft» (акт про впровадження від 13.03.2026) та у НДЛ протидії кіберзагрозам авіаційної галузі КАІ (акт про впровадження від 14.04.2026) для вирішення прикладних завдань забезпечення сталого функціонування інформаційно-комунікаційних систем.

Ключові слова: критична інфраструктура, об’єкт критичної інфраструктури, інформаційно-комунікаційні системи, взаємозалежні критичні інфраструктури, кіберзагрози, кібербезпека, стійкість, кіберстійкість, мережева стійкість, оцінювання ефективності, показники ефективності, ризик, надійність, доступність, інциденти.

ABSTRACT

Sydorenko S.Yu. Methods for assessing the effectiveness and security of information and communication systems of critical infrastructure of the state. – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in the field of knowledge 12 «Information Technologies» in the specialty 122 «Computer Sciences». – National University «Kyiv Aviation Institute», Kyiv, 2026.

The dissertation is devoted to the study of methods for assessing the effectiveness of the functioning and security of information and communication systems (ICS) of critical infrastructure (CI), namely – a method for assessing the effectiveness of the functioning of information security systems of interdependent critical infrastructures, a method for assessing the impact of incidents on the level of security of the ICS and a method for increasing the level of security of the critical information systems (CIS) of CI.

An analysis of current approaches to assessing the effectiveness of functioning of security systems for interdependent critical infrastructures was carried out. It was established that existing methods are based on reliability theory, risk analysis, optimization, and stochastic modeling. At the same time, most of them consider interdependencies between critical infrastructure objects only partially or within separate models, which does not ensure comprehensive consideration of system functioning dynamics and limits the justification of rational resource allocation. The analysis of approaches to assessing the impact of incidents on the security level of ICS showed that existing solutions are mainly focused on risk assessment, incident prioritization, or determination of separate impact indicators. At the same time, the absence of a formalized relationship between incident characteristics and system state parameters, as well as the limited integrated

consideration of their impact on the generalized security level, was identified. The analysis of approaches to improving the security level of critical information systems demonstrated that modern studies focus on separate components, particularly risk, reliability, and system resilience assessment, often within the 3R concept framework. At the same time, it was found that existing approaches do not provide comprehensive consideration of interrelationships among these characteristics and are insufficiently oriented toward optimization of security assurance strategies under resource constraints. The conducted analysis made it possible to formulate the objectives of the dissertation research related to the development and improvement of methods for assessment and enhancement of the security of information and communication systems of state critical infrastructure.

The method for assessing the effectiveness of functioning of security systems of interdependent critical infrastructures has been improved through the use of graph-based representation of object interdependencies and Markov and semi-Markov state modeling processes, which enables the evaluation of probabilistic characteristics of system functioning and substantiation of investment allocation for ensuring the security of critical infrastructure objects. In addition, practical recommendations for rational allocation of investments and resources under existing constraints have been developed. The results of experimental research showed that the probability of ensuring a заданий level of effectiveness varies within $Psat = 0.39\text{-}0.78$ depending on the interconnection structure and the level of redundancy, while the performance increase reaches $\Delta P = 0.16–0.22$.

The method for assessing the impact of incidents on the level of security of information and communication systems of critical infrastructure has been improved, which, due to the formalization of the relationship between the characteristics of incidents and the parameters of the system state, as well as the use of weighting factors of their impact, allows us to quantitatively take into account the impact of incidents on the integral security indicator and assess the

overall state of the system's functioning. Based on the developed method, a methodology for assessing the impact of incidents has been formed, which allows us to take into account their consequences when making decisions on managing the functioning of information and communication systems. The obtained results of the experimental study showed that the application of the method allows quantitatively assessing the impact of incidents on the level of ICS security, which is confirmed by the change in the integral indicator from S(t)=0.17 in adverse conditions to S(t)=0.441 in conditions of reducing the negative impact of incidents on the functioning of the system.

The method of increasing the level of CIS security has been further developed, which, due to the formalization of the relationships between risk, reliability and stability, the use of an integral indicator of the level of security and taking into account technical and organizational factors, makes it possible to carry out a comprehensive assessment of the state of the system, predict the impact of threats and optimize strategies for increasing stability in conditions of limited resources. Software has been developed that provides a comprehensive assessment of the state of information and communication systems, predict the impact of threats, and also practical recommendations have been formed on the choice of a rational set of organizational and technical measures for the functioning of critical information infrastructure facilities. The results of the experimental study have shown that the application of the method provides an increase in the level of CIS security in the transport sector by 17–26%, which confirms the effectiveness of the method and the validity of the selected security improvement strategies.

Based on the proposed methods and the developed specialized software, an experimental study was conducted and the methods developed in the work were verified. The results of the dissertation are implemented and used in the activities of LLC "AxxonSoft" (implementation act dated 03.13.2026) and in the NDL for countering cyber threats to the aviation industry of the KAI (implementation act

dated 04.14.2026) to solve applied tasks of ensuring the sustainable functioning of information and communication systems.

Keywords: critical infrastructure, critical infrastructure facility, information and communication systems, interdependent critical infrastructures, cyber threats, cybersecurity, resilience, cyber resilience, network resilience, performance assessment, performance indicators, risk, reliability, availability, incidents.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Смірнова Т.В., Сидоренко С.Ю. Модель визначення критичності галузевих інформаційно-телекомунікаційних систем. *Проблеми інформатизації та управління.* 2022. Т. 2. № 70. С. 28-37. DOI: https://doi.org/10.18372/2073-4751.70.16844

2. Гнатюк С.О., Сидоренко В.М., Березовий І.Р., Сидоренко С.Ю., Тараненко К.О. Модель оцінювання ефективності функціонування систем інформаційної безпеки взаємозалежних критичних інфраструктур. *Проблеми інформатизації та управління.* 2022. Т. 4.№ 72. С. 17-25. DOI: https://doi.org/10.18372/2073-4751.72.17457

3. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об’єктах критичної інформаційної інфраструктури держави. *Проблеми інформатизації та управління*. 2024. Т. 2. №78. С. 104-114. DOI: https://doi.org/10.18372/2073-4751.78.18967

4. Сидоренко В.М., Сидоренко С.Ю. Метод підвищення рівня захищеності критичних інформаційних систем держави. *Кібербезпека: освіта, наука, техніка.* 2025. Т.2. №30. С. 500-510. DOI: https://doi.org/10.28925/2663-4023.2025.30.988

Статті в іноземних виданнях:

5. Gnatyuk S., Sydorenko V., Polozhentsev A., Sydorenko S. Experimental Study of the Method for Cyber Incidents Management in Aviation Critical Infrastructure. In: Ostroumov, I., Marais, K., Zaliskyi, M. (eds) Advances

in Civil Aviation Systems Development. ACASD 2025. *Lecture Notes in Networks and Systems*, Vol. 1418. P. 74–91, Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-91992-3_6. (*Scopus*) Q4, ISSN 2367-3370.

6. Lutskyi M., Sydorenko V., Polozhentsev A., Apenko N., Sydorenko S. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures. *CEUR Workshop Proceedings.* 2023. Vol. 3421. P. 214-222. URL: https://ceur-ws.org/Vol-3421/short7.pdf (*Scopus*) Q4, ISSN 1613-0073.

Публікації, які додатково відображають наукові результати дисертації:

7. Жигаревич О.К., Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю. Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи». *Кіберзахист особи, суспільства і держави*: наук.-практ. конф., с. Велятино, 24-27 січня 2024 р.: тези доп., Київ: НАУ, 2024. С. 14-15.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВКІ – взаємозалежні критичні інфраструктури;

ІБ – інформаційна безпека;

ІКС – інформаційно-комунікаційні системи;

ІС – інформаційна система;

ІТ – інформаційні технології;

КІ – критична інфраструктура;

КІІ – критична інформаційна інфраструктура;

КІС – критичні інформаційні системи;

ОКІ – об’єкт критичної інфраструктури;

ОКІІ – об’єкт критичної інформаційної інфраструктури;

ПЗ – програмне забезпечення.

ВСТУП

Актуальність. В умовах цифрової трансформації та стрімкого розвитку інформаційних технологій забезпечення захисту інформаційно-комунікаційних систем стає однією з ключових складових національної безпеки держави. Особливого значення набуває проблема забезпечення стійкого функціонування критичної інфраструктури, оскільки від її надійності залежить стабільність економіки, безпека населення та безперервність надання життєво важливих послуг.

Критична інфраструктура включає енергетичні, транспортні, фінансові, промислові та інші системи, функціонування яких забезпечується інформаційно-комунікаційними системами. Взаємозв’язки між об’єктами критичної інфраструктури формують взаємозалежні критичні інфраструктури, що обумовлює можливість виникнення каскадних ефектів у разі порушення функціонування окремих елементів. У таких умовах зростає складність оцінювання стану систем та прийняття обґрунтованих рішень щодо забезпечення їх захищеності.

Аналіз сучасних наукових досліджень показав, що існуючі підходи до оцінювання ефективності функціонування систем безпеки базуються на використанні інструментарію теорії надійності, ризик-аналізу, стохастичного моделювання та оптимізації, однак не забезпечують комплексного врахування взаємозалежностей між об’єктами та динаміки зміни їх станів. Водночас підходи до оцінювання впливу інцидентів переважно орієнтовані на оцінювання ризиків або їх пріоритизацію і не встановлюють формалізованого взаємозв’язку між характеристиками інцидентів та станом системи. Крім того, сучасні підходи до підвищення рівня захищеності зосереджені на окремих складових, зокрема ризику, надійності та стійкості, і не забезпечують їх комплексного поєднання та оптимізації стратегій захисту в умовах обмежених ресурсів.

Питаннями оцінювання ефективності та захищеності інформаційно-комунікаційних систем критичної інфраструктури займаються такі вітчизняні та закордонні вчені: Качинський А., Кириленко С. П., Мохор В., Мурасов Р., Суходоля О., Третьяков О., Шевченко Н., Jablanski D., Kong J., Limnios N., Mahmood Y., Mohd Safari M., Nozick L., Papastergiou S. та інші. Незважаючи на значну кількість досліджень, більшість із них спрямовані на розв'язання окремих аспектів забезпечення безпеки та не враховують комплексного впливу взаємозалежностей і інцидентів на ефективність функціонування систем.

Таким чином, *актуальною науково-технічною задачею* є розроблення методів оцінювання ефективності функціонування та рівня захищеності інформаційно-комунікаційних систем взаємозалежних критичних інфраструктур, які забезпечують комплексне врахування взаємозалежностей між об'єктами, стохастичного характеру їх функціонування та впливу інцидентів, а також дозволяють обґрунтовувати раціональний розподіл ресурсів і підвищення ефективності функціонування систем.

Тема дисертації відповідає освітньо-науковій програмі «Комп'ютерні науки» за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» в Національному університеті «Київський авіаційний інститут».

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота безпосередньо пов'язана з пріоритетними тематичними напрямами наукових досліджень і науково-технічних розробок, визначеними постановою Кабінету Міністрів України від 30 квітня 2024 р. № 476, та відповідає напряму розвитку інформаційно-комунікаційних технологій у частині розроблення методів оцінювання ефективності та захищеності інформаційно-комунікаційних систем. Тематика дослідження узгоджується зі Стратегією цифрового розвитку інноваційної діяльності України до 2030 року в частині розвитку інформаційно-аналітичних технологій та підтримки прийняття рішень щодо забезпечення функціонування інформаційно-

комунікаційних систем. Теоретичні та практичні положення дисертаційної роботи використано під час виконання науково-дослідної роботи у Державному університеті «Київський авіаційний інститут», а саме НДР «Методи, моделі та програмні засоби управління інцидентами кібербезпеки в критичній інфраструктурі держави» (д.р. № 0125U000624, 2025–2026 рр.).

Мета і задачі дослідження. Метою дисертаційної роботи є розроблення методів оцінювання ефективності та захищеності інформаційно-комунікаційних систем критичної інфраструктури держави для підтримки прийняття обґрунтованих рішень щодо забезпечення їх сталого функціонування в умовах обмеженості ресурсів.

Для досягнення поставленої мети необхідно розв’язати такі **основні задачі:**

1) провести аналіз сучасних підходів до оцінювання ефективності та захищеності інформаційно-комунікаційних систем критичної інфраструктури держави для виявлення їх переваг та недоліків;

2) удосконалити метод оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур для оцінювання ймовірнісних характеристик та обґрунтування розподілу інвестицій;

3) удосконалити метод оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем критичної інфраструктури для кількісного врахування їх впливу на інтегральний показник захищеності та стан функціонування системи;

4) удосконалити метод підвищення рівня захищеності критичних інформаційних систем критичної інфраструктури для комплексного оцінювання їх стану та забезпечення стійкості в умовах обмеженості ресурсів;

5) провести верифікацію розроблених методів із використанням програмного забезпечення для підтвердження їх ефективності та придатності до практичного застосування.

Об’єктом дослідження є процеси оцінювання ефективності та захищеності ІКС критичної інфраструктури держави.

Предметом дослідження є методи та програмні засоби оцінювання ефективності та захищеності ІКС критичної інфраструктури в умовах реалізації загроз та обмежених ресурсів захисту.

Методи дослідження. Проведені дослідження базуються на сучасних методах: *теорії ймовірностей і математичної статистики* – для оцінювання ймовірнісних характеристик функціонування інформаційно-комунікаційних систем; *теорії марковських і напівмарковських процесів* – для моделювання станів систем та аналізу їх переходів; *теорії графів* – для подання та дослідження взаємозалежностей об’єктів критичної інфраструктури; *теорії надійності та ризик-аналізу* – для оцінювання рівня захищеності та стійкості систем; *методів системного аналізу* – для формалізації структури та процесів функціонування інформаційно-комунікаційних систем; *методів оптимізації* – для обґрунтування раціонального розподілу ресурсів; а також *методів комп’ютерного моделювання* – для проведення експериментальних досліджень, обробки результатів та верифікації ефективності розроблених методів і програмного забезпечення.

Наукова новизна одержаних результатів полягає у такому:

– *удосконалено* метод оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур, за рахунок використання графового подання взаємозалежностей об’єктів, марківських і напівмарківських процесів моделювання станів, що забезпечує оцінювання ймовірнісних характеристик функціонування системи та обґрунтування

розподілу інвестицій у забезпечення безпеки об’єктів критичної інфраструктури.

– *удосконалено* метод оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем критичної інфраструктури, який за рахунок формалізації взаємозв’язку між характеристиками інцидентів та параметрами стану системи, а також використання вагових коефіцієнтів їх впливу, дозволяє кількісно враховувати вплив інцидентів на інтегральний показник захищеності та оцінювати загальний стан функціонування системи;

– *отримав подальшого розвитку* метод підвищення рівня захищеності критичних інформаційних інфраструктур, який завдяки формалізації взаємозв’язків між ризиком, надійністю та стійкістю, використанню інтегрального показника рівня захищеності та врахуванню технічних і організаційних факторів, дає можливість здійснювати комплексне оцінювання стану системи, прогнозування впливу загроз і оптимізацію стратегій підвищення стійкості в умовах обмежених ресурсів.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати можуть бути використані у сфері інформаційних технологій для оцінювання, прогнозування та забезпечення сталого функціонування інформаційно-комунікаційних систем об’єктів критичної інфраструктури в умовах деструктивних впливів.

Практична цінність роботи полягає у такому:

– сформовано практичні рекомендації щодо раціонального розподілу інвестицій та ресурсів з урахуванням наявних обмежень;

– розроблено методику оцінювання впливу інцидентів, що дозволяє враховувати їх наслідки при прийнятті рішень щодо управління функціонуванням інформаційно-комунікаційних систем;

– розроблено програмне забезпечення, яке забезпечує комплексне оцінювання стану інформаційно-комунікаційних систем, прогнозування впливу загроз, а також сформовано практичні рекомендації щодо вибору раціональної сукупності організаційних і технічних заходів функціонування об’єктів критичної інформаційної інфраструктури.

– результати дисертації впроваджені і використовуються у діяльності ТОВ «AxxonSoft» (акт про впровадження від 13.03.2026) та у НДЛ протидії кіберзагрозам авіаційної галузі КАІ (акт про впровадження від 14.04.2026) для вирішення прикладних завдань забезпечення сталого функціонування інформаційно-комунікаційних систем.

Особистий внесок здобувача. Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [2, 6] – розроблення методу оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур; [3] – проведено верифікацію розробленого методу оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем критичної інфраструктури; [4] – теоретичне обґрунтування та розроблення методу підвищення рівня захищеності КІС; [1, 4-7] – аналіз підходів до оцінювання ефективності та захищеності інформаційно-комунікаційних систем критичної інфраструктури держави.

З робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація результатів дисертації. Результати досліджень дисертаційної роботи доповідалися та обговорювалися на таких наукових конференціях: міжнародній науково-практичній конференції «Advances in Civil Aviation Systems Development» (ACASD-2025) (США, м. Київ, Україна, 18–20 березня 2025 р.); міжнародній науково-практичній конференції

«Cybersecurity Providing in Information and Telecommunication Systems» (CPITS-2024) (м. Київ, Україна, 28 лютого 2024 р.); всеукраїнській науково-практичній конференції «Кіберзахист особи, суспільства і держави» (с. Велятино, Україна, 24-27 січня 2024 р.); та інших.

Публікації. Основні положення дисертації опубліковано у 7 наукових працях, у тому числі: 6 наукових статтях, серед них 2 – у закордонних рецензованих виданнях, які входять до наукометричної бази даних Scopus, 4 – у вітчизняних фахових наукових журналах, а також у 1 матеріалах теза доповідей на конференціях.

Структура роботи та її обсяг. Дисертація складається з анотації, вступу, чотирьох розділів, висновків, додатків, списку використаних джерел і має 118 сторінок основного тексту, 31 рисунки, 36 таблиць, 37 сторінок додатків. Список використаних джерел містить 97 найменування і займає 12 сторінок. Загальний обсяг роботи 188 сторінок.

РОЗДІЛ 1
СУЧАСНІ ПІДХОДИ ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

1.1. Аналіз нормативно-правових засад забезпечення захисту інформаційно-комунікаційних систем критичної інфраструктури

Сучасні інформаційно-комунікаційні системи (ІКС) критичної інфраструктури (КІ) функціонують в умовах зростання кількості деструктивних інформаційно-технічних впливів, ускладнення архітектури цифрових сервісів, посилення взаємозалежностей між секторами та підвищення ролі кіберфізичних систем. За таких умов захист ІКС перестає бути виключно задачею технічного захисту інформації та набуває ознак комплексної міжсекторальної проблеми, що охоплює правові, організаційні, технологічні й управлінські аспекти. Це обумовлює необхідність формування ефективної нормативно-правової бази, здатної регламентувати не лише вимоги до захисту окремих об’єктів, а й забезпечення стійкого функціонування взаємопов’язаних систем у динамічних умовах загроз.

На сучасному етапі нормативно-правове забезпечення захисту ІКС формується на декількох рівнях: законодавчому, підзаконному, галузевому та міжнародному. Така багаторівнева структура регулювання дозволяє поєднувати стратегічні принципи захисту КІ з конкретними технічними й організаційними вимогами щодо забезпечення кіберзахисту, управління ризиками та реагування на інциденти.

Основу нормативно-правового забезпечення в Україні становлять законодавчі акти, які визначають базові принципи функціонування та захисту КІ. Зокрема, Закон України «Про критичну інфраструктуру» [1] формує правові та організаційні засади створення національної системи захисту КІ, визначає повноваження суб’єктів забезпечення безпеки, підходи до ідентифікації об’єктів

критичної інфраструктури (ОКІ) та загальні вимоги до їх стійкості. Важливим положенням цього закону є закріплення ризик-орієнтованого підходу до захисту об’єктів та акцент на безперервності їх функціонування.

Закон України «Про основні засади забезпечення кібербезпеки України» [2] деталізує підходи до захисту критичної інформаційної інфраструктури (КІІ), визначає суб’єктів національної системи кібербезпеки, регламентує порядок реагування на кіберінциденти та створює правову основу, у межах якої кіберзагрози підлягають моніторингу, аналізу та оцінюванню. Особливе значення цього закону полягає у виокремленні об’єктів критичної інформаційної інфраструктури (ОКІІ) як окремого класу об’єктів захисту.

Подальша деталізація вимог до забезпечення захисту ІКС здійснюється на рівні підзаконних нормативних актів. Постановою Кабінету Міністрів України №1109 [3] визначено порядок віднесення об’єктів до КІ, встановлено секторальний підхід до їх класифікації та перелік життєво важливих послуг, порушення яких може призвести до критичних наслідків.

Постанова Кабінету Міністрів України №518 [4] визначає критерії категоризації об’єктів за рівнем критичності, що є важливим елементом диференціації захисних вимог залежно від потенційного рівня загроз та наслідків порушення функціонування.

Водночас постанова Кабінету Міністрів України №1426 [5] визначає організаційно-технічну модель кіберзахисту, регламентує взаємодію суб’єктів національної системи кібербезпеки, а також встановлює вимоги до побудови систем моніторингу, виявлення та реагування на кіберінциденти. На відміну від базових законодавчих актів, ця постанова більшою мірою орієнтована на практичну реалізацію механізмів захисту ІКС.

Окрему групу нормативного забезпечення становлять спеціалізовані документи у сфері технічного та криптографічного захисту інформації. Методика оцінки стану захищеності ОКІ [6] визначає підходи до оцінювання

стану захищеності, формалізує перелік критеріїв контролю та забезпечує основу для проведення аудиту безпеки.

Наказ Державної служби спеціального зв'язку та захисту інформації України №54 [7] визначає базові заходи кіберзахисту, включаючи контроль доступу, журналювання подій безпеки, резервування, моніторинг, управління вразливостями та реагування на інциденти. Його значення полягає в тому, що він поєднує організаційні та технічні заходи безпеки в єдину систему базових контролів.

Крім зазначених документів, важливими для захисту саме ІКС є нормативні документи системи технічного захисту інформації (НД ТЗІ), а також вимоги щодо побудови комплексних систем захисту інформації (КСЗІ), які традиційно застосовувалися для інформаційно-телекомунікаційних систем, а в сучасних умовах поширюються і на ІКС КІ.

Таким чином, українська нормативна база достатньо повно регламентує базові вимоги до захисту ІКС, однак переважно орієнтована на регуляторне визначення заходів захисту, а не на кількісне оцінювання ефективності їх функціонування.

Поряд із національними нормативними актами важливу роль відіграють міжнародні стандарти та рекомендації. Зокрема, ISO/IEC 27001:2022 [8] визначає вимоги до систем управління інформаційною безпекою, орієнтованих на побудову циклу безперервного вдосконалення захисту. Стандарт фокусується на управлінні контролями безпеки, процесах моніторингу та аудиті ефективності заходів захисту.

Стандарт ISO/IEC 27005 [9] деталізує методологічні підходи до управління ризиками інформаційної безпеки, що особливо важливо для ОКІ, де ризик-орієнтоване управління є основою вибору захисних стратегій.

Cybersecurity Framework Національного інституту стандартів і технологій США (NIST CSF) [10] пропонує структурований підхід до

забезпечення кібербезпеки через функції Identify – Protect – Detect – Respond – Recover (рис. 1.1). Особливістю цього підходу є орієнтація не лише на захист, а й на забезпечення відновлюваності та стійкості функціонування систем.

Рис. 1.1. Основні функції управління захистом ІКС (за [10])

Особливе значення для захисту саме інформаційно-комунікаційних і промислових систем КІ має серія стандартів IEC 62443 [11], яка регламентує кіберзахист industrial control systems, SCADA та distributed control systems. На відміну від загальних стандартів інформаційної безпеки (ІБ), в цих документах враховується мережева стійкість (сегментація), багаторівнева архітектура захисту, контроль промислових протоколів та захист технологічних процесів.

Додатково NIST SP 800-82 (Guide to Industrial Control Systems Security) [12] деталізує вимоги до захисту ICS/SCADA-систем, включаючи управління ризиками, сегментацію мереж, контроль доступу, безпечне адміністрування та реагування на інциденти саме в технологічному середовищі.

Архітектурна багаторівневість ІКС та наявність міжрівневих взаємодій обумовлюють необхідність багаторівневого захисту та сегментації мережевого середовища (рис. 1.2).

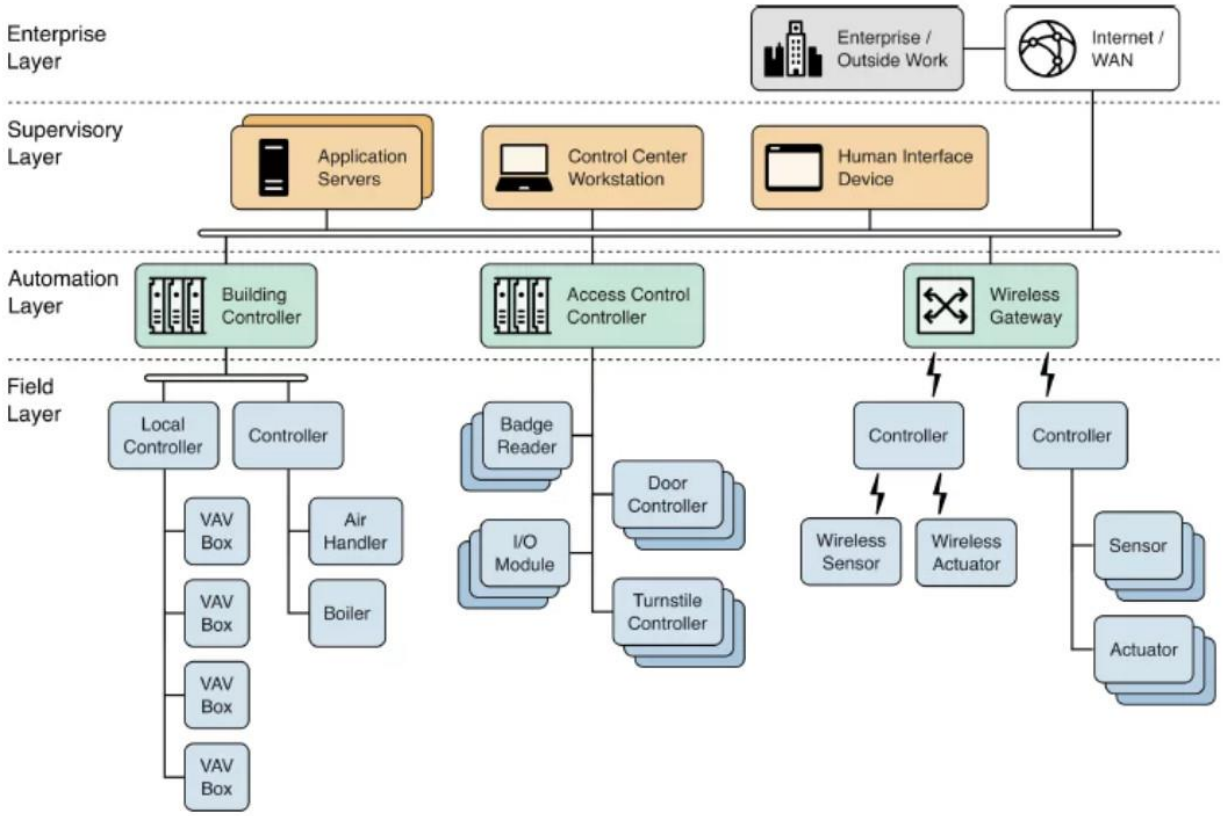

Рис. 1.2. Типова багаторівнева архітектура ICS/SCADA-системи з позицій захисту ІКС (за [19])

Як видно з рис. 1.2, багаторівнева структура ІКС формує множину міжрівневих залежностей, що ускладнює забезпечення їх захисту та потребує врахування каскадних ефектів.

Сучасний розвиток нормативного забезпечення характеризується переходом від моделей захисту до моделей стійкості. Це відображено у Директиві NIS2 [13] та CER Directive [14], які розширюють традиційні вимоги кіберзахисту, інтегруючи управління ризиками, безперервність функціонування, звітування про інциденти та врахування взаємозалежностей між ОКІ.

Практичні рекомендації щодо підвищення рівня захищеності наведені також у документах Cybersecurity and Infrastructure Security Agency [15], які акцентують увагу на управлінні кіберризиками для операторів КІ та побудові стійких архітектур захисту.

Для узагальнення результатів аналізу доцільно систематизувати нормативні документи за основними критеріями (табл. 1.1):

1. CI – урахування вимог щодо захисту ІКС;
2. CR – регламентація управління ризиками;
3. CE – регламентація реагування на інциденти;
4. CD – урахування взаємозалежностей між об’єктами;
5. CQ – наявність положень щодо кількісного оцінювання ефективності.

Таблиця 1.1

Порівняльний аналіз нормативно-правових і стандартних документів щодо захисту ІКС

№	Документ	CI	CR	CE	CD	CQ
1	Закон про КІ	+	+	–	–	–
2	Закон про кібербезпеку	+	+	+	–	–
3	КМУ №1426	+	+	+	–	–
4	НД ТЗІ / КСЗІ	+	+	+	–	–
5	ISO 27001	+	+	±	–	–
6	NIST CSF	+	+	+	–	±
7	IEC 62443	+	+	+	+	±
8	NIST SP 800-82	+	+	+	+	±
9	NIS2	+	+	+	+	±

З табл. 1.1 видно, що більшість нормативних документів орієнтовані на регламентацію базових заходів кіберзахисту, управління ризиками та реагування на інциденти, тоді як урахування взаємозалежностей між об’єктами (CD) та кількісне оцінювання ефективності функціонування КІС (CQ) відображені лише частково, що обмежує можливість врахування каскадних ефектів та обґрунтування раціональних стратегій забезпечення захищеності.

Зазначені прогалини нормативного регулювання підтверджують доцільність подальшого аналізу сучасних викликів захисту ІКС, що також відображено в аналітичних звітах державних органів. Зокрема, за даними Державного центру кіберзахисту [16] та РНБО України [17], спостерігається зростання кількості складних кіберінцидентів, спрямованих на ОКІ, що свідчить про недостатність лише нормативного регулювання без розвитку методів оцінювання ефективності захисту.

Особливу роль у структурі КІ відіграють ***критичні інформаційні системи (КІС)***, які є складовою ІКС. У межах даного дослідження під КІС пропонується розуміти сукупність взаємопов'язаних інформаційних, комунікаційних і технологічних компонентів, від безперебійного функціонування яких залежить стабільність роботи ОКІ, а також безпека, економічна стійкість і життєдіяльність держави [18-19].

З урахуванням сучасних умов функціонування важливим є врахування взаємозалежностей між об'єктами. У цьому контексті під ***взаємозалежними критичними інфраструктурами (ВКІ)*** у даному дослідженні пропонується розуміти сукупність ОКІ, між якими існують взаємні впливи, за яких порушення роботи одного об'єкта може призвести до каскадних відмов або зниження ефективності функціонування інших об'єктів [20-21].

Відповідно, ***безпека ВКІ*** розглядається як стан захищеності КІС взаємопов'язаних ОКІ від внутрішніх і зовнішніх загроз, який забезпечує їх стійке, надійне та безперервне функціонування з урахуванням взаємозалежностей та впливу інцидентів на суміжні системи [20-21].

Таким чином, проведений аналіз показав, що існуюча нормативно-правова база визначає основні принципи та вимоги до захисту ІКС КІ, достатньо повно регламентує базові організаційні й технічні заходи безпеки, однак недостатньо формалізує питання кількісного оцінювання ефективності функціонування КІС, урахування взаємозалежностей між об'єктами та

обґрунтування раціональних стратегій забезпечення їх захищеності. Це обумовлює необхідність удосконалення відповідних методів оцінювання ефективності функціонування ІКС.

1.2. Аналіз підходів до оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур

Забезпечення ефективного функціонування систем безпеки ВКІ є складною науково-практичною задачею, що обумовлена високим рівнем взаємозв’язків між їх елементами, динамічним характером загроз та обмеженістю ресурсів. У сучасних умовах КІ функціонує як інтегрована система захисту, у якій порушення роботи окремих об’єктів може призводити до каскадних ефектів і суттєво впливати на загальну ефективність функціонування [20-24].

Аналіз наукових джерел свідчить, що існуючі підходи до оцінювання ефективності функціонування систем безпеки базуються на використанні методів теорії надійності, ризик-аналізу, оптимізації та стохастичного моделювання. Водночас більшість підходів враховує взаємозалежності лише частково або в межах окремих моделей, що не забезпечує повного урахування взаємозв’язків між ОКІ та динаміки зміни їх станів [22-33].

Проаналізовані підходи до оцінювання ефективності функціонування систем безпеки ВКІ доцільно згрупувати за такими основними напрямами: *інвестиційні*, що орієнтовані на обґрунтування раціонального розподілу ресурсів і визначення економічної доцільності заходів захисту; *ризик-орієнтовані*, які базуються на оцінюванні ймовірності реалізації загроз та можливих наслідків їх впливу; *стохастичні*, що враховують випадковий характер функціонування систем і зміну їх станів у часі; а також *оптимізаційні*, спрямовані на визначення ефективних стратегій функціонування та відновлення систем в умовах обмежених ресурсів. Водночас встановлено, що більшість існуючих підходів розглядають

зазначені напрями ізольовано, що обмежує можливість інтегрованого поєднання моделей взаємозалежностей, стохастичних процесів та оптимізаційних процедур [22, 24, 27, 30-33].

Деталізацію основних підходів до оцінювання ефективності функціонування систем безпеки ВКІ та їх обмежень наведено далі.

У роботі [22] розглянуто підхід до оцінювання ефективності функціонування взаємозалежних інфраструктур, що базується на аналізі їх продуктивності та оптимізації інвестицій. Автори показують, що ефективність функціонування системи залежить від структури взаємозв'язків між її елементами та обґрунтованого розподілу ресурсів.

У роботі [23] запропоновано концептуальні основи аналізу ВКІ, які передбачають їх класифікацію за типами (фізичні, кібернетичні, географічні, логічні). Узагальнену структуру взаємозалежностей та їх основні характеристики наведено на рис. 1.3. Показано, що такі взаємозв'язки можуть призводити до каскадних ефектів, однак кількісні методи оцінювання ефективності функціонування ВКІ не наведені.

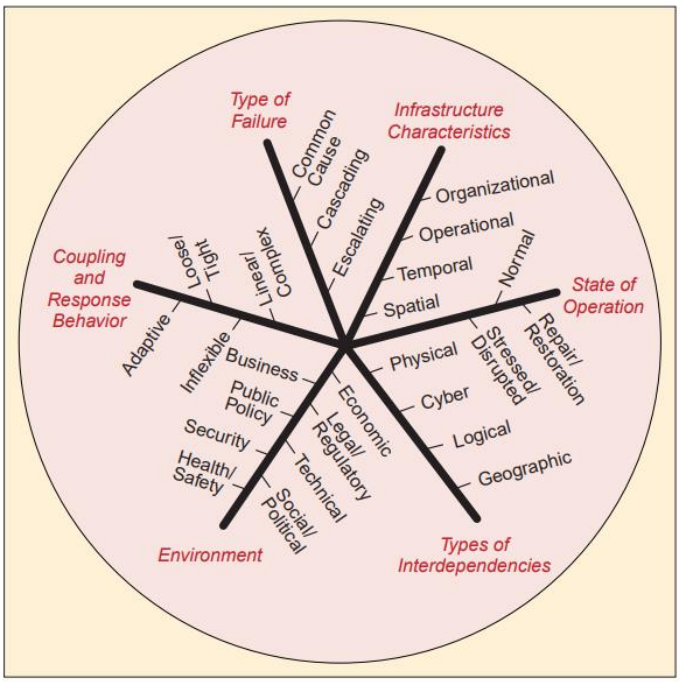

Рис. 1.3. Основні виміри взаємозалежностей КІ (за [23])

У дослідженні [24] розглянуто підхід до оптимізації інвестицій у відновлення взаємозалежних інфраструктур. Запропоновано модель розподілу ресурсів, що дозволяє визначати ефективні стратегії відновлення функціонування системи, проте не враховує стохастичний характер зміни її станів.

У роботі [25] розглянуто SCADA-системи як технологічну основу функціонування значної частини об'єктів КІ. Показано, що інтеграція інформаційних технологій (ІТ) процесів підвищує ефективність управління, водночас актуалізує кіберзагрози та збільшує кількість векторів атак.

У дослідженні [26] наведено огляд підходів до побудови SCADA-систем на основі сучасних протоколів обміну даними, що забезпечує гнучкість і масштабованість систем, однак не орієнтований на оцінювання ефективності функціонування систем інформаціної безпеки (ІБ).

У роботі [27] запропоновано підхід до оцінювання та оптимізації стійкості взаємопов'язаних інфраструктур, що базується на багатокритеріальній оптимізації. Автори враховують взаємозалежності між об'єктами, обмеженість ресурсів та вплив заходів безпеки, що дозволяє оцінювати ефективність функціонування системи ВКІ в умовах деструктивних впливів.

У роботі [28] наведено концептуальні засади забезпечення захисту КІ, які базуються на інтеграції різних механізмів безпеки, однак не містять формалізованих методів оцінювання ефективності функціонування ВКІ.

У роботі [29] запропоновано підхід до оцінювання стійкості (resilience) КІ на основі інтегральних показників, що дозволяє враховувати комплексний вплив факторів, проте не забезпечує формалізованого кількісного врахування взаємозалежностей між об'єктами.

У дослідженні [30] розглянуто ризик-орієнтований підхід до оцінювання функціонування інфраструктури, що базується на комплексному аналізі факторів ризику. Такий підхід дозволяє враховувати різні фактори впливу, але має обмеження щодо динаміки функціонування системи.

У роботі [31] запропоновано методи імітаційної оптимізації, які можуть застосовуватись для оцінювання ефективності функціонування системи за різними сценаріями. Недоліком є висока складність реалізації та значні обчислювальні витрати.

У роботі [32] запропоновано інвестиційно-орієнтований підхід до оцінювання ефективності функціонування систем ІБ, що базується на інтегральних показниках ефективності. Він дозволяє враховувати економічні аспекти, однак обмежено відображають складні взаємозалежності між об’єктами та процесами в системі.

У роботі [33] наведено теоретичні основи застосування напівмарківських процесів для моделювання надійності складних систем, що дозволяє враховувати стохастичний характер їх функціонування, проте не орієнтований на моделювання взаємозалежностей інфраструктур.

Для порівняльного аналізу у табл. 1.2 використано такі критерії:

1. Урахування взаємозалежностей (CI);
2. Урахування стохастичного характеру (CP);
3. Наявність оптимізаційного апарату (CO);
4. Оцінювання ефективності (CE);
5. Практична реалізованість (CR).

Оцінювання за критеріями здійснювалось на основі аналізу наявності відповідного математичного апарату, моделей та результатів, представлених у роботах [20-33].

Таблиця 1.2

Порівняльний аналіз підходів до оцінювання ефективності функціонування систем ВКІ

№	Джерело	CI	CP	CO	CE	CR
1	Nozick L. et al.	+	–	+	+	–
2	Rinaldi S. et al.	+	–	–	–	+
3	Xu N. et al.	+	–	+	+	–
4	Boyer S.	–	–	–	–	+
5	Abbas H. et al.	–	–	–	–	+
6	Kong J. et al.	+	–	+	+	+
7	Mussington D.	–	–	–	–	–
8	Petit F. et al.	+	–	–	+	+
9	Phillips J. et al.	–	–	–	+	+
10	Gürkan G. et al.	–	+	+	+	–
11	Євсеєв С.	+	–	+	+	+
12	Limnios N., et al.	–	+	–	–	–

З табл. 1.2 видно, що найбільш розвиненими є підходи, орієнтовані на оптимізацію ресурсів та оцінювання ефективності (CO, CE), зокрема роботи [22], [24], [27], [31-32]. Водночас урахування взаємозалежностей між об’єктами (CI) реалізовано лише в окремих підходах, а стохастичний характер функціонування систем (CP) враховується обмежено, переважно в роботах [31] та [33].

Крім того, більшість підходів не забезпечує комплексного поєднання критеріїв CI, CP та CO, що є необхідним для адекватного оцінювання ефективності функціонування ВКІ. Це обмежує можливість отримання узагальненої оцінки стану системи та обґрунтованого прийняття рішень щодо розподілу ресурсів.

Таким чином, виникає необхідність удосконалення методу оцінювання ефективності функціонування систем безпеки ВКІ, який забезпечує комплексне врахування взаємозалежностей між об'єктами, стохастичного характеру їх функціонування та дозволяє обґрунтовувати розподіл ресурсів і підвищення ефективності функціонування системи.

1.3. Аналіз підходів до оцінювання впливу інцидентів на рівень захищеності ІКС

Оцінювання впливу інцидентів на рівень захищеності ІКС КІ є важливою складовою забезпечення їх сталого функціонування. Сучасні ІКС функціонують в умовах постійного виникнення інцидентів різної природи, що відрізняються за ймовірністю виникнення, рівнем критичності, тривалістю впливу та наслідками для системи. Це зумовлює необхідність розроблення підходів, які дозволяють кількісно оцінювати вплив інцидентів на стан функціонування системи. Приклади можливих інцидентів та їх впливу на функціонування КІ наведено на рис. 1.4.

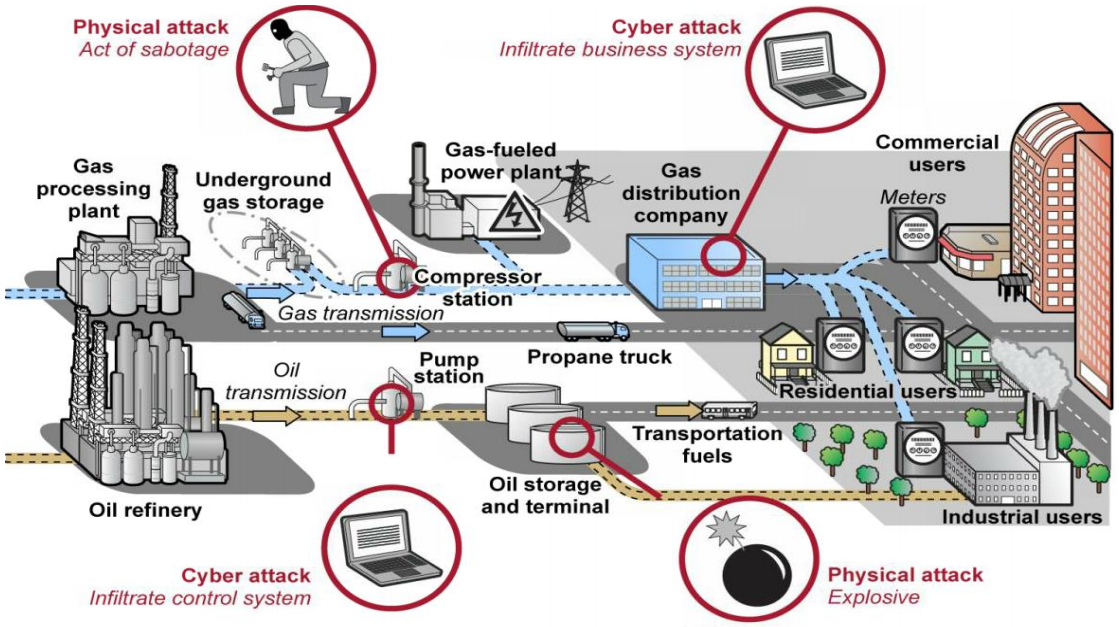

Рис. 1.4. Приклад інцидентів та вразливостей КІ та їх впливу на функціонування систем (за [34])

Як видно з рис. 1.4, інциденти можуть мати як фізичну, так і інформаційну природу та впливати на різні елементи інфраструктури, що призводить до порушення їх функціонування та виникнення каскадних ефектів.

Аналіз наукових джерел [35-51] свідчить, що існуючі підходи переважно орієнтовані на оцінювання ризиків, пріоритизацію інцидентів або визначення окремих показників їх впливу. Водночас недостатньо дослідженими залишаються питання формалізації взаємозв'язку між характеристиками інцидентів та параметрами стану ІКС, а також інтегрованого врахування їх впливу на рівень захищеності. Це ускладнює можливість кількісного оцінювання загального стану функціонування системи та обґрунтованого прийняття управлінських рішень.

З огляду на викладене, проведено аналіз сучасних підходів до оцінювання впливу інцидентів на рівень захищеності ІКС.

У роботі [41] розглянуто підхід до оцінювання ризиків кібербезпеки інформаційних систем (ІС) ОКІ, що базується на використанні векторної та інтегральної моделей ризику. Автори враховують множину параметрів ризику та їх вагомість за допомогою вагових коефіцієнтів, що дозволяє отримати узагальнену кількісну оцінку рівня ризику. Запропонований підхід орієнтований на комплексне оцінювання стану системи з позиції ризиків та може бути використаний для підтримки прийняття рішень у сфері ІБ.

У роботі [42] досліджено підхід до управління ІТ-інцидентами в ІКС КІ, що передбачає використання моделі оцінювання загроз із застосуванням методу аналізу ієрархій. Автори пропонують враховувати різні критерії, що характеризують інциденти, та визначати їх пріоритетність для забезпечення ефективного реагування. Основна увага приділяється організації процесу управління інцидентами та підтримці прийняття рішень.

У статті [43] розглянуто сучасні підходи до управління інцидентами ІБ на ОКІ з урахуванням міжнародних стандартів та практик. Автори аналізують процеси виявлення, оброблення та реагування на інциденти, а також підкреслюють важливість своєчасного відновлення функціонування системи. Запропоновано узагальнену модель управління інцидентами, спрямовану на підвищення стійкості ІКС.

У роботі [44] представлено метод визначення стану захищеності ОКІІ на основі оцінювання ІТ-ризиків. Підхід базується на аналізі ймовірності виникнення інцидентів, рівня вразливостей та можливих наслідків їх реалізації. Узагальнення цих показників дозволяє отримати інтегральну оцінку рівня захищеності системи та оцінити її поточний стан.

У статті [45] розглянуто методи аналізу вразливостей і ризиків КІ з урахуванням складної структури систем та взаємозалежностей між їх елементами. Автори пропонують підхід, що дозволяє оцінювати вплив різних подій на функціонування системи, враховуючи як ймовірність їх виникнення, так і наслідки. Особлива увага приділяється врахуванню взаємозалежностей та каскадного поширення наслідків інцидентів.

У роботі [46] запропоновано концептуальну модель стійкості енергетичних систем, яка враховує здатність системи протистояти, адаптуватися та відновлюватися після впливу деструктивних подій. Автори розглядають вплив зовнішніх і внутрішніх факторів на функціонування системи та визначають ключові складові її стійкості. Підхід дозволяє оцінювати зміну стану системи під впливом збурень.

У роботі [47] представлено систему оброблення, попередження та реагування на інциденти кібербезпеки та кіберстійкості для ІКС КІ. Запропонований підхід забезпечує інтеграцію процесів виявлення, аналізу та реагування на інциденти, а також підтримку прийняття рішень у реальному часі. Система захисту дозволяє враховувати різні типи інцидентів та їх вплив

на функціонування КІ, проте не орієнтована на кількісне оцінювання інтегрального впливу інцидентів на рівень захищеності системи.

У роботі [48] розглянуто сучасні аспекти кібербезпеки, зокрема природу кіберінцидентів, їх класифікацію та вплив на функціонування інформаційних систем (ІС) та КІ. Автори аналізують наслідки кіберінцидентів для різних секторів та підкреслюють необхідність комплексного підходу до забезпечення кіберстійкості, однак не запропоновано формалізованого методу кількісного оцінювання впливу інцидентів на рівень захищеності.

У роботі [49] запропоновано підхід до оцінювання ризику реалізації загроз безпеки у телекомунікаційних системах, що базується на використанні інтегрального показника ризику з урахуванням вагомості окремих факторів впливу. Автори враховують імовірність реалізації загроз, можливі наслідки та взаємозв’язки між параметрами ризику, що дозволяє формувати кількісну оцінку стану захищеності системи. Водночас підхід орієнтований переважно на оцінювання ризику та не забезпечує формалізованого оцінювання впливу інцидентів на динаміку зміни стану функціонування ІКС.

У роботі [50] запропоновано модель пріоритизації інцидентів безпеки на основі ризикового індексу, що враховує характеристики інцидентів, їх критичність та відносну вагомість окремих критеріїв. Підхід базується на використанні вагових коефіцієнтів і дозволяє ранжувати інциденти за пріоритетністю реагування. Разом з тим основна увага приділяється пріоритизації інцидентів, тоді як кількісне оцінювання їх інтегрального впливу на рівень захищеності системи залишається обмеженим.

У роботі [51] запропоновано модель оцінювання вартості реагування на інциденти в інфраструктурах Advanced Metering Infrastructure, що враховує характеристики інцидентів, параметри стану системи та витрати на реагування. Підхід дозволяє кількісно оцінювати вплив різних сценаріїв

інцидентів на функціонування системи та підтримувати вибір раціональних стратегій реагування. Водночас модель орієнтована переважно на оцінювання витрат реагування й не забезпечує узагальненого оцінювання рівня захищеності ІКС.

У табл. 1.3 систематизовано результати аналізу підходів до оцінювання впливу інцидентів на рівень захищеності ІКС за запропонованими критеріями:

1. Урахування характеристик інцидентів (CI) – відображає ступінь урахування параметрів інцидентів (типу, тривалості, критичності, частоти виникнення) при оцінюванні.

2. Урахування параметрів стану системи (CS) – характеризує наявність взаємозв’язку між параметрами інцидентів та показниками функціонування ІКС.

3. Використання вагових коефіцієнтів (CW) – визначає застосування механізмів зважування для врахування відносної значущості окремих факторів.

4. Наявність інтегрального показника (IG) – характеризує можливість формування узагальненого показника для оцінювання рівня захищеності системи.

5. Оцінювання впливу інцидентів (CE) – відображає можливість кількісного оцінювання впливу інцидентів на параметри функціонування системи.

6. Оцінювання стану функціонування системи (CF) – характеризує здатність підходу визначати узагальнений стан функціонування ІКС.

7. Орієнтація на КІ (CC) – відображає врахування специфічних особливостей функціонування ОКІ.

Таблиця 1.3

Порівняльний аналіз підходів до оцінювання впливу інцидентів на рівень захищеності ІКС

№	Джерело	CI	CS	CW	IG	CE	CF	CC
1	Mokhor V. et al.	+	+	+	+	–	+	+
2	Качинський А. та ін.	+	–	+	–	–	–	+
3	Sysoienko S. et al.	+	+	–	–	–	+	+
4	Jablanski D.	+	+	+	+	–	+	+
5	Kröger W. et al.	+	+	–	–	+	+	+
6	Panteli M. et al.	+	+	–	–	+	+	+
7	Papastergiou S. et al.	+	+	–	–	+	+	+
8	Behl A. et al.	+	–	–	–	+	±	+
9	Король О. та ін.	+	+	+	+	–	+	–
10	Anuar N. et al.	+	–	+	+	±	–	–
11	Mahmood Y. et al.	+	+	+	+	+	±	+

Представлений у табл. 1.3 аналіз показує, що більшість існуючих підходів орієнтовані на оцінювання ризиків, управління інцидентами або визначення стійкості систем. При цьому найбільш дослідженими є критерії CI та CS. Водночас оцінювання безпосереднього впливу інцидентів на інтегральний показник захищеності (IG) реалізовано лише частково, а формалізований взаємозв’язок між характеристиками інцидентів, параметрами стану системи та узагальненим показником її функціонування залишається недостатньо опрацьованим. Це ускладнює можливість кількісного оцінювання загального стану функціонування системи та обґрунтованого прийняття рішень щодо реагування на інциденти.

Таким чином, існує необхідність удосконалення підходів до оцінювання впливу інцидентів на рівень захищеності ІКС, які забезпечують комплексне врахування розглянутих критеріїв при формуванні інтегрального показника впливу інцидентів.

1.4. Аналіз підходів до підвищення рівня захищеності критичних інформаційних систем держави

Забезпечення належного рівня захищеності КІС є одним із ключових завдань держави, оскільки від їх сталого функціонування залежить національна кібербезпека, економічна стабільність та обороноздатність країни. Сучасні виклики, пов’язані з деструктивними інформаційно-технічними впливами, фізичними та технологічними ризиками, зумовлюють необхідність застосування комплексних підходів до підвищення рівня захищеності таких систем. Водночас аналіз наукових джерел свідчить, що перспективним напрямом є інтеграція існуючих підходів, яка дозволяє поєднати оцінювання ризиків, надійності та стійкості в єдину методологічну основу.

Для вирішення завдань, пов’язаних із забезпеченням захищеності КІС, проведено аналіз сучасних публікацій, розглянуто існуючі підходи до визначення рівня захищеності та здійснено їх порівняльний аналіз.

У роботі [53] Мурасов Р. та Мельник Я. розглянуто підхід до оцінювання захищеності кіберпростору ОКІ України, який базується на системному аналізі ризиків, уразливостей та потенційних наслідків реалізації загроз. Автори пропонують методику, що враховує особливості функціонування ІС ОКІ та передбачає використання сучасних засобів моніторингу і тестування кібербезпеки, однак підхід лише обмежено враховує взаємозалежності між ОКІ.

В аналітичній доповіді [54] Суходолі О. представлено системне дослідження стійкості критичної енергетичної інфраструктури та механізмів забезпечення життєдіяльності громад в умовах кризових ситуацій. Автор акцентує увагу на важливості інтегрованого підходу, що поєднує оцінювання ризиків, управління надійністю та забезпечення здатності систем до відновлення.

У роботі [55] Шевченка Н. І. та Плахотнюка Р. В. запропоновано методичні підходи до оцінювання стійкості функціонування ОКІ України в умовах особливого періоду. Автори обґрунтовують необхідність комплексного врахування технічних, організаційних, кадрових і фінансових чинників, що впливають на кіберстійкість систем, та розробляють багатокритеріальну модель оцінювання з інтегральним показником стійкості, однак підхід орієнтований переважно на оцінювання стійкості та не деталізує механізми підвищення захищеності КІС.

У дослідженні [56] Кириленка С. П. та Тищенка В. В. розглянуто формалізовані моделі оцінювання ризиків для ОКІ в умовах збройного конфлікту. Автори пропонують математичний апарат для кількісного оцінювання ризику, що враховує ймовірність реалізації загроз, рівень уразливості та очікувані наслідки, проте підхід переважно фокусується на ризиковому оцінюванні й обмежено враховує питання оптимізації заходів підвищення захищеності.

У роботі [57] Третьякова О. В. та ін. запропоновано підхід до кількісного оцінювання стійкості ОКІ, який базується на використанні системи нормованих показників і вагових коефіцієнтів, що відображають вплив технічних, організаційних та інформаційних чинників. Отримана інтегральна оцінка дозволяє визначати рівень стійкості об’єкта та динаміку його змін у часі, однак підхід переважно орієнтований на оцінювання стану системи та не містить механізмів оптимізації заходів підвищення її захищеності.

У статті [58] Mahmood Y., Afrin T. та ін. обґрунтовано системний підхід до сталого розвитку інфраструктур на основі концепції 3R (Risk–Reliability–Resilience) (рис. 1.5). Запропоновано взаємопов’язану матрицю, що відображає взаємозв’язки між ризиками, надійністю та стійкістю систем і дозволяє формалізувати їх у єдиній моделі оцінювання.

Рис. 1.5. Ієрархія складових сталого функціонування систем (Risk–Reliability–Resilience–Sustainability) (джерело: [58])

У публікації [59] Mohd Safari M. A., Masseran N. та ін. представлено робастний метод оцінювання параметрів надійності технічних систем, що ґрунтується на експоненційному розподілі часу безвідмовної роботи. Запропонований підхід дозволяє зменшити вплив аномальних даних та підвищити точність визначення інтенсивності відмов, однак підхід орієнтований переважно на параметри надійності та не враховує безпосередньо заходи підвищення захищеності КІС.

У статті [60] Kong J., Zhang C. та ін. запропоновано підхід до оптимізації стійкості взаємопов’язаних інфраструктур шляхом поєднання технічних і організаційних заходів підвищення безпеки. Автори застосували методи багатокритеріальної оптимізації для визначення раціонального набору рішень з урахуванням обмежень ресурсів, часу та рівня ризику, що дозволяє оцінювати зміну рівня стійкості систем унаслідок реалізації відповідних стратегій.

У статті [61] Rehak D., Flynnova L. та ін. розглянуто вдосконалений метод оцінювання стійкості елементів КІ (CIERA+), який доповнено складовою опору (resistance). Автори підкреслюють, що здатність системи протидіяти впливу загроз є невід'ємною складовою її стійкості, проте підхід зосереджений переважно на оцінюванні стійкості й не деталізує механізми вибору заходів підвищення захищеності.

У роботі [62] Irankunda G., Zhang W. та ін. представлено багатосценарний підхід до оцінювання стійкості ОКІ, який поєднує виявлення сценаріїв ризику, оцінювання наслідків та агрегацію результатів у єдиний інтегральний показник стійкості (рис. 1.6). Автори наголошують на важливості врахування взаємозалежностей між різними типами загроз та адаптивних можливостей системи.

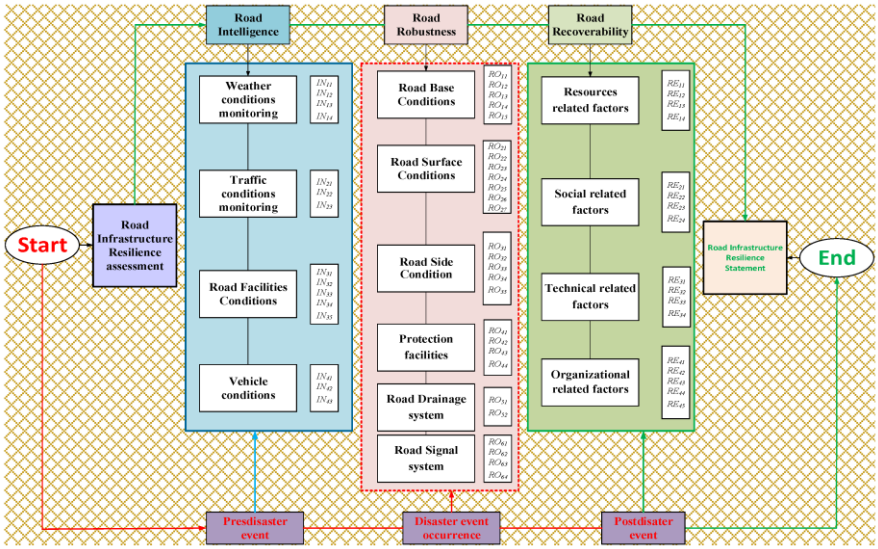

Рис. 1.6. Структура оцінювання стійкості ОКІ з урахуванням етапів функціонування та впливу факторів (джерело: [62])

Представлений підхід демонструє комплексний характер оцінювання стійкості, проте орієнтований на окремі типи інфраструктури та не забезпечує інтегрованого врахування взаємозв'язків між ризиком, надійністю та стійкістю систем при обґрунтуванні стратегій їх функціонування.

У табл. 1.4 на основі узагальнення результатів попередніх досліджень [19, 52-62] представлено порівняльний аналіз підходів до оцінювання рівня захищеності ІКС за такими критеріями (запропонованими автором):

1. Рівень ризику реалізації загроз (RR) – відображає ймовірність настання подій, що можуть призвести до порушення функціонування КІС; розраховується на основі множини потенційних загроз та сценаріїв їх реалізації.

2. Імовірність відмови елементів системи (RF) – характеризує надійність КІС як сукупність компонентів, що здатні зберігати працездатність під впливом внутрішніх та зовнішніх факторів.

3. Рівень адаптивності до загроз (RA) – здатність системи змінювати конфігурацію, алгоритми чи режими роботи з метою мінімізації наслідків потенційних атак або збоїв.

4. Ефективність стратегій захищеності (RE) – інтегральна оцінка результативності обраних стратегій (технічних, організаційних, кадрових) за критерієм максимального зниження ризику при обмежених ресурсах.

5. Оперативність реагування (RRs) – середній час і послідовність дій, необхідних для локалізації інциденту та відновлення ключових функцій КІС.

6. Стійкість інформаційних потоків (RI) – здатність ІС підтримувати безперервність та достовірність обміну даними у кризових умовах.

7. Ресурсна забезпеченість захисту (RC) – доступність фінансових, технічних і людських ресурсів для реалізації заходів підвищення захищеності, у тому числі резервних каналів і дублюючих систем.

8. Інтегральний показник ефекту (PSI) – узагальнений критерій, що відображає ступінь досягнення заданого рівня захищеності в результаті реалізації стратегії 3R, визначається за співвідношенням між початковим і поточним рівнем стійкості.

Таблиця 1.4

Порівняльний аналіз підходів до оцінювання рівня захищеності КІС

№	Джерело	Критерії							
		RR	**RF**	**RA**	**RE**	**RRs**	**RI**	**RC**	**PSI**
1.	Мурасов Р. та ін.	+	±	–	±	+	+	–	±
2.	Суходоля О.	±	–	±	±	–	±	+	–
3.	Шевченко Н. І. та ін.	+	+	±	+	±	+	±	+
4.	Кириленко С. П. та ін.	+	±	–	–	–	–	±	–
5.	Третьяков О. В. та ін.	±	+	±	±	±	+	±	+
6.	Mahmood Y. et al.	+	+	+	+	±	+	±	+
7.	Mohd Safari M.A. et al.	–	+	–	±	–	–	±	±
8.	Kong J. et al.	±	+	+	+	±	+	±	+
9.	Rehak D. et al.	±	±	+	+	±	+	±	+
10.	Irankunda G. et al.	+	±	+	+	+	+	±	+

Представлений у табл. 1.4 порівняльний аналіз підходів до оцінювання рівня захищеності ІКС показав, що найбільш повно представленими є критерії рівня ризику реалізації загроз (RR), надійності елементів системи (RF) та стійкості інформаційних потоків (RI). Зазначені аспекти є центральними у більшості проаналізованих праць, зокрема зарубіжних, що ґрунтуються на принципах 3R.

Водночас встановлено, що адаптивність систем (RA), ресурсна забезпеченість заходів захисту (RC) та оперативність реагування (RRs) враховуються фрагментарно або не мають формалізованого представлення, особливо в контексті вітчизняних досліджень. Крім того, існуючі підходи, як правило, не забезпечують комплексного врахування взаємозв’язків між ризиком, надійністю та стійкістю систем, а також не орієнтовані на оптимізацію стратегій підвищення захищеності в умовах обмеженості ресурсів.

Питаннями оцінювання ефективності та захищеності ІКС КІ держави займаються такі вітчизняні та закордонні вчені: Качинський А., Кириленко С. П., Мохор В., Мурасов Р., Суходоля О., Третьяков О., Шевченко Н., Jablanski D., Kong J., Limnios N., Mahmood Y., Mohd Safari M., Nozick L., Papastergiou S. та інші. Проте, слід зазначити, що переважна більшість проаналізованих робіт спрямована на вирішення окремих задач забезпечення безпеки. При цьому встановлено, що існуючі підходи не забезпечують комплексного врахування взаємозалежностей ОКІ, впливу інцидентів на стан систем та оптимізації стратегій їх захисту в умовах обмежених ресурсів.

Таким чином, виникає необхідність розроблення методу підвищення рівня захищеності КІС, який забезпечує інтегроване оцінювання їх стану з урахуванням взаємозв’язків між ризиком, надійністю та стійкістю системи, а також дозволяє обґрунтовувати вибір раціональних стратегій забезпечення стійкості в умовах обмежених ресурсів.

1.5. Постановка завдання дисертаційного дослідження

Таким чином, у першому розділі на основі проведеного аналізу визначено та обґрунтовано основні задачі дослідження, розв’язання яких необхідне для досягнення поставленої мети дисертаційної роботи.

Для досягнення поставленої мети необхідно вирішити такі задачі:

1. Розробити метод оцінювання ефективності функціонування систем безпеки ВКІ (п. 2.1).
2. Розробити метод оцінювання впливу інцидентів на рівень захищеності ІКС КІ (п. 2.2).
3. Розробити метод підвищення рівня захищеності КІС КІ (п. 3.1).
4. Сформувати практичні рекомендації щодо раціонального розподілу інвестицій та ресурсів з урахуванням наявних обмежень (п. 4.1).

5. Розробити методику оцінювання впливу інцидентів, що дозволяє враховувати їх наслідки при прийнятті рішень щодо управління функціонуванням ІКС (п. 4.2).

6. Розробити програмне забезпечення, яке забезпечує комплексне оцінювання стану ІКС, прогнозування впливу загроз та сформувати практичні рекомендації щодо вибору раціональної сукупності організаційних і технічних заходів забезпечення захищеності ОКІІ (п. 4.3).

1.6. Висновки до першого розділу

У результаті проведеного аналізу підходів до оцінювання ефективності функціонування систем безпеки ВКІ встановлено, що існуючі методи базуються на використанні інструментарію теорії надійності, ризик-аналізу, оптимізації та стохастичного моделювання. Водночас більшість із них враховує взаємозалежності між ОКІ лише частково або в межах окремих моделей, що не забезпечує комплексного урахування динаміки функціонування систем та обмежує можливості обґрунтованого розподілу ресурсів.

Аналіз підходів до оцінювання впливу інцидентів на рівень захищеності ІКС показав, що існуючі рішення переважно орієнтовані на оцінювання ризиків, пріоритизацію інцидентів або визначення окремих показників їх впливу. При цьому встановлено відсутність формалізованого взаємозв’язку між характеристиками інцидентів та параметрами стану системи, а також обмеженість інтегрованого врахування їх впливу на узагальнений рівень захищеності.

У ході аналізу підходів до підвищення рівня захищеності КІС встановлено, що сучасні дослідження зосереджені на окремих складових, зокрема оцінюванні ризику, надійності та стійкості систем, часто в рамках концепції 3R. Разом із тим виявлено, що існуючі підходи не забезпечують

комплексного врахування взаємозв’язків між зазначеними характеристиками, а також недостатньо орієнтовані на оптимізацію стратегій забезпечення захищеності в умовах обмежених ресурсів.

Проведений системний аналіз дозволив формалізувати завдання дисертаційного дослідження щодо розроблення та вдосконалення методів оцінювання ефективності функціонування, впливу інцидентів та підвищення рівня захищеності ІКС КІ держави.

1.7. Список літератури до першого розділу

1. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

3. Кабінет Міністрів України. «Деякі питання забезпечення безпеки та стійкості критичної інфраструктури». Постанова від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2021-п.

4. Кабінет Міністрів України. «Про затвердження критеріїв віднесення об’єктів до категорій критичності». Постанова від 13.05.2022 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2022-п.

5. Кабінет Міністрів України. «Про затвердження Положення про організаційно-технічну модель кіберзахисту». Постанова від 29.12.2021 № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п.

6. Адміністрація Державної служби спеціального зв’язку та захисту інформації України. Методика оцінки стану захищеності об’єктів критичної інфраструктури: наказ від 14.01.2025 № 17. URL: https://zakon.rada.gov.ua/laws/show/z0375-25.

7. Адміністрація Державної служби спеціального зв’язку та захисту інформації України. «Про затвердження Базових заходів з кіберзахисту»: наказ від 30.01.2025 № 54.

8. ISO/IEC 27001:2022. Information technology — Security techniques — Information security management systems — Requirements. 2022.

9. ISO/IEC 27005. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. 2022.

10. National Institute of Standards and Technology. Cybersecurity Framework. Version 2.0. 2024. URL: https://www.nist.gov/cyberframework

11. IEC 62443-3-3:2013. Security for Industrial Automation and Control Systems – System Security Requirements and Security Levels. Geneva: International Electrotechnical Commission, 2013.

12. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82 Rev. 3). Gaithersburg, MD: National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.SP.800-82r3.

13. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union. 2022.

14. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). Official Journal of the European Union. 2022.

15. Cybersecurity and Infrastructure Security Agency. Cybersecurity Performance Goals. 2023. URL: https://www.cisa.gov.

16. Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації України. Річний звіт. 2025.

17. Рада національної безпеки і оборони України. Річний аналітичний огляд. 2024.

18. Сидоренко В., Максимець А. Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. Кібербезпека: освіта, наука, техніка. 2025. № 3(27). С. 560–571. DOI: https://doi.org/10.28925/2663-4023.2025.27.779.

19. Сидоренко В. М., Сидоренко С. Ю. Метод підвищення рівня захищеності критичних інформаційних систем держави. Кібербезпека: освіта, наука, техніка. 2025. Т. 2. № 30. С. 500–510. DOI: https://doi.org/10.28925/2663-4023.2025.30.988.

20. Гнатюк С.О., Сидоренко В.М., Березовий І.Р., Сидоренко С.Ю., Тараненко К.О. Модель оцінювання ефективності функціонування систем інформаційної безпеки взаємозалежних критичних інфраструктур. Проблеми інформатизації та управління. 2022. Т. 4. № 72. С. 17-25. DOI: https://doi.org/10.18372/2073-4751.72.17457.

21. Lutskyi M., Sydorenko V., Polozhentsev A., Apenko N., Sydorenko S. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures. CEUR Workshop Proceedings. 2023. Vol. 3421. P. 214-222. URL: https://ceur-ws.org/Vol-3421/short7.pdf

22. Nozick L., Turnquist M., Jones D., Davis J., Lawton C. Assessing the Performance of Interdependent Infrastructures and Optimizing Investment. Proceedings of the 37th Hawaii International Conference on System Sciences. 2004.

23. Rinaldi S. M., Peerenboom J. P., Kelly T. K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine. 2001. Vol. 21, No. 6. P. 11–25.

24. Xu N., Nozick L. K., Turnquist M. A., Jones D. A. Optimizing Investment for Recovery in Interdependent Infrastructure. Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS’07). Waikoloa, HI, USA, 2007. P. 112–112. DOI: 10.1109/HICSS.2007.413.

25. Boyer S. A. SCADA: Supervisory Control and Data Acquisition. 4th ed. USA: ISA – International Society of Automation, 2010. 179 p.

26. Abbas H. A., Mohamed A. M. Review in the design of web-based SCADA systems based on OPC DA protocol. International Journal of Computer Networks. 2011. Vol. 2, No. 6. P. 266–277.

27. Kong J., Zhang C., Simonovic S. P. Optimizing the resilience of interdependent infrastructures to regional natural hazards with combined improvement measures. Reliability Engineering & System Safety. 2021. Vol. 210. Article 107538. DOI: 10.1016/j.ress.2021.107538.

28. Mussington D. Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development. Santa Monica, CA: RAND Science and Technology Institute, 2002. 29 p.

29. Petit F., Wallace K., Phillips J. An Approach to Critical Infrastructure Resilience. The CIP Report. 2014. Vol. 12, No. 7. P. 17–20.

30. Phillips J. A., Bassett G. W., Buehring W. A., Carlson J. L., Whitfield R. G., Peerenboom J. P. A Framework for Assessing Infrastructure Risk. Risk Analysis: Advancing Analysis. Society for Risk Analysis, 2012.

31. Gürkan G., Ozge Y., Robinson S. Sample Path Optimization in Simulation. Proceedings of the 1994 Winter Simulation Conference. 1994. P. 247-254.

32. Євсеєв С. П. Оцінка ефективності інвестицій в безпеку організацій банківського сектора на основі синергетичної моделі загроз. Системи обробки інформації. 2017. Вип. 2 (148).

33. Limnios N., Oprisan G. Semi-Markov Processes and Reliability. Boston: Birkhäuser, 2001.

34. Government Accountability Office. U.S. Pipeline Systems' Basic Components and Vulnerabilities. 2019.

35. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів IT-інцидентів на об'єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації

та управління. 2024. Т. 2. №78. С. 104-114. DOI: https://doi.org/10.18372/2073-4751.78.18967.

36. Gnatyuk S., Sydorenko V., Polozhentsev A., Sydorenko S. Experimental Study of the Method for Cyber Incidents Management in Aviation Critical Infrastructure. In: Ostroumov, I., Marais, K., Zaliskyi, M. (eds) Advances in Civil Aviation Systems Development. ACASD 2025. Lecture Notes in Networks and Systems, Vol. 1418. P. 74–91, Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-91992-3_6.

37. Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Смірнова Т.В., Сидоренко С.Ю. Модель визначення критичності галузевих інформаційно-телекомунікаційних систем. Проблеми інформатизації та управління. 2022. Т. 2. № 70. С. 28-37. DOI: https://doi.org/10.18372/2073-4751.70.16844.

38. Жигаревич О.К., Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю. Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи». Кіберзахист особи, суспільства і держави: наук.-практ. конф., с. Велятино, 24-27 січня 2024 р.: тези доп., Київ: НАУ, 2024. С. 14-15.

39. Nosal K., Solecka K. Application of AHP Method for Multi-Criteria Evaluation of Variants of the Integration of Urban Public Transport. Transportation Research Procedia. 2014. Vol. 3. P. 269–278. DOI: 10.1016/j.trpro.2014.10.006.

40. Saaty T. L. Decision Making with the Analytic Hierarchy Process. International Journal of Services Sciences. 2008. Vol. 1, No. 1. P. 83–98. DOI: 10.1504/IJSSCI.2008.017590.

41. Mokhor, V. V., Honchar, S. F. Evaluation of risks of cyber security of information systems of objects of critical infrastructure. Elektronnoe Modelirovanie. 2019. Vol. 41, No. 6. P. 65–76. DOI: 10.15407/emodel.41.06.065.

42. Качинський А. Б., Варичева Д. І., Свириденко С. В. Ефективне управління IT-інцидентами в критичній інформаційній інфраструктурі. Інформація і право. 2016. № 2(17). С. 114–126.

43. Sysoienko, S., Babenko, V., Lada, N. Information security incident management at critical infrastructure facilities. Herald of Khmelnytskyi National University. Technical Sciences. 2025. No. 4. P. 555–559.

44. Jablanski, D. Method for Determining the State of Protection of Critical Information Infrastructure Objects from IT Risks. 2023. URL: https://www.researchcybersecurity.com/state-protection-method/.

45. Kröger, W., Zio, E. Vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety. 2011. Vol. 96, No. 6. P. 637–645.

46. Panteli, M., Mancarella, P. The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. IEEE Power & Energy Magazine. 2015. Vol. 13, No. 3. P. 58–66.

47. Papastergiou, S., Mouratidis, H., Kalogeraki, E.-M., Vidalis, S., Kolokotronis, N. Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE). arXiv. 2020. DOI: https://doi.org/10.48550/arXiv.2003.05720.

48. Behl, A., Behl, K., Rao, S. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2022. 240 p.

49. Король О. Г., Огурцова К. В., Євсеєв С. П. Оцінка ризику реалізації загроз безпеки у телекомунікаційних системах. Автоматика, телемеханіка, зв'язок. Збірник наукових праць ДонІЗТ. 2013. № 36. С. 55–63.

50. Anuar N., Furnell S., Papadaki M., Clarke N. A Risk Index Model for Security Incident Prioritisation. Proceedings of the 9th Australian Information Security Management Conference (AISM). Perth, Australia, 2011. P. 25–39.

51. Mahmood Y., Abid M., Javaid N., Razzaq S. A Response Cost Model for Advanced Metering Infrastructures. International Journal of Distributed Sensor Networks. 2015. Vol. 11, No. 6. Article ID 457021. DOI: 10.1155/2015/457021.

52. Сидоренко В. (2025). Метод оцінювання стійкості об’єктів критичної інформаційної інфраструктури держави. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 837–853. https://doi.org/10.28925/2663-4023.2025.29.944.

53. Мурасов, Р., Мельник, Я. (2023). Оцінювання захищеності кіберпростору об’єктів критичної інфраструктури України. Сучасні інформаційні технології, (3), 98–112. https://sit.nuou.org.ua/article/view/280288.

54. Суходоля, О. (2022). Стійкість критичної енергетичної інфраструктури та життєдіяльності громад. Аналітична доповідь НІСД, 72 с. https://chtyvo.org.ua/.../Stiikist_krytychnoi_enerhetychnoi_infrastruktury_ta_zhyttiediialnosti_hromad.

55. Шевченко, Н. І., Плахотнюк, Р. В. (2024). Методичні підходи до оцінювання стійкості функціонування об’єктів критичної інфраструктури в умовах особливого періоду функціонування економіки України. Реформування економіки та інноваційні стратегії розвитку, 14(2), 112–126. https://reicst.com.ua/pmtl/article/view/2024-14-02-08.

56. Кириленко, С. П., Тищенко, В. В. (2023). Моделі оцінювання ризиків для критичної інфраструктури в умовах збройного конфлікту. Безпека життєдіяльності, 3(9), 74–88.

57. Третьяков, О. В., Халмурадов, Б. Д., Кічата, Н. М., & Ремська, А. В. (2025). Підхід до кількісної оцінки стійкості об’єктів критичної інфраструктури. Системи управління, навігації та зв’язку, 1(79), 178–183. https://doi.org/10.26906/SUNZ.2025.1.178-183.

58. Mahmood, Y., Afrin, T., Huang, Y., & Yodo, N. (2023). Sustainable development for oil and gas infrastructure from risk, reliability, and resilience perspectives. Sustainability, 15(6), 4953. https://doi.org/10.3390/su15064953.

59. Mohd Safari, M.A., Masseran, N., Abdul Majid, M.H. (2021). Robust and Efficient Reliability Estimation for Exponential Distribution. Computers, Materials & Continua, 69(2), 2807–2824. https://doi.org/10.32604/cmc.2021.018815.

60. Kong, J., Zhang, C., & Simonovic, S. P. (2021). Optimizing the resilience of interdependent infrastructures to regional natural hazards with combined improvement measures. Reliability Engineering & System Safety, 210, 107538. https://doi.org/10.1016/j.ress.2021.107538.

61. Rehak, D., Flynnova, L., Hromada, M., & Fuggini, C. (2023). The importance of resistance in the context of critical infrastructure resilience: An extension of the CIERA method. Systems, 11(10), 506. https://doi.org/10.3390/systems11100506.

62. Irankunda, G., Zhang, W., Fernand, M., & Zhang, J. (2024). Assessing the Resilience of Critical Infrastructure Facilities toward a Holistic and Theoretical Approach: A Multi-Scenario Evidence and Case Study. Sustainability, 16(20), 8735. https://doi.org/10.3390/su16208735

РОЗДІЛ 2
РОЗРОБКА МЕТОДУ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМ ТА МЕТОДУ ОЦІНЮВАННЯ ВПЛИВУ ІНЦИДЕНТІВ НА РІВЕНЬ ЗАХИЩЕНОСТІ ІКС

2.1. Метод оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур

У роботах [1-2] запропоновано метод оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур (ВКІ). Зазначений метод розроблено з урахуванням результатів, наведених у [3-14], а також проведеного в підрозділі 1.2 аналізу підходів до оцінювання функціонування систем. Розроблений метод передбачає послідовне виконання п’яти етапів, що узагальнено представлені у вигляді структурної схеми (рис. 2.1).

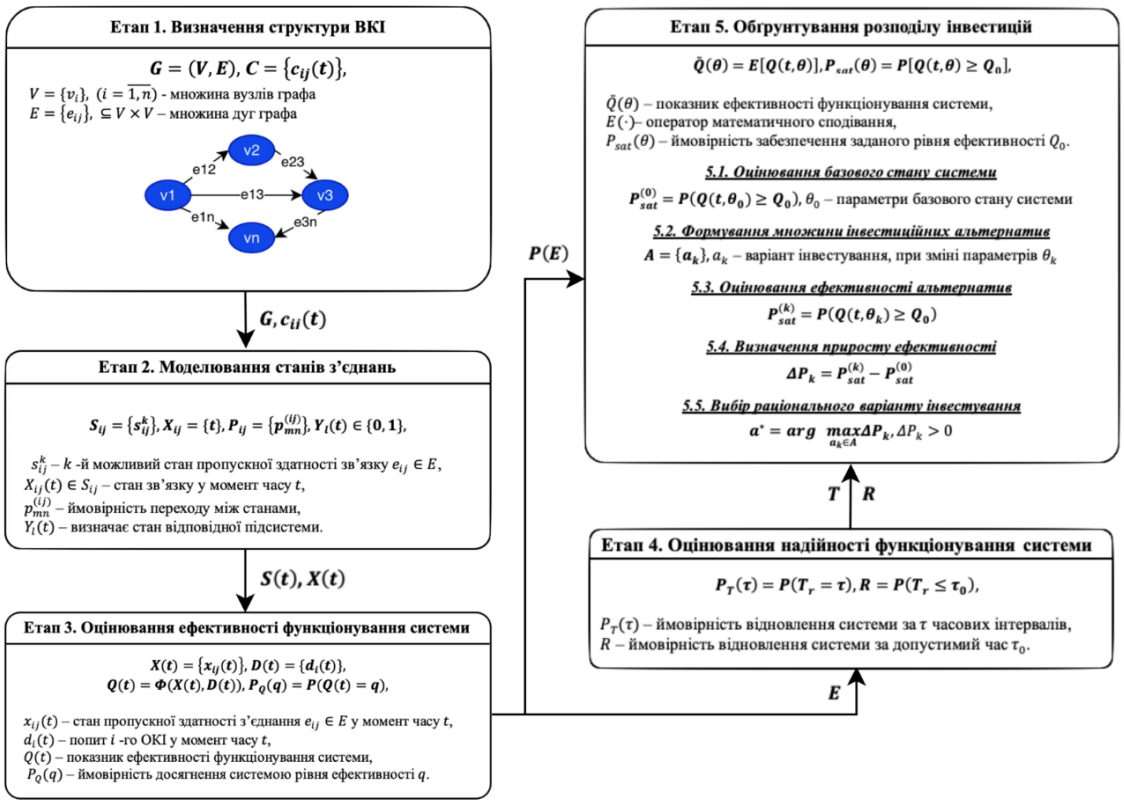

Рис. 2.1. Схема реалізації методу оцінювання ефективності функціонування систем безпеки ВКІ

Розглянемо детально кожен з етапів реалізації запропонованого методу.

Етап 1. Визначення структури ВКІ

Для формалізації структури ВКІ введемо орієнтований граф у наступному вигляді:

$$G = (V, E), \tag{2.1}$$

де $V = \{v_i\}, (i = \overline{1,n})$ – множина вузлів графа, що відповідають ОКІ, $E = \{e_{ij}\}, \subseteq V \times V$ – множина дуг графа, що відображають зв'язки між ОКІ.

Для врахування характеристик зв'язків введемо множину:

$$C = \{c_{ij}(t)\}, \tag{2.2}$$

де $c_{ij}(t)$ – пропускна здатність зв'язку між об'єктами v_i та v_j у момент часу t.

Етап 2. Моделювання станів з'єднань

Для опису зміни станів з'єднань у часі введемо множину станів:

$$S_{ij} = \{s_{ij}^k\}, \tag{2.3}$$

де s_{ij}^k – k-й можливий стан пропускної здатності зв'язку $e_{ij} \in E$.

Зміну станів зв'язків у часі опишемо стохастичним процесом:

$$X_{ij} = \{t\}, \tag{2.4}$$

де $X_{ij}(t) \in S_{ij}$ – стан зв'язку у момент часу t.

Процес $X_{ij}(t)$ описується як марківський або напівмарківський процес [1-2, 14] із матрицею переходів:

$$P_{ij} = \{p_{mn}^{(ij)}\}, \tag{2.5}$$

де $p_{mn}^{(ij)}$ – ймовірність переходу між станами.

Для врахування впливу системи керування введемо випадкову величину:

$$Y_l(t) \in \{0,1\}, \tag{2.6}$$

де $Y_l(t)$ – визначає стан відповідної підсистеми SCADA, що визначає залежність станів з'єднань, які обслуговуються відповідною підсистемою [6-7].

Стан з'єднань визначається значенням відповідної випадкової величини $Y_l(t)$, що відображає вплив підсистеми керування та їх взаємозалежність.

Етап 3. Оцінювання ефективності функціонування системи

Для оцінювання ефективності функціонування системи введемо множину станів з'єднань у момент часу t у такому вигляді:

$$X(t) = \{x_{ij}(t)\}, \tag{2.7}$$

де $x_{ij}(t)$ – стан пропускної здатності з'єднання $e_{ij} \in E$ у момент часу t.

Для опису потреб ОКІ введемо множину:

$$D(t) = \{d_i(t)\}, \tag{2.8}$$

де $d_i(t)$ – попит i-го ОКІ у момент часу t.

Показники ефективності функціонування системи визначимо у вигляді:

$$Q(t) = \Phi\big(X(t), D(t)\big), \tag{2.9}$$

де $Q(t)$ – показники ефективності функціонування системи, $\Phi(\cdot)$ – функція оцінювання, що відображає ступінь задоволення попиту за наявного стану з'єднань, визначається на основі задачі потокового розподілу ресурсів.

Імовірнісне оцінювання ефективності функціонування системи здійснюється на основі розподілу:

$$P_Q(q) = P\big(Q(t) = q\big), \tag{2.10}$$

де $P_Q(q)$ – ймовірність досягнення системою рівня ефективності q.

Оцінювання показника $Q(t)$ виконується шляхом імітаційного моделювання реалізацій стохастичних процесів станів з'єднань, що дозволяє визначити ймовірнісні характеристики ефективності функціонування системи.

Етап 4. Оцінювання надійності функціонування системи

Для оцінювання надійності функціонування системи введемо випадкову величину T_r, де T_r – кількість часових інтервалів, необхідних для переходу системи зі стану зниженого функціонування до стану, за якого забезпечується виконання заданих вимог.

Імовірнісні характеристики надійності визначаються на основі розподілу ймовірностей часу відновлення:

$$P_T(\tau) = P\big(T_r = \tau\big), \tag{2.11}$$

де $P_T(\tau)$ – ймовірність відновлення системи за τ часових інтервалів.

Для інтегрального оцінювання надійності введемо показник:

$$R = P\big(T_r \le \tau_0\big), \tag{2.12}$$

де R – ймовірність відновлення системи за допустимий час τ_0.

Оцінювання показників T_r та R здійснюється шляхом імітаційного моделювання процесів зміни станів з'єднань, що дозволяє визначити здатність системи до відновлення та забезпечення заданого рівня її функціонування.

Етап 5. Обґрунтування розподілу інвестицій

Інвестиційні можливості, що впливають на ефективність функціонування системи, представимо у вигляді змін параметрів стохастичних процесів станів з'єднань, зокрема матриць переходів марківських та напівмарківських процесів [3, 5, 14].

Нехай показник ефективності функціонування системи визначається як:

$$\bar{Q}(\theta) = \mathrm{E}\left[Q(t,\theta)\right], \tag{2.13}$$

де θ – параметри системи, що визначаються вибором інвестицій, $\bar{Q}(\theta)$ – показники ефективності функціонування системи, $\mathrm{E}(\cdot)$ – оператор математичного сподівання.

Для оцінювання ефективності інвестицій використаємо показник:

$$P_{sat}(\theta) = P\left[Q(t,\theta) \geq Q_0\right], \tag{2.14}$$

де $P_{sat}(\theta)$ – ймовірність забезпечення заданого рівня ефективності Q_0.

Обґрунтування розподілу інвестицій здійснюється за наступною процедурою і складається з чотирьох кроків:

Крок 5.1. Оцінювання базового стану системи

Виконується імітаційне моделювання базового стану системи та визначається значення показника $P_{sat}^{(0)}$.

$$P_{sat}^{(0)} = P\left(Q(t,\theta_0) \geq Q_0\right), \tag{2.15}$$

де θ_0 – параметри базового стану системи.

Крок 5.2. Формування множини інвестиційних альтернатив

Формується множина допустимих інвестиційних альтернатив:

$$A = \left\{a_k\right\}, \tag{2.16}$$

де a_k – варіант інвестування, що відповідає зміні параметрів θ_k.

Крок 5.3. Оцінювання ефективності альтернатив

Для кожної альтернативи $a_k \in A$ виконується моделювання зміненого стану системи та визначається значення показника:

$$P_{sat}^{(k)} = P\left(Q(t,\theta_k) \geq Q_0\right). \tag{2.17}$$

Крок 5.4. Визначення приросту ефективності

Для кожної альтернативи $a_k \in A$ визначається приріст ефективності:

$$\Delta P_k = P_{sat}^{(k)} - P_{sat}^{(0)}. \tag{2.18}$$

Крок 5.5. Вибір раціонального варіанту інвестування

Раціональний варіант інвестування визначається як альтернатива, що забезпечує максимальний приріст ефективності функціонування системи:

$$a^* = \arg\max_{a_k \in A} \Delta P_k, \tag{2.19}$$

за умови $\Delta P_k > 0,$ та за умови дотримання бюджетних обмежень.

У разі відсутності альтернатив із додатним приростом ефективності процес завершується.

Таким чином, удосконалено метод оцінювання ефективності функціонування систем безпеки ВКІ, який забезпечує оцінювання ймовірнісних характеристик функціонування системи та обґрунтування розподілу інвестицій у забезпечення безпеки ОКІ.

2.2. Метод оцінювання впливу інцидентів на рівень захищеності ІКС

У роботах [15-16] запропоновано метод оцінювання впливу інцидентів на рівень захищеності ІКС. Зазначений метод розроблено з урахуванням результатів, наведених у [17-27], а також проведеного в підрозділі 1.3 аналізу підходів до оцінювання впливу інцидентів на ІКС.

Розроблений метод передбачає послідовне виконання таких етапів: 1. Формування множини інцидентів ІКС; 2. Визначення критеріїв впливу інцидентів на систему; 3. Оцінювання вагових коефіцієнтів критеріїв та інцидентів; 4. Оцінювання впливу інцидентів на інтегральний показник захищеності; 5. Інтегральне оцінювання рівня захищеності системи.

Узагальнену схему реалізації методу наведено на рис. 2.2.

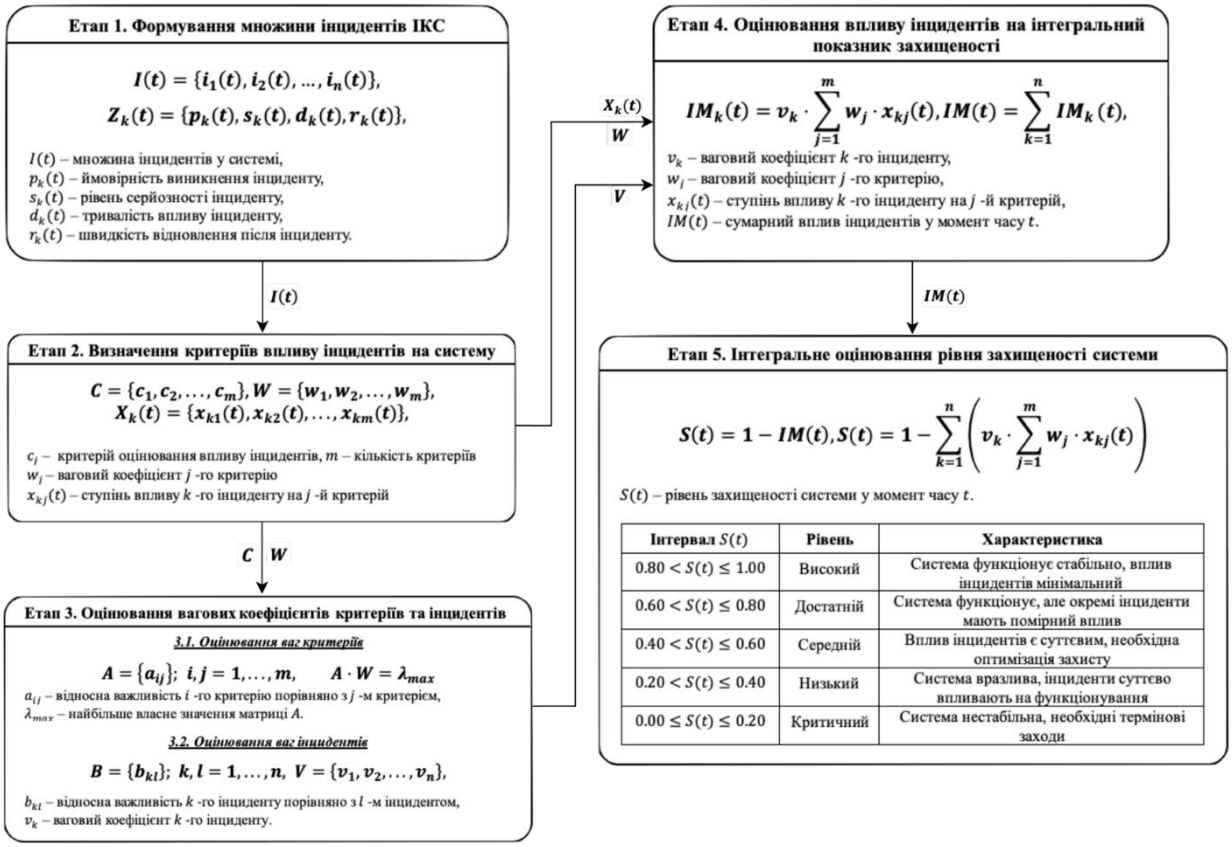

Рис. 2.2. Схема реалізації методу оцінювання впливу інцидентів на рівень захищеності ІКС

Розглянемо детально кожен з етапів реалізації запропонованого методу.

Етап 1. Формування множини інцидентів ІКС

Для формалізації процесу оцінювання впливу інцидентів на рівень захищеності ІКС КІ введемо множину інцидентів у момент часу t у вигляді:

$$I(t) = \{i_1(t), i_2(t), ..., i_n(t)\}, \quad (2.20)$$

де $I(t)$ – множина інцидентів у системі, $i_k(t)$ – k-й інцидент, що виникає в системі у момент часу t, n – кількість інцидентів.

Для врахування характеристик інцидентів введемо множину параметрів:

$$Z_k(t) = \{p_k(t), s_k(t), d_k(t), r_k(t)\}, \quad (2.21)$$

де $p_k(t)$ – ймовірність виникнення інциденту, $s_k(t)$ – рівень серйозності інциденту, $d_k(t)$ – тривалість впливу інциденту, $r_k(t)$ – швидкість відновлення після інциденту.

Отримане подання дозволяє формалізувати множину інцидентів та врахувати їх основні характеристики, що є основою для подальшого оцінювання впливу інцидентів на рівень захищеності системи [15-16].

Етап 2. Визначення критеріїв впливу інцидентів на систему

Для оцінювання впливу інцидентів на рівень захищеності ІКС введемо множину критеріїв:

$$C = \{c_1, c_2, ..., c_m\}, \quad (2.22)$$

де c_j – j-й критерій оцінювання впливу інцидентів, m – кількість критеріїв.

У межах дослідження як основні критерії обрано: конфіденційність, цілісність, доступність, стійкість системи.

Для врахування різної важливості критеріїв введемо вектор вагових коефіцієнтів:

$$W = \{w_1, w_2, ..., w_m\}, \quad (2.23)$$

де w_j – ваговий коефіцієнт j-го критерію, причому виконується умова нормування $\sum_{j=1}^{m} w_j = 1$.

Для кожного інциденту $i_k(t)$ введемо вектор впливу на критерії:

$$X_k(t) = \{x_{k1}(t), x_{k2}(t), ..., x_{km}(t)\}, \quad (2.24)$$

де $x_{kj}(t)$ – ступінь впливу k-го інциденту на j-й критерій.

Отримане подання дозволяє формалізувати систему критеріїв оцінювання та кількісно врахувати вплив кожного інциденту на основні характеристики функціонування системи, що є основою для подальшого визначення інтегрального показника її захищеності.

Етап 3. Оцінювання вагових коефіцієнтів критеріїв та інцидентів

Для врахування різної важливості критеріїв та інцидентів введемо вагові коефіцієнти, які визначаються на основі методу попарних порівнянь [21-22].

Крок 3.1. Оцінювання ваг критеріїв

Для визначення вагових коефіцієнтів критеріїв сформуємо матрицю попарних порівнянь:

$$A = \{a_{ij}\}; i, j = 1, ..., m, \quad (2.25)$$

де a_{ij} – відносна важливість i-го критерію порівняно з j-м критерієм.

Вагові коефіцієнти критеріїв визначаються методом попарних порівнянь. Отриманий вектор ваг задовольняє умову:

$$A \cdot W = \lambda_{\max} W, \quad (2.26)$$

де $\lambda_{\max}$ – найбільше власне значення матриці A.

Крок 3.2. Оцінювання ваг інцидентів

Аналогічно введемо матрицю попарних порівнянь інцидентів:

$$B = \{b_{kl}\}; k,l = 1,...,n, \tag{2.27}$$

де b_{kl} – відносна важливість k-го інциденту порівняно з l-м інцидентом.

Вектор ваг інцидентів визначається методом попарних порівнянь аналогічно до (2.26):

$$V = \{v_1, v_2, ..., v_n\}, \tag{2.28}$$

де v_k – ваговий коефіцієнт k-го інциденту.

Отримані вагові коефіцієнти дозволяють врахувати відносну важливість критеріїв та інцидентів і використовуються на наступних етапах для оцінювання їх впливу на інтегральний показник захищеності системи.

Етап 4. Оцінювання впливу інцидентів на інтегральний показник захищеності

Для кількісного оцінювання впливу інцидентів на рівень захищеності системи визначимо інтегральний вплив кожного інциденту з урахуванням його характеристик та вагових коефіцієнтів критеріїв.

Інтегральний вплив k-го інциденту визначається як:

$$IM_k(t) = v_k \cdot \sum_{j=1}^{m} w_j \cdot x_{kj}(t), \tag{2.29}$$

де v_k – ваговий коефіцієнт k-го інциденту, w_j – ваговий коефіцієнт j-го критерію, $x_{kj}(t)$ – ступінь впливу k-го інциденту на j-й критерій.

Сукупний вплив усіх інцидентів на систему визначається як:

$$IM(t) = \sum_{k=1}^{n} IM_k(t), \tag{2.30}$$

де $IM(t)$ – сумарний вплив інцидентів у момент часу t.

Отримані значення дозволяють кількісно врахувати вплив інцидентів на систему з урахуванням їх важливості та ступеня впливу на ключові критерії функціонування.

Етап 5. Інтегральне оцінювання рівня захищеності системи

Для оцінювання загального стану ІКС КІ введемо інтегральний показник захищеності, який враховує сукупний вплив інцидентів.

Інтегральний показник захищеності системи визначається як:

$$S(t) = 1 - IM(t), \tag{2.31}$$

де $S(t)$ – рівень захищеності системи у момент часу t, $I(t)$ – сумарний вплив інцидентів, визначений за (2.30).

З урахуванням (2.29-2.30), показник захищеності можна подати у розгорнутому вигляді:

$$S(t) = 1 - \sum_{k=1}^{n} \left(v_k \cdot \sum_{j=1}^{m} w_j \cdot x_{kj}(t) \right). \tag{2.32}$$

Отримане значення $S(t)$ належить інтервалу: $0 \le S(t) \le 1$, де значення, близькі до 1, відповідають високому рівню захищеності системи, а значення, близькі до 0, – критичному стану.

Крім того, для інтерпретації результатів інтегрального показника захищеності $S(t)$ використовується шкала рівнів захищеності, сформована з урахуванням існуючих підходів до оцінювання стану захищеності ОКІ та адаптована до запропонованого методу (табл. 2.1).

Таблиця 2.1

Шкала оцінювання інтегрального показника рівня захищеності ІКС

Інтервал $S(t)$	**Рівень**	**Характеристика**
$0.80 < S(t) \leq 1.00$	Високий	Система функціонує стабільно, вплив інцидентів мінімальний
$0.60 < S(t) \leq 0.80$	Достатній	Система функціонує, але окремі інциденти мають помірний вплив
$0.40 < S(t) \leq 0.60$	Середній	Вплив інцидентів є суттєвим, необхідна оптимізація захисту
$0.20 < S(t) \leq 0.40$	Низький	Система вразлива, інциденти суттєво впливають на функціонування
$0.00 \leq S(t) \leq 0.20$	Критичний	Система нестабільна, необхідні термінові заходи

Отриманий інтегральний показник захищеності дозволяє не лише кількісно оцінити загальний стан функціонування ІКС з урахуванням впливу інцидентів, але й здійснити його якісну інтерпретацію на основі запропонованої шкали рівнів захищеності.

Це забезпечує можливість виявлення критичних станів системи, оцінювання ступеня її вразливості та обґрунтованого прийняття управлінських рішень щодо підвищення рівня її захищеності.

Таким чином, удосконалено метод оцінювання впливу інцидентів на рівень захищеності ІКС КІ, який дозволяє кількісно враховувати вплив інцидентів на інтегральний показник захищеності та оцінювати загальний стан функціонування системи.

Методика оцінювання впливу інцидентів на рівень захищеності ІКС

На основі розробленого методу оцінювання впливу інцидентів на рівень захищеності ІКС було створено методику (рис. 2.3), що дозволяє враховувати їх наслідки при прийнятті рішень щодо управління функціонуванням ІКС.

Методика складається з наступних кроків:

1) Формування множини інцидентів $I(t)$

Формування множини інцидентів ІКС $I(t)$ згідно до (2.20) та опис характеристик інцидентів за допомогою множини параметрів $Z_k(t)$ згідно (2.21.)

2) Визначення критеріїв впливу

Визначення множини критеріїв оцінювання впливу інцидентів C відповідно до (2.22), формування вектора вагових коефіцієнтів критеріїв W відповідно до (2.23) з урахуванням умови нормування, а також визначення векторів впливу інцидентів на критерії $X_k(t)$ відповідно до (2.24).

3) Оцінювання ваг інцидентів та критеріїв

Оцінювання вагових коефіцієнтів критеріїв та інцидентів на основі методу попарних порівнянь: формування матриці попарних порівнянь критеріїв A відповідно до (2.25) та визначення вектора їх ваг W відповідно до (2.26), а також формування матриці попарних порівнянь інцидентів B відповідно до (2.27) і визначення вектора їх ваг V відповідно до (2.28).

4) Розрахунок впливу інцидентів

Оцінювання впливу інцидентів на інтегральний показник захищеності: визначення інтегрального впливу кожного інциденту $IM_k(t)$ з урахуванням вагових коефіцієнтів інцидентів, критеріїв та ступеня їх впливу відповідно до (2.29), а також обчислення сумарного впливу інцидентів на систему $IM(t)$ відповідно до (2.30).

5) Інтегральна оцінка захищеності

Інтегральне оцінювання рівня захищеності системи: визначення інтегрального показника захищеності $S(t)$ відповідно до (2.32) та інтерпретація отриманих значень за шкалою рівнів захищеності (табл. 2.1).

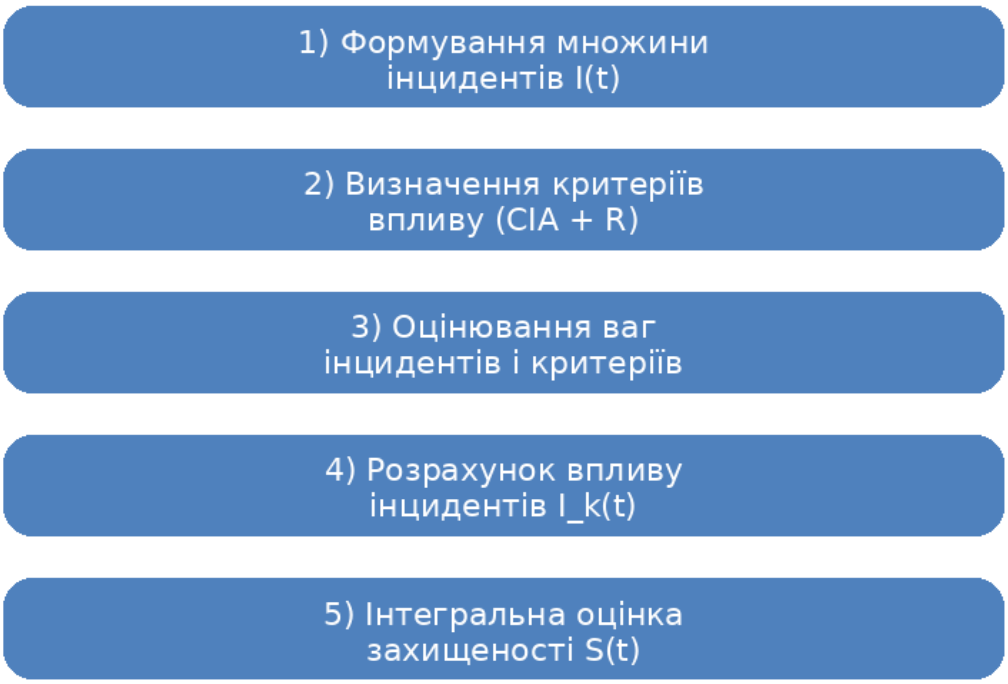

Рис. 2.3. Методика оцінювання впливу інцидентів на рівень захищеності ІКС

Запропонована методика забезпечує оцінювання впливу інцидентів та врахування їх наслідків при прийнятті рішень щодо управління функціонуванням ІКС.

2.3. Висновки до другого розділу

Удосконалено метод оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур, за рахунок використання графового подання взаємозалежностей об’єктів, марківських і напівмарківських процесів моделювання станів, забезпечує оцінювання

ймовірнісних характеристик функціонування системи та обґрунтування розподілу інвестицій у забезпечення безпеки об’єктів критичної інфраструктури.

Удосконалено метод оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем критичної інфраструктури, який за рахунок формалізації взаємозв’язку між характеристиками інцидентів та параметрами стану системи, а також використання вагових коефіцієнтів їх впливу, дозволяє кількісно враховувати вплив інцидентів на інтегральний показник захищеності та оцінювати загальний стан функціонування системи.

На основі запропонованого методу розроблено методику, яка забезпечує оцінювання впливу інцидентів та врахування їх наслідків при прийнятті рішень щодо управління функціонуванням ІКС.

2.4. Список літератури до другого розділу

1. Гнатюк С.О., Сидоренко В.М., Березовий І.Р., Сидоренко С.Ю., Тараненко К.О. Модель оцінювання ефективності функціонування систем інформаційної безпеки взаємозалежних критичних інфраструктур. Проблеми інформатизації та управління. 2022. Т. 4. № 72. С. 17-25. DOI: https://doi.org/10.18372/2073-4751.72.17457.

2. Lutskyi M., Sydorenko V., Polozhentsev A., Apenko N., Sydorenko S. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures. CEUR Workshop Proceedings. 2023. Vol. 3421. P. 214-222. URL: https://ceur-ws.org/Vol-3421/short7.pdf

3. Boyer S. A. SCADA: Supervisory Control and Data Acquisition. 4th ed. USA: ISA – International Society of Automation, 2010. 179 p.

4. Abbas H. A., Mohamed A. M. Review in the design of web-based SCADA systems based on OPC DA protocol. International Journal of Computer Networks. 2011. Vol. 2, No. 6. P. 266–277.

5. Nozick L., Turnquist M., Jones D., Davis J., Lawton C. Assessing the Performance of Interdependent Infrastructures and Optimizing Investment. Proceedings of the 37th Hawaii International Conference on System Sciences. 2004.

6. Xu N., Nozick L. K., Turnquist M. A., Jones D. A. Optimizing Investment for Recovery in Interdependent Infrastructure. Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). Waikoloa, HI, USA, 2007. P. 112–112. DOI: 10.1109/HICSS.2007.413.

7. Limnios N., Oprisan G. Semi-Markov Processes and Reliability. Boston: Birkhäuser, 2001.

8. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об'єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління. 2024. Т. 2. №78. С. 104-114. DOI: https://doi.org/10.18372/2073-4751.78.18967.

9. Gnatyuk S., Sydorenko V., Polozhentsev A., Sydorenko S. Experimental Study of the Method for Cyber Incidents Management in Aviation Critical Infrastructure. In: Ostroumov, I., Marais, K., Zaliskyi, M. (eds) Advances in Civil Aviation Systems Development. ACASD 2025. Lecture Notes in Networks and Systems, Vol. 1418. P. 74–91, Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-91992-3_6.

10. Mokhor, V. V., Honchar, S. F. Evaluation of risks of cyber security of information systems of objects of critical infrastructure. Elektronnoe Modelirovanie. 2019. Vol. 41, No. 6. P. 65–76. DOI: 10.15407/emodel.41.06.065.

11. Качинський А. Б., Варичева Д. І., Свириденко С. В. Ефективне управління ІТ-інцидентами в критичній інформаційній інфраструктурі. Інформація і право. 2016. № 2(17). С. 114–126.

12. Sysoienko, S., Babenko, V., Lada, N. Information security incident management at critical infrastructure facilities. Herald of Khmelnytskyi National University. Technical Sciences. 2025. No. 4. P. 555–559.

13. Jablanski, D. Method for Determining the State of Protection of Critical Information Infrastructure Objects from IT Risks. 2023. URL: https://www.researchcybersecurity.com/state-protection-method/.

14. Kröger, W., Zio, E. Vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety. 2011. Vol. 96, No. 6. P. 637-645.

15. Panteli, M., Mancarella, P. The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. IEEE Power & Energy Magazine. 2015. Vol. 13, No. 3. P. 58–66.

16. Papastergiou, S., Mouratidis, H., Kalogeraki, E.-M., Vidalis, S., Kolokotronis, N. Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE). arXiv. 2020. DOI: https://doi.org/10.48550/arXiv.2003.05720.

17. Behl, A., Behl, K., Rao, S. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2022. 240 p.

18. Король О. Г., Огурцова К. В., Євсеєв С. П. Оцінка ризику реалізації загроз безпеки у телекомунікаційних системах. Автоматика, телемеханіка, зв'язок. Збірник наукових праць ДонІЗТ. 2013. № 36. С. 55–63.

19. Anuar N., Furnell S., Papadaki M., Clarke N. A Risk Index Model for Security Incident Prioritisation. Proceedings of the 9th Australian Information Security Management Conference (AISM). Perth, Australia, 2011. P. 25–39.

20. Mahmood Y., Abid M., Javaid N., Razzaq S. A Response Cost Model for Advanced Metering Infrastructures. International Journal of Distributed Sensor Networks. 2015. Vol. 11, No. 6. Article ID 457021. DOI: 10.1155/2015/457021.

21. Nosal K., Solecka K. Application of AHP Method for Multi-Criteria Evaluation of Variants of the Integration of Urban Public Transport. Transportation Research Procedia. 2014. Vol. 3. P. 269–278. DOI: 10.1016/j.trpro.2014.10.006.

22. Saaty T. L. Decision Making with the Analytic Hierarchy Process. International Journal of Services Sciences. 2008. Vol. 1, No. 1. P. 83–98. DOI: 10.1504/IJSSCI.2008.017590.

РОЗДІЛ 3
РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ДЕРЖАВИ

3.1. Метод підвищення рівня захищеності критичних інформаційних систем держави

У роботі [1] запропоновано метод підвищення рівня захищеності критичних інформаційних систем (КІС), призначений для комплексного оцінювання стану системи, прогнозування впливу загроз і оптимізації стратегій підвищення її стійкості в умовах обмежених ресурсів. Зазначений метод розроблено з урахуванням результатів аналізу підходів до оцінювання рівня захищеності КІС [2-13].

Проведений у підрозділі 1.4 аналіз підходів до підвищення рівня захищеності показав, що існуючі рішення переважно зосереджені на окремих складових, зокрема оцінюванні ризику, надійності та стійкості, і не забезпечують їх комплексного поєднання та оптимізації стратегій захисту. Це обумовлює доцільність розроблення методу, який передбачає інтегроване врахування зазначених характеристик при оцінюванні стану системи.

Математичний опис розробленого методу, з урахуванням положень [9-13], реалізується шляхом послідовного виконання таких етапів (рис. 3.1):

1) Визначення множини потенційних загроз КІС.

2) Визначення множини сценаріїв, що характеризують потенційні загрози певної КІС.

3) Оцінка ризиків елемента КІС.

4) Оцінка надійності елемента КІС.

5) Оцінка стійкості елемента КІС.

6) Інтегральна оцінка рівня захищеності КІС.

7) Оптимізація стратегій захищеності КІС.

8) Оцінка ефекту підвищення захищеності КІС.

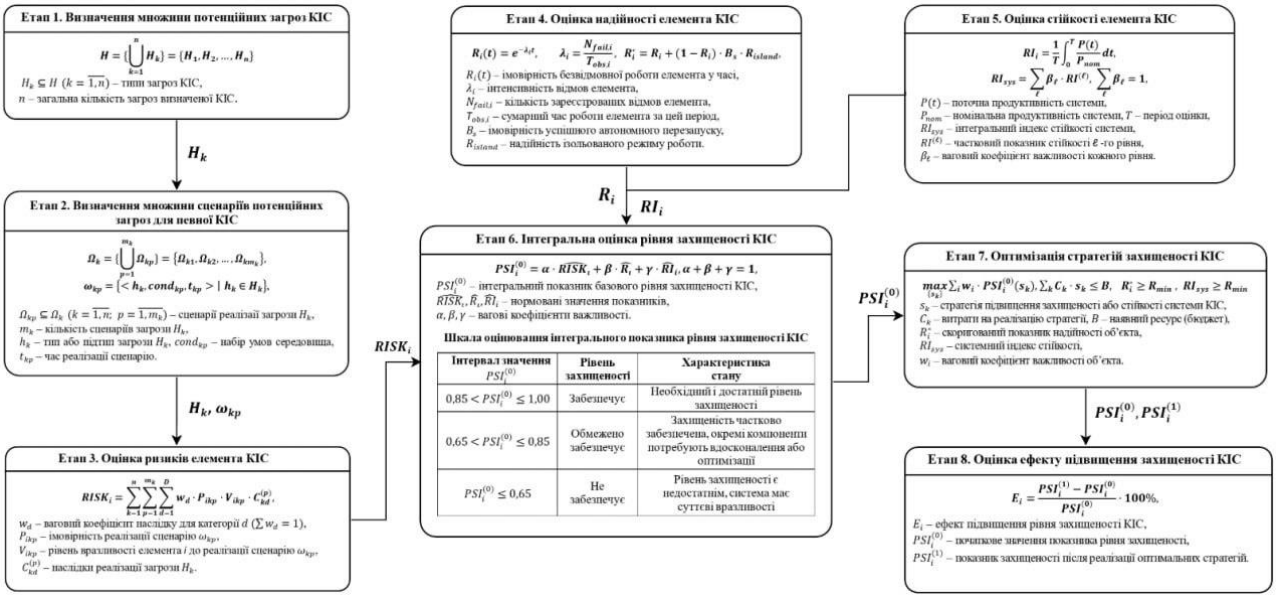

Рис. 3.1. Схема реалізації методу підвищення рівня захищеності КІС

Розглянемо детально кожен з етапів реалізації запропонованого методу.

Етап 1. Визначення множини потенційних загроз КІС

Для визначення загального переліку потенційних загроз КІС введемо множину $\mathbf{H}$ у наступному вигляді:

$$\mathbf{H} = \{\bigcup_{k=1}^{n} H_k\} = \{H_1, H_2, \ldots, H_n\}, \tag{3.1}$$

де $H_k \subseteq \mathbf{H}\ (k = \overline{1,n})$ – типи потенційних загроз КІС, n – загальна кількість потенційних загроз певної КІС.

Етап 2. Визначення множини сценаріїв, що характеризують потенційні загрози певної КІС

Для визначення переліку сценаріїв, що характеризують певну потенційну загрозу H_k, введемо множину $\mathbf{\Omega}_k$ у наступному вигляді:

$$\mathbf{\Omega}_k = \{\bigcup_{p=1}^{m_k} \Omega_{kp}\} = \left\{\Omega_{k1}, \Omega_{k2}, \ldots, \Omega_{km_k}\right\}, \tag{3.2}$$

де $\Omega_{kp} \subseteq \mathbf{\Omega}_k$ $(k = \overline{1,n};\ p = \overline{1,m_k})$ – сценарії, що характеризують певну загрозу H_k, m_k – кількість сценаріїв, певної загрози H_k.

Для представлення сценарію Ω_{kp}, що характеризує реалізацію конкретної загрози H_k, з урахуванням підходу [9], представимо кортеж ω_{kp}, який враховує комбінацію типу загрози, умов середовища та часу її реалізації у наступному вигляді:

$$\omega_{kp} = \left\{< h_k, cond_{kp}, t_{kp} > \middle|\ h_k \in H_k\right\}, \tag{3.3}$$

де h_k – тип або підтип загрози з множини H_k, $cond_{kp}$ – набір умов середовища (наприклад, рівень готовності персоналу, стан інфраструктури, кліматичні умови, інформаційна насиченість), t_{kp} – момент або інтервал часу реалізації сценарію.

Етап 3. Оцінка ризиків елемента КІС

Для забезпечення кількісної інтерпретації можливих наслідків кожної потенційної загрози на елемент КІС, необхідно визначити ризик. У загальному випадку ризик визначається як добуток імовірності реалізації загрози, її вразливості та очікуваних наслідків. Представимо очікуваний рівень втрат від реалізації загрози для кожного елемента КІС у наступному вигляді:

$$RISK_i = \sum_{k=1}^{n} \sum_{p=1}^{m_k} \sum_{d=1}^{D} w_d \cdot P_{ikp} \cdot V_{ikp} \cdot C_{kd}^{(p)}, \tag{3.4}$$

де w_d – ваговий коефіцієнт наслідку для категорії d $\left(\sum w_d = 1\right)$, P_{ikp} – імовірність реалізації сценарію ω_{kp} для елемента i, V_{ikp} – рівень вразливості

елемента i до реалізації сценарію ω_{kp}, $C_{kd}^{(p)}$ – очікувані наслідки реалізації загрози H_k за сценарієм p та категорією наслідку d (соціальні, економічні, екологічні тощо).

Етап 4. Оцінка надійності елемента КІС

Оцінка надійності елемента КІС визначається як ймовірність безвідмовного функціонування елемента КІС протягом заданого часу експлуатації.

Надійність визначеного елемента КІС описується експоненційною залежністю:

$$R_i(t) = e^{-\lambda_i t}, \tag{3.5}$$

де $R_i(t)$ – імовірність безвідмовної роботи елемента i у часі t, λ_i – інтенсивність відмов елемента i [9]. Інтенсивність відмов λ_i визначається згідно з [10] за емпіричними даними або статистикою експлуатації, відповідно до виразу:

$$\lambda_i = \frac{N_{fail,i}}{T_{obs,i}}, \tag{3.6}$$

де $N_{fail,i}$ – кількість зареєстрованих відмов елемента i за період спостереження, $T_{obs,i}$ – сумарний час роботи елемента за цей період.

Слід зазначити, що функція $R_i(t)$ описує експоненційне зниження надійності у процесі старіння або навантаження системи. У випадку наявності резервних або автономних режимів (наприклад, *black start*), можна оцінити розширену надійність елемента, відповідно до [1, 9], у наступному вигляді:

$$R_i^* = R_i + (1 - R_i) \cdot B_s \cdot R_{island}, \tag{3.7}$$

де B_s – імовірність успішного автономного перезапуску, R_{island} – надійність ізольованого режиму роботи.

Етап 5. Оцінка стійкості елемента КІС

Стійкість КІС визначається як її здатність зберігати або швидко відновлювати функціонування після дії дестабілізуючого чинника. Індекс стійкості відображає середню ефективність системи у часі:

$$RI_i = \frac{1}{T}\int_0^T \frac{P(t)}{P_{nom}}dt, \tag{3.8}$$

де $P(t)$ – поточна продуктивність системи, P_{nom} – номінальна продуктивність у нормальному стані, T – період оцінки.

У складних об’єктах КІС (наприклад, енергетичні, транспортні або комунальні мережі) стійкість формується на кількох рівнях – технологічному, інформаційному, організаційному тощо. Тому інтегральний показник стійкості визначається з урахуванням [8], як зважена сума часткових індексів:

$$RI_{sys} = \sum_{\ell} \beta_\ell \cdot RI^{(\ell)}, \sum_{\ell} \beta_\ell = 1, \tag{3.9}$$

де RI_{sys} – інтегральний індекс стійкості всієї системи, $RI^{(\ell)}$ – частковий показник стійкості ℓ-го рівня (наприклад, мережева стійкість енергопостачання, ІТ-інфраструктури, управління тощо), β_ℓ – ваговий коефіцієнт важливості кожного рівня.

Етап 6. Інтегральна оцінка рівня захищеності КІС

На цьому етапі здійснюється об’єднання результатів трьох складових методу – ризику (Risk), надійності (Reliability) та стійкості (Resilience) – у єдиний інтегральний показник рівня захищеності КІС [1, 9]. Для цього використовується нормована лінійна модель:

$$PSI_i^{(0)} = \alpha \cdot RISK_i + \beta \cdot R_i + \gamma \cdot RI_i, \quad \alpha + \beta + \gamma = 1, \qquad (3.10)$$

де $PSI_i^{(0)}$ – інтегральний показник базового рівня захищеності КІС, $RISK_i, R_i, RI_i$ – нормовані значення відповідних показників, α, β, γ – вагові коефіцієнти, що визначають їхню відносну важливість.

Для інтерпретації результатів інтегрального показника $PSI_i^{(0)}$ використовується шкала рівнів захищеності, визначена у Методиці оцінки стану захищеності ОКІ [1, 14], наведена у Табл. 3.1.

Таблиця 3.1

Шкала оцінювання інтегрального показника рівня захищеності КІС

Інтервал значення $PSI_i^{(0)}$	**Рівень захищеності**	**Характеристика стану**
$0,85 < PSI_i^{(0)} \le 1,00$	Забезпечує	Система забезпечує необхідний рівень захищеності, функціонує стабільно, критичних вразливостей не виявлено.
$0,65 < PSI_i^{(0)} \le 0,85$	Обмежено забезпечує	Захищеність частково відповідає вимогам, окремі компоненти потребують вдосконалення або оптимізації стратегій безпеки.
$PSI_i^{(0)} \le 0,65$	Не забезпечує	Рівень захищеності є недостатнім, система має суттєві вразливості; необхідне впровадження додаткових заходів підвищення стійкості.

Як видно з Табл. 3.1, оцінки інтегрального показника рівня захищеності $PSI_i^{(0)}$ варіюються від 0 до 1, що дозволяє класифікувати стан КІС за трьома рівнями забезпеченості – «забезпечує», «обмежено забезпечує» та «не забезпечує» [1, 14].

Етап 7. Оптимізація стратегій захищеності КІС

Для визначення оптимального набору стратегій захищеності та стійкості системи КІС s_k, що забезпечують максимізацію інтегрального показника безпеки при обмежених ресурсах, з урахуванням положень [9, 11], введемо вираз у наступному вигляді:

$$\max_{\{s_k\}} \sum_i w_i \cdot PSI_i^{(0)}(s_k), \text{ за умов } \sum_k C_k \cdot s_k \le B, \;\; R_i^* \ge R_{\min}, \;\; RI_{sys} \ge R_{\min}, \qquad (3.11)$$

де s_k – стратегія підвищення захищеності або стійкості системи КІС, C_k – витрати на реалізацію стратегії, B – наявний ресурс (бюджет), R_i^* – скоригований показник надійності об'єкта, RI_{sys} – системний індекс стійкості, w_i – ваговий коефіцієнт важливості об'єкта.

Етап 8. Оцінка ефекту підвищення захищеності КІС

На цьому етапі визначається ефект підвищення рівня захищеності КІС у результаті реалізації оптимальних стратегій. Оцінювання базується на порівнянні інтегральних показників до та після впровадження заходів, що описується співвідношенням:

$$E_i = \frac{PSI_i^{(1)} - PSI_i^{(0)}}{PSI_i^{(0)}} \cdot 100\%, \qquad (3.12)$$

де E_i – ефект підвищення рівня захищеності КІС, виражений у відсотках, $PSI_i^{(0)}$ – початкове значення інтегрального показника рівня захищеності, визначене за допомогою (3.10), $PSI_i^{(1)}$ – інтегральний показник після реалізації оптимальних стратегій [1].

Отримані значення E_i дозволяють кількісно визначити результативність застосування оптимальних стратегій та підтвердити її ефективність у підвищенні рівня безпеки КІС.

Таким чином, було розроблено метод підвищення рівня захищеності КІС, який дає можливість здійснювати комплексне оцінювання стану системи, прогнозування впливу загроз і оптимізацію стратегій підвищення стійкості в умовах обмежених ресурсів.

3.2. Висновки до третього розділу

Отримав подальшого розвитку метод підвищення рівня захищеності КІС, який завдяки формалізації взаємозв'язків між ризиком, надійністю та стійкістю, використанню інтегрального показника рівня захищеності та врахуванню технічних і організаційних факторів, дає можливість здійснювати комплексне оцінювання стану системи, прогнозування впливу загроз і оптимізацію стратегій підвищення стійкості в умовах обмежених ресурсів.

3.3. Список літератури до третього розділу

1. Сидоренко В. М., Сидоренко С. Ю. Метод підвищення рівня захищеності критичних інформаційних систем держави. Кібербезпека: освіта, наука, техніка. 2025. Т. 2. № 30. С. 500–510. DOI: https://doi.org/10.28925/2663-4023.2025.30.988.

2. Сидоренко В., Максимець А. Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. Кібербезпека: освіта, наука, техніка. 2025. № 3(27). С. 560–571. DOI: https://doi.org/10.28925/2663-4023.2025.27.779.

3. Сидоренко В. (2025). Метод оцінювання стійкості об'єктів критичної інформаційної інфраструктури держави. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 837–853. https://doi.org/10.28925/2663-4023.2025.29.944.

4. Мурасов, Р., Мельник, Я. (2023). Оцінювання захищеності кіберпростору об’єктів критичної інфраструктури України. Сучасні інформаційні технології, (3), 98–112. https://sit.nuou.org.ua/article/view/280288.

5. Суходоля, О. (2022). Стійкість критичної енергетичної інфраструктури та життєдіяльності громад. Аналітична доповідь НІСД, 72 с. https://chtyvo.org.ua/.../Stiikist_krytychnoi_enerhetychnoi_infrastruktury_ta_zhyttiediialnosti_hromad.

6. Шевченко, Н. І., Плахотнюк, Р. В. (2024). Методичні підходи до оцінювання стійкості функціонування об’єктів критичної інфраструктури в умовах особливого періоду функціонування економіки України. Реформування економіки та інноваційні стратегії розвитку, 14(2), 112–126. https://reicst.com.ua/pmtl/article/view/2024-14-02-08.

7. Кириленко, С. П., Тищенко, В. В. (2023). Моделі оцінювання ризиків для критичної інфраструктури в умовах збройного конфлікту. Безпека життєдіяльності, 3(9), 74–88.

8. Третьяков, О. В., Халмурадов, Б. Д., Кічата, Н. М., & Ремська, А. В. (2025). Підхід до кількісної оцінки стійкості об’єктів критичної інфраструктури. Системи управління, навігації та зв’язку, 1(79), 178–183. https://doi.org/10.26906/SUNZ.2025.1.178-183.

9. Mahmood, Y., Afrin, T., Huang, Y., & Yodo, N. (2023). Sustainable development for oil and gas infrastructure from risk, reliability, and resilience perspectives. Sustainability, 15(6), 4953. https://doi.org/10.3390/su15064953.

10. Mohd Safari, M.A., Masseran, N., Abdul Majid, M.H. (2021). Robust and Efficient Reliability Estimation for Exponential Distribution. Computers, Materials & Continua, 69(2), 2807–2824. https://doi.org/10.32604/cmc.2021.018815.

11. Kong, J., Zhang, C., & Simonovic, S. P. (2021). Optimizing the resilience of interdependent infrastructures to regional natural hazards with

combined improvement measures. Reliability Engineering & System Safety, 210, 107538. https://doi.org/10.1016/j.ress.2021.107538.

12. Rehak, D., Flynnova, L., Hromada, M., & Fuggini, C. (2023). The importance of resistance in the context of critical infrastructure resilience: An extension of the CIERA method. Systems, 11(10), 506. https://doi.org/10.3390/systems11100506.

13. Irankunda, G., Zhang, W., Fernand, M., & Zhang, J. (2024). Assessing the Resilience of Critical Infrastructure Facilities toward a Holistic and Theoretical Approach: A Multi-Scenario Evidence and Case Study. Sustainability, 16(20), 8735. https://doi.org/10.3390/su16208735.

14. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. Методика оцінки стану захищеності об'єктів критичної інфраструктури: наказ від 14.01.2025 № 17. URL: https://zakon.rada.gov.ua/laws/show/z0375-25.

РОЗДІЛ 4
ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ МЕТОДІВ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА ЗАХИЩЕНОСТІ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

4.1. Експериментальне дослідження методу оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур

У роботах [1–2] проведено експериментальне дослідження методу оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур (ВКІ). Експериментальна перевірка методу здійснюється відповідно до етапів, наведених у розділі 2.1, і передбачає формування структури ВКІ, моделювання станів їх елементів, оцінювання ефективності та надійності функціонування системи, а також обґрунтування розподілу інвестицій.

У межах експериментального дослідження проведено три верифікації та використано узагальнену модель ВКІ, яка не прив’язана до конкретного галузевого сектору та дозволяє відобразити типові функціональні й інформаційні взаємозв’язки між об’єктами.

Верифікація 1. Базовий сценарій функціонування ВКІ

Для підтвердження можливості використання запропонованого методу оцінювання ефективності функціонування систем безпеки ВКІ розглянемо базовий сценарій функціонування модельної системи, що складається з шести ОКІ та восьми з’єднань між ними.

Етап 1. Визначення структури ВКІ

Відповідно до запропонованого методу, з урахуванням (2.1), структуру ВКІ представимо множину вузлів графа, у вигляді:

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6\},$$

де v_1 – центр обробки даних, v_2 – телекомунікаційний вузол, v_3 – енергетичний об’єкт, v_4 – диспетчерський пункт, v_5 – резервний вузол керування, v_6 – кінцевий об’єкт обслуговування.

Множину дуг графа, що відображають зв’язки між об’єктами, з урахуванням (2.1), подамо у вигляді:

$$E = \{e_{12}, e_{13}, e_{24}, e_{34}, e_{25}, e_{45}, e_{46}, e_{56}\}.$$

Дуги графа відображають функціональні та інформаційні зв’язки між ОКІ, а також їх взаємозалежність.

Структуру ВКІ для Верифікації 1, сформовану з урахуванням загальної моделі (рис. 2.1), наведено на рис. 4.1.

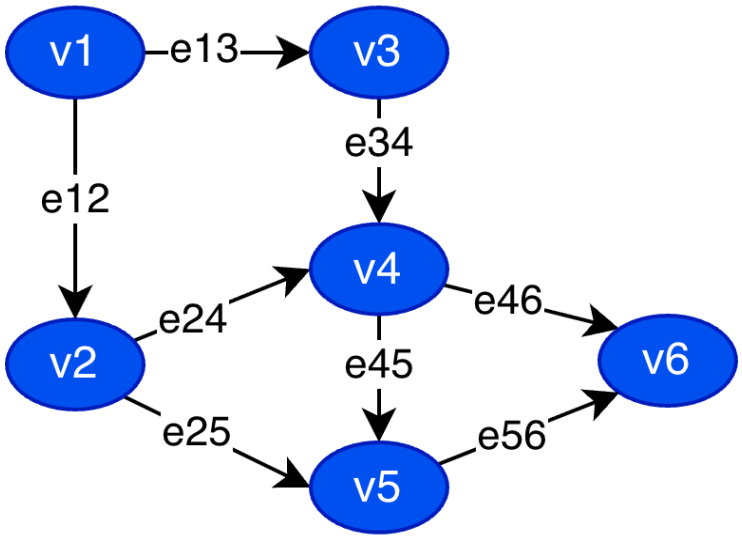

Рис. 4.1. Представлення структури ВКІ для Верифікації 1

Для врахування характеристик зв’язків, відповідно до (2.2), введемо множину пропускних здатностей:

$$C = \{c_{12}(t), c_{13}(t), c_{24}(t), c_{34}(t), c_{25}(t), c_{45}(t), c_{46}(t), c_{56}(t)\}.$$

У базовому сценарії початкові значення пропускних здатностей зв'язків приймемо такими:

$$C_0 = \{90, 80, 100, 85, 75, 95, 90, 70\}.$$

Ці значення відповідають номінальному режиму функціонування системи. Параметри з'єднань у базовому сценарії наведено в табл. 4.1.

Таблиця 4.1

Параметри вузлів та з'єднань ВКІ

№	З'єднання	c_{ij}	Підсистема SCADA
1	e_{12}	90	SCADA 1
2	e_{13}	80	–
3	e_{24}	100	SCADA 1
4	e_{34}	85	SCADA 2
5	e_{25}	75	SCADA 1
6	e_{45}	95	SCADA 2
7	e_{46}	90	SCADA 2
8	e_{56}	70	–

Етап 2. Моделювання станів з'єднань

Для опису зміни станів з'єднань у часі, відповідно до (2.3), для кожного зв'язку введемо множину станів пропускної здатності:

$$S_{ij} = \{s_{ij}^1, s_{ij}^2, s_{ij}^3\},$$

s_{ij}^1 – стан зниженої пропускної здатності, s_{ij}^2 – номінальний стан s_{ij}^3 – стан підвищеної пропускної здатності.

У базовому сценарії значення станів пропускної здатності задаються як відносні відхилення від номінального значення, визначеного на Етапі 1:

$$S_{ij} = \{0.7c_{ij}, c_{ij}, 1.1c_{ij}\},$$

де c_{ij} – номінальна пропускна здатність з'єднання e_{ij}.

З урахуванням (2.4), зміну станів з'єднань у часі представимо стохастичним процесом: $X_{ij}(t), e_{ij} \in E$.

Відповідно до (2.5), процес $X_{ij}(t)$ опишемо марківським процесом [3-5] із матрицею переходів:

$$X_{ij} = \begin{pmatrix} 0.70 & 0.25 & 0.05 \\ 0.15 & 0.70 & 0.15 \\ 0.05 & 0.25 & 0.70 \end{pmatrix}.$$

Зазначена матриця відображає ймовірності переходів між станами зниженої, номінальної та підвищеної пропускної здатності.

Для врахування впливу системи керування, згідно з (2.6), введемо випадкову величину: $Y_l(t) \in \{0,1\}$, де $Y_l(t) = 1$ відповідає нормальному стану підсистеми SCADA, $Y_l(t) = 0$ – це зниженому стану її функціонування [6-7].

У базовому сценарії розглянемо дві підсистеми SCADA:

- підсистема $l = 1$ обслуговує з'єднання e_{12}, e_{24}, e_{25};
- підсистема $l = 2$ обслуговує з'єднання e_{34}, e_{45}, e_{46}.

Імовірності станів підсистем SCADA задамо так:

$$P(Y_1(t) = 1) = 0.92, \; P(Y_1(t) = 0) = 0.08;$$
$$P(Y_2(t) = 1) = 0.90, \; P(Y_1(t) = 0) = 0.10.$$

Це дозволяє врахувати взаємозалежність станів відповідних з'єднань у базовому режимі функціонування.

Параметри станів та процесів наведено в табл. 4.2.

Таблиця 4.2

Параметри стохастичних процесів

З'єднання	**Стани**	**Тип процесу**
e_{12}	{63, 90, 99}	Марківський
e_{13}	{56, 80, 88}	Марківський
e_{24}	{70, 100, 110}	Марківський
e_{34}	{60, 85, 94}	Марківський
e_{25}	{52, 75, 82}	Марківський
e_{45}	{67, 95, 105}	Марківський
e_{46}	{63, 90, 99}	Марківський
e_{56}	{49, 70, 77}	Марківський

Етап 3. Оцінювання ефективності функціонування системи

Для оцінювання ефективності функціонування системи, відповідно до (2.7), множину станів з'єднань у момент часу tподамо у вигляді:

$$X(t) = \{x_{12}(t), x_{13}(t), x_{24}(t), x_{34}(t), x_{25}(t), x_{45}(t), x_{46}(t), x_{56}(t)\}.$$

Для опису потреб ОКІ, з урахуванням (2.8), введемо множину:

$$D(t) = \{d_1(t), d_2(t), d_3(t), d_4(t), d_5(t), d_6(t)\}.$$

У базовому сценарії значення попиту приймемо сталими:

$$D(t) = \{0, 20, 25, 30, 15, 40\}.$$

Для Верифікації 1, відповідно до (2.9-2.10), оцінювання показника $Q(t)$ виконується шляхом імітаційного моделювання 1000 реалізацій по 500 часових інтервалів кожна [3, 8-11].

За результатами імітаційного моделювання визначаються: середнє значення показника ефективності функціонування; розподіл $P_Q(q)$; імовірність забезпечення заданого рівня ефективності. Результати наведено в табл. 4.3.

Таблиця 4.3

Результати оцінювання ефективності

Показник	**Значення**
$\bar{Q}$ Середнє значення	0.82
$Q_{\min}$ Мінімальне значення	0.61
$Q_{\max}$ Максимальне значення	0.93
$P(Q \geq 0.85)$ Ймовірність досягнення заданого рівня	0.47

Результати імітаційного моделювання подано на рис. 4.2.

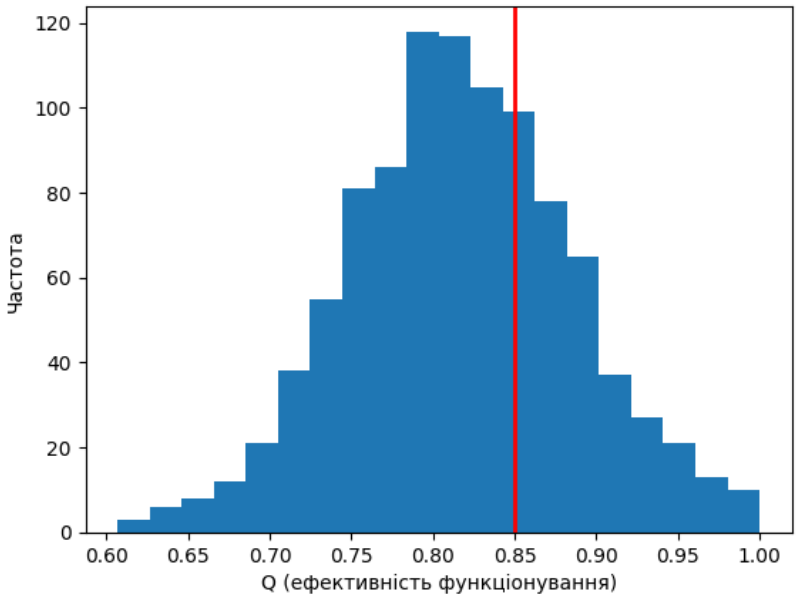

Рис. 4.2. Розподіл ймовірностей ефективності функціонування системи

На рис. 4.2 наведено розподіл ймовірностей ефективності функціонування системи, отриманий за результатами імітаційного моделювання. Вертикальною лінією позначено порогове значення $Q_0 = 0.85,$ що відповідає заданому рівню ефективності. Аналіз розподілу показує, що лише частина реалізацій забезпечує досягнення даного рівня, що підтверджує значення ймовірності $P(Q \geq Q_0) = 0.47,$ отримане в базовому сценарії.

Етап 4. Оцінювання надійності функціонування системи

Імовірнісні характеристики надійності, згідно з (2.11), визначаються на основі розподілу ймовірностей часу відновлення: $P_T(\tau) = P\left(T_r = \tau\right).$

Для інтегрального оцінювання надійності введемо показник показник (2.12): $R = P\left(T_r \leq \tau_0\right),$ де R – ймовірність відновлення системи за допустимий час $\tau_0 = 10$ – допустимий час відновлення системи.

У межах Верифікації 1 шляхом імітаційного моделювання визначаються: середній час відновлення системи; розподіл часу відновлення; імовірність відновлення за допустимий час. Результати оцінювання надійності наведено в табл. 4.4.

Таблиця 4.4

Результати оцінювання надійності

Показник	**Значення**
$\overline{T_r}$ Середній час відновлення	8.6
$T_{r,\min}$ Мінімальний час відновлення	2
$T_{r,\max}$ Максимальний час відновлення	17
$P(Q \geq 0.85)$ Ймовірність відновлення за допустимий час	0.74
R Інтегральний показник надійності	0.74

Етап 5. Обґрунтування розподілу інвестицій

Для Верифікації 1 розглянемо три інвестиційні альтернативи, що впливають на параметри стохастичних процесів станів з'єднань:

$$A = \{a_1, a_2, a_3\},$$

a_1 – інвестування у підвищення надійності з'єднання e_{24};

a_2 – інвестування у підвищення надійності з'єднання e_{45};

a_3 – інвестування у підвищення надійності першої підсистеми SCADA.

Для оцінювання ефективності інвестицій, згідно з (2.14), використовується показник: $Q_0 = 0.85$.

Результати оцінювання інвестиційних альтернатив наведено в табл. 4.5.

Таблиця 4.5

Порівняння інвестиційних альтернатив

Альтернатива	Опис	Вартість	$P_{sat}^{(k)}$	ΔP_k
a_1	Покращення e_{24}	10	0.58	+0.11
a_2	Покращення e_{45}	12	0.62	+0.15
a_3	Покращення SCADA 1	15	0.67	+0.20

З табл. 4.5. видно, що у базовому сценарії ймовірність забезпечення заданого рівня ефективності становить $P_{sat}^{(0)} = 0.47$. Застосування інвестиційних альтернатив дозволяє підвищити даний показник до $P_{sat}^{(k)} = 0.67$, що відповідає приросту ефективності на $\Delta P_k = 20\%$. При цьому встановлено, що найбільший вплив на ефективність функціонування системи має інвестування у підсистеми керування, що підтверджує необхідність врахування взаємозалежностей у ВКІ.

Верифікація 2. Сценарій функціонування ВКІ з альтернативною топологією зв’язків

Для підтвердження можливості використання запропонованого методу оцінювання ефективності функціонування систем безпеки ВКІ розглянемо другий сценарій функціонування модельної системи, що відрізняється від Верифікації 1 топологією взаємозв’язків, також складається з шести ОКІ та семи інших з’єднань між ними.

Етап 1. Визначення структури ВКІ

Відповідно до запропонованого методу, з урахуванням (2.1), структуру ВКІ представимо множину вузлів графа, у вигляді:

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6\},$$

де v_1 – центр обробки даних, v_2 – телекомунікаційний вузол, v_3 – енергетичний об’єкт, v_4 – диспетчерський пункт, v_5 – резервний вузол керування, v_6 – кінцевий об’єкт обслуговування.

Множину дуг графа, що відображають зв’язки між об’єктами, з урахуванням (2.1), подамо у вигляді:

$$E = \{e_{12}, e_{23}, e_{34}, e_{45}, e_{56}, e_{13}, e_{26}\}.$$

Дуги графа відображають функціональні та інформаційні зв’язки між ОКІ, а також їх взаємозалежність.

Структуру ВКІ для Верифікації 2, сформовану з урахуванням загальної моделі (рис. 2.1), наведено на рис. 4.3.

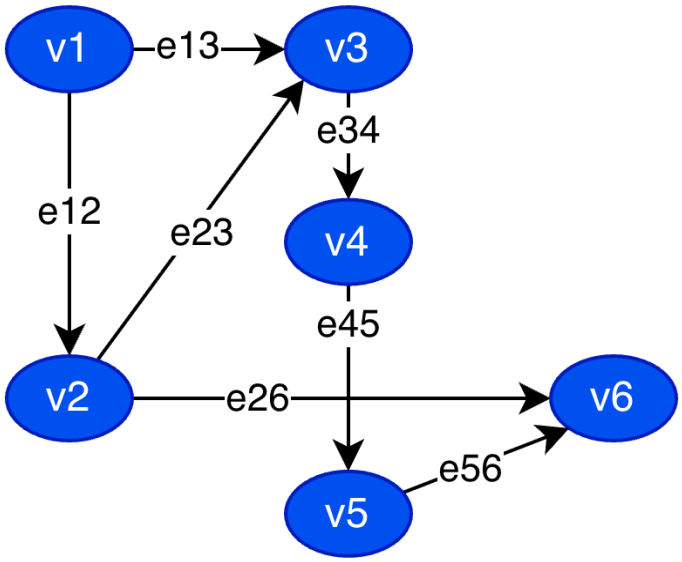

Рис. 4.3. Представлення структури ВКІ для Верифікації 2

Для врахування характеристик зв'язків, відповідно до (2.2), введемо множину пропускних здатностей:

$$C = \{c_{12}(t), c_{23}(t), c_{34}(t), c_{45}(t), c_{56}(t), c_{13}(t), c_{26}(t)\}.$$

У другому сценарії початкові значення пропускних здатностей зв'язків приймемо такими:

$$C_0 = \{85, 75, 90, 80, 70, 65, 95\}.$$

Ці значення відповідають номінальному режиму функціонування системи. Параметри з'єднань у другому сценарії наведено в табл. 4.6.

Таблиця 4.6

Параметри вузлів та з'єднань ВКІ

№	З'єднання	c_{ij}	Підсистема SCADA
1	e_{12}	85	SCADA 1
2	e_{23}	75	SCADA 1
3	e_{34}	90	SCADA 2

4	e_{45}	80	SCADA 2
5	e_{56}	70	SCADA 2
6	e_{13}	65	SCADA 1
7	e_{26}	95	SCADA 2

Етап 2. Моделювання станів з'єднань

Для опису зміни станів з'єднань у часі, відповідно до (2.3), для кожного зв'язку введемо множину станів пропускної здатності:

$$S_{ij} = \left\{ s_{ij}^1, s_{ij}^2, s_{ij}^3 \right\},$$

s_{ij}^1 – стан зниженої пропускної здатності, s_{ij}^2 – номінальний стан s_{ij}^3 – стан підвищеної пропускної здатності.

У другому сценарії значення станів пропускної здатності задаються як відносні відхилення від номінального значення, визначеного на Етапі 1:

$$S_{ij} = \left\{ 0.7c_{ij}, c_{ij}, 1.1c_{ij} \right\},$$

де c_{ij} – номінальна пропускна здатність з'єднання e_{ij}.

З урахуванням (2.4), зміну станів з'єднань у часі представимо стохастичним процесом: $X_{ij}(t), e_{ij} \in E$.

Відповідно до (2.5), процес $X_{ij}(t)$ опишемо марківським процесом [3-5] із матрицею переходів:

$$X_{ij} = \begin{pmatrix} 0.72 & 0.23 & 0.05 \\ 0.18 & 0.67 & 0.15 \\ 0.08 & 0.22 & 0.70 \end{pmatrix}.$$

Зазначена матриця відображає ймовірності переходів між станами зниженої, номінальної та підвищеної пропускної здатності.

Для врахування впливу системи керування, згідно з (2.6), введемо випадкову величину: $Y_l(t) \in \{0,1\}$, де $Y_l(t) = 1$ відповідає нормальному стану підсистеми SCADA, $Y_l(t) = 0$ – це зниженому стану її функціонування [6-7].

У другому сценарії розглянемо дві підсистеми SCADA:

- підсистема $l = 1$ обслуговує з'єднання e_{12}, e_{23}, e_{13};
- підсистема $l = 2$ обслуговує з'єднання $e_{34}, e_{45}, e_{56}, e_{26}$.

Імовірності станів підсистем SCADA задамо так:

$$P(Y_1(t) = 1) = 0.90,\ P(Y_1(t) = 0) = 0.10;$$
$$P(Y_2(t) = 1) = 0.88,\ P(Y_1(t) = 0) = 0.12.$$

Це дозволяє врахувати взаємозалежність станів відповідних з'єднань у другому режимі функціонування.

Параметри станів та процесів наведено в табл. 4.7.

Таблиця 4.7

Параметри стохастичних процесів

З'єднання	**Стани**	**Тип процесу**
e_{12}	{60, 85, 94}	Марківський
e_{23}	{53, 75, 83}	Марківський
e_{34}	{63, 90, 99}	Марківський
e_{45}	{56, 80, 88}	Марківський
e_{56}	{49, 70, 77}	Марківський
e_{13}	{46, 65, 72}	Марківський
e_{26}	{67, 95, 105}	Марківський

Етап 3. Оцінювання ефективності функціонування системи

Для оцінювання ефективності функціонування системи, відповідно до (2.7), множину станів з'єднань у момент часу t подамо у вигляді:

$$X(t) = \{x_{12}(t), x_{23}(t), x_{34}(t), x_{45}(t), x_{56}(t), x_{13}(t), x_{26}(t)\}.$$

Для опису потреб ОКІ, з урахуванням (2.8), введемо множину:

$$D(t) = \{d_1(t), d_2(t), d_3(t), d_4(t), d_5(t), d_6(t)\}.$$

У другому сценарії значення попиту приймемо сталими:

$$D(t) = \{0{,}18, 22, 28, 20, 45\}.$$

Для Верифікації 2, відповідно до (2.9-2.10), оцінювання показника $Q(t)$ виконується шляхом імітаційного моделювання 1000 реалізацій по 500 часових інтервалів кожна [3, 8-11].

За результатами імітаційного моделювання визначаються: середнє значення показника ефективності функціонування; розподіл $P_Q(q)$; імовірність забезпечення заданого рівня ефективності. Результати наведено в табл. 4.8.

Таблиця 4.8

Результати оцінювання ефективності

Показник	**Значення**
$\bar{Q}$ Середнє значення	0.78
$Q_{\min}$ Мінімальне значення	0.55
$Q_{\max}$ Максимальне значення	0.91
$P(Q \geq 0.85)$ Ймовірність досягнення заданого рівня	0.39

Результати імітаційного моделювання подано на рис. 4.4.

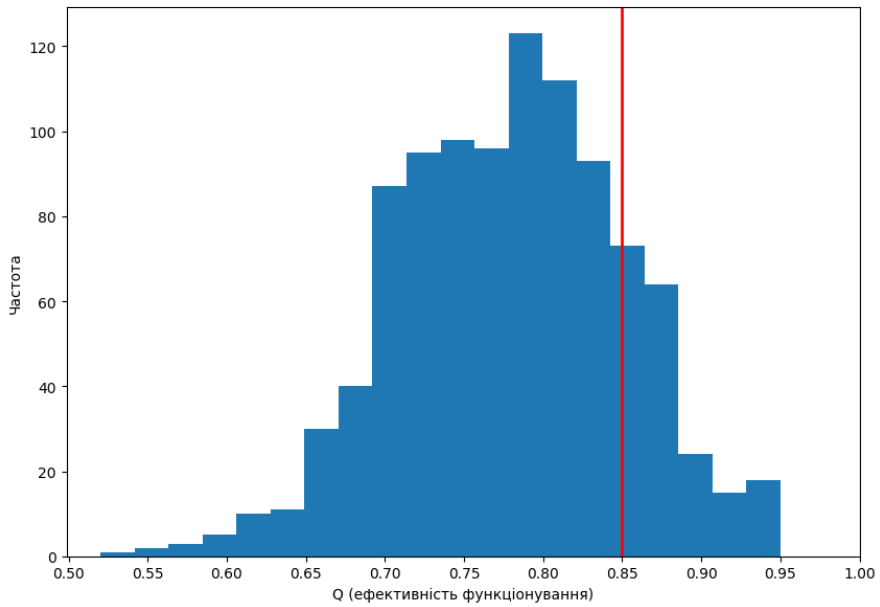

Рис. 4.4. Розподіл ймовірностей ефективності функціонування системи

На рис. 4.4 наведено розподіл ймовірностей ефективності функціонування системи, отриманий за результатами імітаційного моделювання. Вертикальною лінією позначено порогове значення $Q_0 = 0.85$, що відповідає заданому рівню ефективності. Аналіз розподілу показує, що лише частина реалізацій забезпечує досягнення даного рівня, що підтверджує значення ймовірності $P(Q \geq Q_0) = 0.39$, отримане вдругому сценарії.

Етап 4. Оцінювання надійності функціонування системи

Імовірнісні характеристики надійності, згідно з (2.11), визначаються на основі розподілу ймовірностей часу відновлення: $P_T(\tau) = P(T_r = \tau)$.

Для інтегрального оцінювання надійності введемо показник показник (2.12): $R = P(T_r \leq \tau_0)$, де R – ймовірність відновлення системи за допустимий час $\tau_0 = 10$ – допустимий час відновлення системи.

У межах Верифікації 2 шляхом імітаційного моделювання визначаються: середній час відновлення системи; розподіл часу відновлення; імовірність відновлення за допустимий час. Результати оцінювання надійності наведено в табл. 4.9.

Таблиця 4.9

Результати оцінювання надійності

Показник	**Значення**
$\overline{T}_r$ Середній час відновлення	9.8
$T_{r,\min}$ Мінімальний час відновлення	3
$T_{r,\max}$ Максимальний час відновлення	19
$P(Q \geq 0.85)$ Ймовірність відновлення за допустимий час	0.66
R Інтегральний показник надійності	0.66

Етап 5. Обґрунтування розподілу інвестицій

Для Верифікації 2 розглянемо три інвестиційні альтернативи, що впливають на параметри стохастичних процесів станів з'єднань:

$$A = \{a_1, a_2, a_3\},$$

a_1 – інвестування у підвищення надійності з'єднання e_{24};

a_2 – інвестування у підвищення надійності з'єднання e_{45};

a_3 – інвестування у підвищення надійності другої підсистеми SCADA.

Для оцінювання ефективності інвестицій, згідно з (2.14), використовується показник: $Q_0 = 0.85$.

Результати оцінювання інвестиційних альтернатив наведено в табл. 4.10.

Таблиця 4.10

Порівняння інвестиційних альтернатив

Альтернатива	Опис	Вартість	$P_{sat}^{(k)}$	ΔP_k
a_1	Покращення e_{24}	11	0.50	+0.11
a_2	Покращення e_{45}	13	0.54	+0.15
a_3	Покращення SCADA 2	16	0.61	+0.22

З табл. 4.10 видно, що у другому сценарії ймовірність забезпечення заданого рівня ефективності становить $P_{sat}^{()} = 0.39.$ Застосування інвестиційних альтернатив дозволяє підвищити даний показник до $P_{sat}^{(k)} = 0.61,$ що відповідає приросту ефективності на $\Delta P_k = 22\%.$ При цьому встановлено, що найбільший вплив на ефективність функціонування системи має інвестування у другу підсистему SCADA, що підтверджує можливість використання запропонованого методу для різних топологій ВКІ.

Верифікація 3. Сценарій підвищеної ефективності та резервування

Для підтвердження можливості використання запропонованого методу оцінювання ефективності функціонування систем безпеки ВКІ розглянемо третій сценарій функціонування модельної системи, що відрізняється від попередніх наявністю додаткових зв'язків та підвищеним рівнем резервування.

Етап 1. Визначення структури ВКІ

Відповідно до запропонованого методу, з урахуванням (2.1), структуру ВКІ представимо множину вузлів графа, у вигляді:

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6\},$$

де v_1 – центр обробки даних, v_2 – телекомунікаційний вузол, v_3 – енергетичний об'єкт, v_4 – диспетчерський пункт, v_5 – резервний вузол керування, v_6 – кінцевий об'єкт обслуговування.

Множину дуг графа, що відображають зв'язки між об'єктами, з урахуванням (2.1), подамо у вигляді:

$$E = \{e_{12}, e_{23}, e_{34}, e_{45}, e_{56}, e_{13}, e_{26}, e_{15}, e_{36}\}.$$

Дуги графа відображають функціональні та інформаційні зв’язки між ОКІ, а також їх взаємозалежність.

Структуру ВКІ для Верифікації 3, сформовану з урахуванням загальної моделі (рис. 2.1), наведено на рис. 4.5.

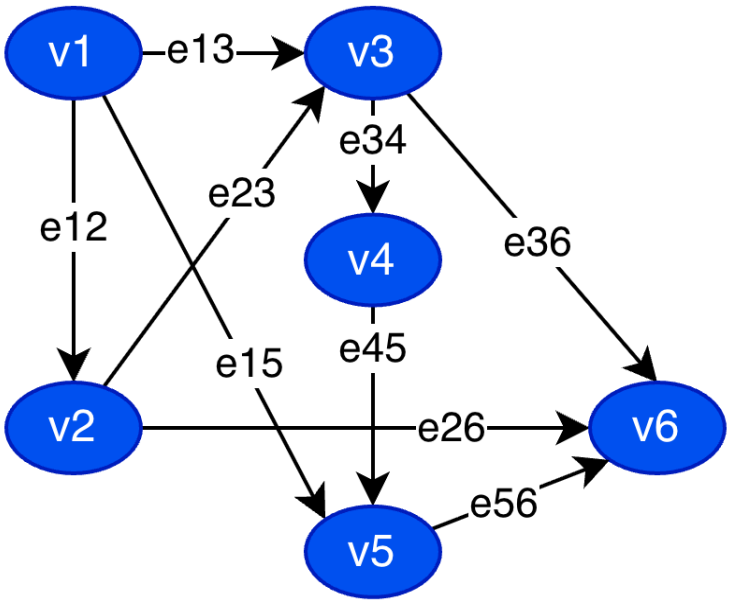

Рис. 4.5. Представлення структури ВКІ для Верифікації 3

Для врахування характеристик зв’язків, відповідно до (2.2), введемо множину пропускних здатностей:

$$C = \{c_{12}(t), c_{23}(t), c_{34}(t), c_{45}(t), c_{56}(t), c_{13}(t), c_{26}(t), c_{15}(t), c_{36}(t)\}.$$

У третьому сценарії початкові значення пропускних здатностей зв’язків приймемо такими:

$$C_0 = \{90, 80, 95, 85, 75, 70, 100, 85, 90\}.$$

Ці значення відповідають номінальному режиму функціонування системи. Параметри з’єднань у другому сценарії наведено в табл. 4.11.

Таблиця 4.11

Параметри вузлів та з'єднань ВКІ

№	З'єднання	c_{ij}	Підсистема SCADA
1	e_{12}	90	SCADA 1
2	e_{23}	80	SCADA 1
3	e_{34}	95	SCADA 2
4	e_{45}	85	SCADA 2
5	e_{56}	75	SCADA 2
6	e_{13}	70	SCADA 1
7	e_{26}	100	SCADA 3
8	e_{15}	85	SCADA 1
9	e_{36}	90	SCADA 2

Етап 2. Моделювання станів з'єднань

Для опису зміни станів з'єднань у часі, відповідно до (2.3), для кожного зв'язку введемо множину станів пропускної здатності:

$$S_{ij} = \left\{ s_{ij}^1, s_{ij}^2, s_{ij}^3 \right\},$$

s_{ij}^1 – стан зниженої пропускної здатності, s_{ij}^2 – номінальний стан s_{ij}^3 – стан підвищеної пропускної здатності.

У третьому сценарії значення станів пропускної здатності задаються як відносні відхилення від номінального значення, визначеного на Етапі 1:

$$S_{ij} = \left\{ 0.8c_{ij}, c_{ij}, 1.15c_{ij} \right\},$$

де c_{ij} – номінальна пропускна здатність з'єднання e_{ij}.

З урахуванням (2.4), зміну станів з'єднань у часі представимо стохастичним процесом: $X_{ij}(t), e_{ij} \in E$.

Відповідно до (2.5), процес $X_{ij}(t)$ опишемо марківським процесом [3-5] із матрицею переходів:

$$X_{ij} = \begin{pmatrix} 0.65 & 0.30 & 0.05 \\ 0.10 & 0.75 & 0.15 \\ 0.05 & 0.20 & 0.75 \end{pmatrix}.$$

Зазначена матриця відображає ймовірності переходів між станами зниженої, номінальної та підвищеної пропускної здатності.

Для врахування впливу системи керування, згідно з (2.6), введемо випадкову величину: $Y_l(t) \in \{0,1\}$, де $Y_l(t) = 1$ відповідає нормальному стану підсистеми SCADA, $Y_l(t) = 0$ – це зниженому стану її функціонування [6-7].

У третьому сценарії розглянемо три підсистеми SCADA:

- підсистема $l = 1$ обслуговує з'єднання $e_{12}, e_{23}, e_{13}, e_{15}$;
- підсистема $l = 2$ обслуговує з'єднання $e_{34}, e_{45}, e_{56}, e_{36}$;
- підсистема $l = 3$ обслуговує з'єднання e_{26}.

Імовірності станів підсистем SCADA задамо так:

$$P(Y_1(t) = 1) = 0.95,\ P(Y_2(t) = 1) = 0.94,\ P(Y_3(t) = 1) = 0.96.$$

Це дозволяє врахувати взаємозалежність станів відповідних з'єднань у третьому режимі функціонування.

Параметри станів та процесів наведено в табл. 4.12.

Таблиця 4.12

Параметри стохастичних процесів

З'єднання	**Стани**	**Тип процесу**
e_{12}	{72, 90, 104}	Марківський
e_{23}	{64, 80, 92}	Марківський
e_{34}	{76, 95, 109}	Марківський
e_{45}	{68, 85, 98}	Марківський
e_{56}	{60, 75, 86}	Марківський
e_{13}	{56, 70, 80}	Марківський
e_{26}	{80, 100, 115}	Марківський
e_{15}	{68, 85, 98}	Марківський
e_{36}	{72, 90, 104}	Марківський

Етап 3. Оцінювання ефективності функціонування системи

Для оцінювання ефективності функціонування системи, відповідно до (2.7), множину станів з'єднань у момент часу t подамо у вигляді:

$$X(t)=\{x_{12}(t),x_{23}(t),x_{34}(t),x_{45}(t),x_{56}(t),x_{13}(t),x_{26}(t),x_{15}(t),x_{36}(t)\}.$$

Для опису потреб ОКІ, з урахуванням (2.8), введемо множину:

$$D(t)=\{d_1(t),d_2(t),d_3(t),d_4(t),d_5(t),d_6(t)\}.$$

У третьому сценарії значення попиту приймемо сталими:

$$D(t)=\{0,20,25,30,20,45\}.$$

Для Верифікації 3, відповідно до (2.9-2.10), оцінювання показника $Q(t)$ виконується шляхом імітаційного моделювання 1000 реалізацій по 500 часових інтервалів кожна [3, 8-11].

За результатами імітаційного моделювання визначаються: середнє значення показника ефективності функціонування; розподіл $P_Q(q)$; імовірність забезпечення заданого рівня ефективності. Результати наведено в табл. 4.13.

Таблиця 4.13

Результати оцінювання ефективності

Показник	**Значення**
$\bar{Q}$ Середнє значення	0.86
$Q_{\min}$ Мінімальне значення	0.68
$Q_{\max}$ Максимальне значення	0.98
$P(Q \geq 0.85)$ Ймовірність досягнення заданого рівня	0.62

Результати імітаційного моделювання подано на рис. 4.6.

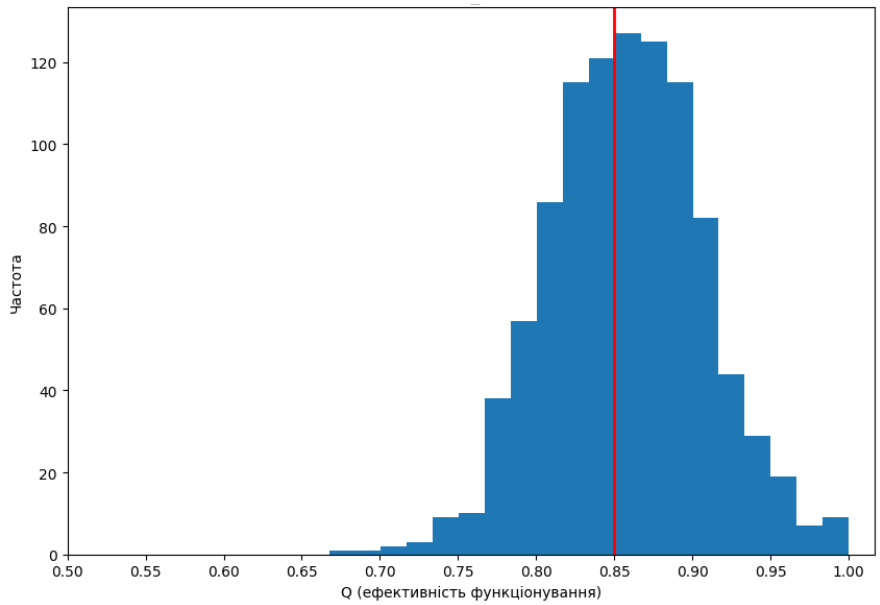

Рис. 4.6. Розподіл ймовірностей ефективності функціонування системи

На рис. 4.6 наведено розподіл ймовірностей ефективності функціонування системи, отриманий за результатами імітаційного моделювання. Вертикальною лінією позначено порогове значення $Q_0 = 0.85$,

що відповідає заданому рівню ефективності. Аналіз розподілу показує, що лише частина реалізацій забезпечує досягнення даного рівня, що підтверджує значення ймовірності $P(Q \geq Q_0) = 0.62,$ отримане в третьому сценарії.

Етап 4. Оцінювання надійності функціонування системи

Імовірнісні характеристики надійності, згідно з (2.11), визначаються на основі розподілу ймовірностей часу відновлення: $P_T(\tau) = P\left(T_r = \tau\right).$

Для інтегрального оцінювання надійності введемо показник показник (2.12): $R = P\left(T_r \leq \tau_0\right),$ де R – ймовірність відновлення системи за допустимий час $\tau_0 = 10$ – допустимий час відновлення системи.

У межах Верифікації 3 шляхом імітаційного моделювання визначаються: середній час відновлення системи; розподіл часу відновлення; імовірність відновлення за допустимий час. Результати оцінювання надійності наведено в табл. 4.14.

Таблиця 4.14

Результати оцінювання надійності

Показник	**Значення**
$\overline{T}_r$ Середній час відновлення	6.5
$T_{r,\min}$ Мінімальний час відновлення	1
$T_{r,\max}$ Максимальний час відновлення	12
$P(Q \geq 0.85)$ Ймовірність відновлення за допустимий час	0.88
R Інтегральний показник надійності	0.88

Етап 5. Обґрунтування розподілу інвестицій

Для Верифікації 3 розглянемо три інвестиційні альтернативи, що впливають на параметри стохастичних процесів станів з’єднань:

$$A = \{a_1, a_2, a_3\},$$

a_1 – інвестування у підвищення надійності з'єднання e_{15};

a_2 – інвестування у підвищення надійності з'єднання e_{36};

a_3 – інвестування у підвищення надійності третьої підсистеми SCADA.

Для оцінювання ефективності інвестицій, згідно з (2.14), використовується показник: $Q_0 = 0.85$.

Результати оцінювання інвестиційних альтернатив наведено в табл. 4.15.

Таблиця 4.15

Порівняння інвестиційних альтернатив

Альтернатива	Опис	Вартість	$P_{sat}^{(k)}$	ΔP_k
a_1	Покращення e_{15}	10	0.70	+0.08
a_2	Покращення e_{36}	12	0.74	+0.12
a_3	Покращення SCADA 3	14	0.78	+0.16

З табл. 4.15 видно, що у третьому сценарії ймовірність забезпечення заданого рівня ефективності становить $P_{sat}^{(0)} = 0.62$. Застосування інвестиційних альтернатив дозволяє підвищити даний показник до $P_{sat}^{(k)} = 0.78$, що відповідає приросту ефективності на $\Delta P_k = 16\%$. При цьому встановлено, що найбільший вплив на ефективність функціонування системи має інвестування у підсистему керування, що підтверджує необхідність врахування взаємозалежностей у ВКІ.

Загальні висновки за результатами Верифікацій 1–3

За результатами проведених верифікацій запропонованого методу встановлено його працездатність та можливість застосування для оцінювання ефективності функціонування систем безпеки ВКІ за різних умов функціонування.

У межах Верифікації 1 досліджено базовий сценарій, який дозволив визначити початкові значення показників ефективності та надійності функціонування системи. Верифікація 2 підтвердила чутливість методу до зміни топології взаємозв'язків між об'єктами, що відобразилось у зниженні ймовірності забезпечення заданого рівня ефективності. У Верифікації 3 показано, що введення додаткових зв'язків та підвищення рівня резервування забезпечує зростання ефективності функціонування системи та покращення показників надійності.

Таблиця 4.16

Узагальнення результатів верифікації методу

Показник	Верифікація 1	Верифікація 2	Верифікація 3
Характеристика сценарію	Базовий	Альтернативна топологія	Підвищене резервування
Кількість з'єднань	8	7	9
Кількість підсистем SCADA	2	2	3
$P_{sat}^{(0)}$	0.47	0.39	0.62
Найкраща альтернатива	a_3	a_3	a_3
P_{sat} після інвестування	0.67	0.61	0.78
ΔP	0.20	0.22	0.16

Дані табл. 4.16 свідчать, що запропонований метод є чутливим до зміни топології взаємозв'язків і рівня резервування системи. Найгірші значення показників ефективності та надійності отримано для Верифікації 2,

тоді як найкращі – для Верифікації 3, що підтверджує доцільність врахування структурних особливостей ВКІ та пріоритетного розподілу інвестицій у підсистеми керування.

Отримані результати свідчать про адекватність запропонованого методу та підтверджують можливість його використання для аналізу впливу структурних та параметричних змін на функціонування ВКІ. Зокрема, встановлено, що врахування взаємозалежностей між об’єктами та станів підсистем керування суттєво впливає на інтегральні показники ефективності та надійності системи.

Слід зазначити, що у межах проведених верифікацій використано марківські процеси як окремий випадок, тоді як запропонований метод допускає узагальнення на напівмарківські процеси, що дозволяє враховувати довільні закони розподілу часу перебування у станах.

Проведена верифікація підтверджує ефективність удосконаленого методу оцінювання ефективності функціонування систем безпеки ВКІ, який, за рахунок використання графового подання взаємозалежностей об’єктів, марківських і напівмарківських процесів моделювання станів, забезпечує оцінювання ймовірнісних характеристик функціонування системи та обґрунтування розподілу інвестицій у забезпечення безпеки ОКІ.

Практичні рекомендації щодо раціонального розподілу інвестицій та ресурсів у системах безпеки ВКІ

За результатами експериментальної апробації ***сформовано практичні рекомендації*** щодо раціонального розподілу інвестицій та ресурсів у системах безпеки ВКІ з урахуванням наявних обмежень (рис. 4.7).

Рис. 4.7. Практичні рекомендації щодо раціонального розподілу інвестицій та ресурсів у системах безпеки ВКІ

Практичні рекомендації передбачають:

- інвестування доцільно спрямовувати у ті елементи системи (з'єднання або підсистеми керування), для яких спостерігається найбільший приріст ймовірності забезпечення заданого рівня ефективності, тобто максимальне значення показника ΔP_k;
- за обмеженого бюджету пріоритет слід надавати інвестиціям у підсистеми керування (SCADA), оскільки вони мають системний вплив на групи з'єднань і забезпечують найбільший приріст ефективності функціонування;

- у разі наявності альтернативних варіантів інвестування доцільно обирати ті, що забезпечують максимальне значення показника P_{sat} при мінімальних витратах, тобто враховувати співвідношення «ефект/вартість»;
- доцільно забезпечувати резервування критичних зв'язків шляхом додавання альтернативних маршрутів, що дозволяє підвищити ймовірність досягнення заданого рівня ефективності та покращити показники надійності системи;
- при плануванні інвестицій необхідно враховувати топологію мережі, оскільки зміна структури взаємозв'язків між об'єктами може суттєво впливати на ефективність функціонування системи;
- у разі відсутності інвестиційних альтернатив, що забезпечують додатний приріст ефективності $(\Delta P_k > 0)$, подальше інвестування є недоцільним;
- для обґрунтування рішень щодо розподілу ресурсів доцільно використовувати імітаційне моделювання, що дозволяє оцінити вплив інвестицій на ймовірнісні характеристики функціонування системи.

Сформовані рекомендації можуть бути використані операторами КІ для обґрунтованого прийняття управлінських рішень щодо раціонального розподілу інвестицій та ресурсів у системах безпеки ВКІ, з урахуванням топології взаємозв'язків, бюджетних обмежень та необхідності забезпечення заданого рівня ефективності функціонування, що підтверджує їх практичну цінність.

4.2. Експериментальне дослідження методу оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем критичної інфраструктури

Експериментальне дослідження методу оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем (ІКС) критичної

інфраструктури (КІ) проведено з урахуванням [12-15] на прикладі енергетичного сектору. Вибір енергетичного сектору обумовлений високим рівнем його критичності, значною кількістю взаємопов'язаних компонентів та підвищеною чутливістю до впливу кіберінцидентів. Особливої актуальності це набуває в умовах повномасштабної агресії проти України, коли об'єкти енергетичної інфраструктури зазнають комплексного впливу, зокрема фізичних атак, кіберінцидентів та дестабілізуючих факторів, що призводить до порушення їх функціонування. За таких умов забезпечення належного рівня захищеності ІКС енергетичного сектору є критично важливим завданням, оскільки від їх стійкості залежить безперервність функціонування ОКІ та стабільність енергопостачання [16-18].

Експериментальна перевірка методу здійснюється відповідно до етапів, наведених у підрозділі 2.2, та передбачає формування множини інцидентів, визначення критеріїв їх впливу на систему, оцінювання вагових коефіцієнтів, а також інтегральне оцінювання рівня захищеності.

У межах дослідження розглянуто три сценарії функціонування системи: базовий, несприятливий та сценарій покращення, що дозволяє оцінити чутливість методу до зміни характеристик інцидентів і умов функціонування ІКС.

Верифікація 1

Базовий сценарій функціонування ІКС енергетичного об'єкта

Етап 1. Формування множини інцидентів ІКС

Для проведення Верифікації 1, відповідно до запропонованого методу та з урахуванням (2.20), множину інцидентів у момент часу t представимо у вигляді:

$$I(t) = \{i_1(t), i_2(t), i_3(t), i_4(t), i_5(t)\},$$

$i_1(t)$ – кібератака на сервери диспетчерського керування, $i_2(t)$ – відмова каналів зв'язку між підстанціями та центром керування, $i_3(t)$ – збій програмного забезпечення SCADA/АСУ ТП, $i_4(t)$ – помилка оператора, $i_5(t)$ – відмова серверного обладнання або порушення електроживлення [16-18].

Для врахування характеристик інцидентів, відповідно до (2.21), введемо множину параметрів у вигляді табл. 4.17.

Таблиця 4.17

Характеристики інцидентів для Верифікації 1

№	Інцидент	$p_k(t)$	$s_k(t)$	$d_k(t)$	$r_k(t)$
i_1	Кібератака на сервери диспетчерського керування	0.25	0.90	0.80	0.40
i_2	Відмова каналів зв'язку	0.20	0.75	0.85	0.50
i_3	Збій ПЗ SCADA/АСУ ТП	0.30	0.80	0.70	0.60
i_4	Помилка оператора	0.35	0.50	0.40	0.80
i_5	Відмова обладнання / електроживлення	0.15	0.85	0.90	0.45

Етап 2. Визначення критеріїв впливу інцидентів на систему

Для оцінювання впливу інцидентів на рівень захищеності ІКС енергетичного об'єкта, відповідно до (2.22), введемо множину критеріїв:

$$C = \{c_1, c_2, c_3, c_4\},$$

де c_2, – конфіденційність, c_2 – цілісність, c_3 – доступність, c_4 – стійкість системи.

Значення ступеня впливу інцидентів на критерії для Верифікації 1 наведено в табл. 4.18.

Таблиця 4.18

Ступінь впливу інцидентів на критерії оцінювання для Верифікації 1

Інцидент	Конфіденційність c_1	Цілісність c_2	Доступність c_3	Стійкість c_4
i_1	0.90	0.85	0.70	0.75
i_2	0.20	0.50	0.95	0.80
i_3	0.40	0.80	0.75	0.70
i_4	0.30	0.60	0.50	0.45
i_5	0.10	0.40	0.90	0.85

Етап 3. Оцінювання вагових коефіцієнтів критеріїв та інцидентів

Для врахування різної важливості критеріїв та інцидентів, відповідно до (2.25-2.28), визначимо вагові коефіцієнти на основі методу попарних порівнянь [19-20].

Крок 3.1. Оцінювання ваг критеріїв

Для визначення вагових коефіцієнтів критеріїв сформуємо матрицю попарних порівнянь, наведену в табл. 4.19.

Таблиця 4.19

Матриця попарних порівнянь критеріїв для Верифікації 1

Критерій	c_1	c_2	c_3	c_4
c_1	1	1/2	1/3	1/2
c_2	2	1	1/2	1
c_3	3	2	1	2
c_4	2	1	1/2	1

За результатами обчислень, відповідно до (2.26), отримаємо вектор вагових коефіцієнтів критеріїв:

$$W = \{0.14, 0.24, 0.38, 0.24\}.$$

Отримані значення свідчать, що у межах Верифікації 1 найбільшу важливість має критерій доступності, тоді як конфіденційність має найменшу вагу.

Крок 3.2. Оцінювання ваг інцидентів

Аналогічно, відповідно до (2.27), сформуємо матрицю попарних порівнянь інцидентів, наведену в табл. 4.20.

Таблиця 4.20

Матриця попарних порівнянь інцидентів для Верифікації 1

Інцидент	i_1	i_2	i_3	i_4	i_5
i_1	1	2	1	3	2
i_2	1/2	1	1/2	2	1
i_3	1	2	1	3	2
i_4	1/3	1/2	1/3	1	1/2
i_5	1/2	1	1/2	2	1

Відповідно до (2.28), вектор вагових коефіцієнтів інцидентів має вигляд:

$$V = \{0.30, 0.17, 0.30, 0.08, 0.15\}.$$

Отримані значення показують, що найбільшу вагу у базовому сценарії мають кібератака на сервери диспетчерського керування та збій програмного забезпечення SCADA/АСУ ТП, тоді як найменшу вагу має помилка оператора.

Етап 4. Оцінювання впливу інцидентів на інтегральний показник захищеності

Для кількісного оцінювання впливу інцидентів на рівень захищеності системи, відповідно до (2.29), визначимо інтегральний вплив кожного

інциденту з урахуванням вагових коефіцієнтів критеріїв та інцидентів, наведені в табл. 4.21.

Таблиця 4.21

Інтегральний вплив інцидентів для Верифікації 1

Інцидент	v_k	$\sum_{j=1}^{m} w_j\, x_{kj}(t)$	$IM_k(t)$
i_1	0.30	0.783	0.235
i_2	0.17	0.674	0.115
i_3	0.30	0.685	0.206
i_4	0.08	0.478	0.038
i_5	0.15	0.611	0.092

Сукупний вплив усіх інцидентів на систему, відповідно до (2.30), визначається як:

$$IM(t) = 0.235 + 0.115 + 0.206 + 0.038 + 0.092 = 0.686.$$

Отримані значення свідчать, що найбільший вплив на рівень захищеності ІКС енергетичного об’єкта мають кібератака на сервери диспетчерського керування та збій програмного забезпечення SCADA/АСУ ТП. Найменший вплив у базовому сценарії має помилка оператора, що пояснюється нижчим значенням вагового коефіцієнта інциденту та меншими значеннями ступеня впливу на критерії.

Етап 5. Інтегральне оцінювання рівня захищеності системи

Для оцінювання загального стану ІКС енергетичного об’єкта, відповідно до (2.31), визначимо інтегральний показник захищеності системи.

$$S(t) = 1 - 0.686 = 0.314.$$

Отриманий результат $S(t) = 0.314$ свідчить, що у межах базового сценарію Верифікації 1 рівень захищеності ІКС енергетичного об'єкта є ***низьким***, що відповідає інтервалу $0.20 < S(t) \leq 0.40$ згідно з табл. 2.1.

Це обумовлено значним впливом інцидентів, пов'язаних із кібератаками та збоями програмного забезпечення, які суттєво впливають на доступність та стійкість функціонування системи.

Верифікація 2.

Несприятливий сценарій функціонування ІКС енергетичного об'єкта

Етап 1. Формування множини інцидентів ІКС

Для проведення Верифікації 2 використовується та сама множина інцидентів, що і у Верифікації 1. Для врахування характеристик інцидентів, відповідно до (2.21), введемо множину параметрів, значення яких наведено в табл. 4.22 [16-18].

Таблиця 4.22

Характеристики інцидентів для Верифікації 2

№	Інцидент	$p_k(t)$	$s_k(t)$	$d_k(t)$	$r_k(t)$
i_1	Кібератака на сервери диспетчерського керування	0.35	0.95	0.90	0.30
i_2	Відмова каналів зв'язку	0.30	0.85	0.90	0.40
i_3	Збій ПЗ SCADA/АСУ ТП	0.40	0.90	0.80	0.50
i_4	Помилка оператора	0.45	0.60	0.50	0.70
i_5	Відмова обладнання / електроживлення	0.25	0.90	0.95	0.35

Етап 2. Визначення критеріїв впливу інцидентів на систему

Для оцінювання впливу інцидентів на рівень захищеності ІКС енергетичного об’єкта, відповідно до (2.22–2.24), використаємо множину критеріїв, що була визначена у Верифікації 1.

Значення ступеня впливу інцидентів на критерії для Верифікації 2 наведено в табл. 4.23.

Таблиця 4.23

Ступінь впливу інцидентів на критерії оцінювання для Верифікації 2

Інцидент	Конфіденційність c_1	Цілісність c_2	Доступність c_3	Стійкість c_4
i_1	0.95	0.90	0.85	0.85
i_2	0.30	0.60	0.98	0.90
i_3	0.50	0.90	0.85	0.80
i_4	0.40	0.70	0.60	0.55
i_5	0.20	0.60	0.95	0.90

Етап 3. Оцінювання вагових коефіцієнтів критеріїв та інцидентів

Оскільки у межах Верифікації 2 змінюються лише характеристики інцидентів та ступінь їх впливу на критерії оцінювання, а множина критеріїв і склад інцидентів залишаються незмінними, вектори вагових коефіцієнтів критеріїв W та інцидентів V, визначені у Верифікації 1, приймаються без змін [19-20].

Етап 4. Оцінювання впливу інцидентів на інтегральний показник захищеності

Для кількісного оцінювання впливу інцидентів на рівень захищеності системи, відповідно до (2.29), визначимо інтегральний вплив кожного інциденту з урахуванням вагових коефіцієнтів критеріїв та інцидентів, наведені в табл. 4.24.

Таблиця 4.24

Інтегральний вплив інцидентів для Верифікації 2

Інцидент	v_k	$\sum_{j=1}^{m} w_j\, x_{kj}(t)$	$IM_k(t)$
i_1	0.30	0.86	0.258
i_2	0.17	0.78	0.133
i_3	0.30	0.79	0.237
i_4	0.08	0.52	0.042
i_5	0.15	0.74	0.111

Сукупний вплив усіх інцидентів на систему, відповідно до (2.30), визначається як:

$$IM(t) = 0.258 + 0.133 + 0.237 + 0.042 + 0.111 = 0.83.$$

Отримані значення свідчать про зростання впливу інцидентів порівняно з базовим сценарієм, що обумовлено погіршенням умов функціонування системи. Найбільший вплив на рівень захищеності ІКС енергетичного об’єкта мають кібератака на сервери диспетчерського керування та збій програмного забезпечення SCADA/АСУ ТП, що пов’язано з високими значеннями їх вагових коефіцієнтів та ступеня впливу на критерії оцінювання. Найменший вплив має помилка оператора, що пояснюється нижчим значенням вагового коефіцієнта інциденту та меншими значеннями впливу на критерії.

Етап 5. Інтегральне оцінювання рівня захищеності системи

Для оцінювання загального стану ІКС енергетичного об’єкта, відповідно до (2.31), визначимо інтегральний показник захищеності системи.

$$S(t) = 1 - 0.83 = 0.17.$$

Отриманий результат $S(t) = 0.17$ свідчить, що у межах несприятливого сценарію Верифікації 2 рівень захищеності ІКС енергетичного об'єкта є ***критичним***, що відповідає інтервалу $0.00 \leq S(t) \leq 0.20$ згідно з табл. 2.1.

Це обумовлено значним впливом інцидентів, пов'язаних із кібератаками, відмовами каналів зв'язку та збоями програмного забезпечення, які суттєво впливають на доступність та стійкість функціонування системи.

Верифікація 3.

Несприятливий сценарій функціонування ІКС енергетичного об'єкта

Етап 1. Формування множини інцидентів ІКС

Для проведення Верифікації 3 використовується та сама множина інцидентів, що і у Верифікації 1. Для врахування характеристик інцидентів, відповідно до (2.21), введемо множину параметрів, значення яких наведено в табл. 4.25 [16-18].

Таблиця 4.25

Характеристики інцидентів для Верифікації 3

№	Інцидент	$p_k(t)$	$s_k(t)$	$d_k(t)$	$r_k(t)$
i_1	Кібератака на сервери диспетчерського керування	0.15	0.80	0.60	0.70
i_2	Відмова каналів зв'язку	0.12	0.70	0.65	0.75
i_3	Збій ПЗ SCADA/АСУ ТП	0.18	0.75	0.60	0.80
i_4	Помилка оператора	0.25	0.40	0.30	0.90
i_5	Відмова обладнання / електроживлення	0.10	0.75	0.70	0.75

Етап 2. Визначення критеріїв впливу інцидентів на систему

Для оцінювання впливу інцидентів на рівень захищеності ІКС енергетичного об’єкта, відповідно до (2.22–2.24), використаємо множину критеріїв, що була визначена у Верифікації 1.

Значення ступеня впливу інцидентів на критерії для Верифікації 3 наведено в табл. 4.26.

Таблиця 4.26

Ступінь впливу інцидентів на критерії оцінювання для Верифікації 3

Інцидент	Конфіденційність c_1	Цілісність c_2	Доступність c_3	Стійкість c_4
i_1	0.70	0.65	0.60	0.60
i_2	0.15	0.40	0.75	0.65
i_3	0.30	0.65	0.60	0.55
i_4	0.20	0.40	0.35	0.30
i_5	0.10	0.35	0.70	0.65

Етап 3. Оцінювання вагових коефіцієнтів критеріїв та інцидентів

Оскільки у межах Верифікації 3 змінюються лише характеристики інцидентів та ступінь їх впливу на критерії оцінювання, а множина критеріїв і склад інцидентів залишаються незмінними, вектори вагових коефіцієнтів критеріїв W та інцидентів V, визначені у Верифікації 1, приймаються без змін [19-20].

Етап 4. Оцінювання впливу інцидентів на інтегральний показник захищеності

Для кількісного оцінювання впливу інцидентів на рівень захищеності системи, відповідно до (2.29), визначимо інтегральний вплив кожного інциденту з урахуванням вагових коефіцієнтів критеріїв та інцидентів, наведені в табл. 4.27.

Таблиця 4.27

Інтегральний вплив інцидентів для Верифікації 3

Інцидент	v_k	$\sum_{j=1}^{m} w_j\, x_{kj}(t)$	$IM_k(t)$
i_1	0.30	0.62	0.186
i_2	0.17	0.55	0.094
i_3	0.30	0.58	0.174
i_4	0.08	0.34	0.027
i_5	0.15	0.52	0.078

Сукупний вплив усіх інцидентів на систему, відповідно до (2.30), визначається як:

$$IM(t) = 0.186 + 0.094 + 0.174 + 0.027 + 0.078 = 0.559.$$

Отримані значення свідчать про зменшення впливу інцидентів порівняно з Верифікаціями 1 та 2, що обумовлено покращенням умов функціонування системи. Найбільший вплив на рівень захищеності ІКС енергетичного об’єкта, як і в попередніх сценаріях, мають кібератака на сервери диспетчерського керування та збій програмного забезпечення SCADA/АСУ ТП, однак рівень їх впливу є суттєво нижчим. Найменший вплив має помилка оператора, що пояснюється зниженням її впливу на критерії оцінювання та меншою значущістю у загальній структурі інцидентів.

Етап 5. Інтегральне оцінювання рівня захищеності системи

Для оцінювання загального стану ІКС енергетичного об’єкта, відповідно до (2.31), визначимо інтегральний показник захищеності системи.

$$S(t) = 1 - 0.559 = 0.441.$$

Отриманий результат $S(t) = 0.441$ свідчить, що у межах сценарію покращення Верифікації 3 рівень захищеності ІКС енергетичного об'єкта є ***середнім***, що відповідає інтервалу $0.40 < S(t) \leq 0.60$ згідно з табл. 2.1.

Це обумовлено зменшенням впливу інцидентів, зниженням їх ймовірності виникнення, тривалості впливу та підвищенням швидкості відновлення, що сприяє покращенню показників доступності та стійкості функціонування системи.

Загальні висновки за результатами Верифікації 1-3

За результатами проведених верифікацій підтверджено працездатність запропонованого методу оцінювання впливу інцидентів на рівень захищеності ІКС КІ та можливість його застосування для аналізу функціонування систем за різних умов.

У межах Верифікації 1 досліджено базовий сценарій функціонування системи, для якого інтегральний показник захищеності становить $S(t) = 0.314$, що відповідає низькому рівню захищеності. Верифікація 2 продемонструвала деградацію стану системи в умовах підвищеного рівня загроз: значення показника зменшилось до $S(t) = 0.17$, що відповідає критичному рівню захищеності. У Верифікації 3 показано можливість покращення функціонування системи за рахунок зниження впливу інцидентів, що забезпечило зростання показника до $S(t) = 0.441$, що відповідає середньому рівню захищеності.

Отримані результати свідчать про чутливість запропонованого методу до зміни характеристик інцидентів та ступеня їх впливу на критерії оцінювання, а також підтверджують його здатність відображати як деградацію, так і покращення стану системи.

Таким чином, запропонований метод дозволяє кількісно оцінювати вплив інцидентів на рівень захищеності ІКС, забезпечує можливість якісної

інтерпретації отриманих результатів та підтримку прийняття обґрунтованих управлінських рішень щодо підвищення рівня їх захищеності.

4.3. Експериментальне дослідження методу підвищення рівня захищеності критичних інформаційних систем держави

У роботах [21] було проведено експериментальне дослідження методу підвищення рівня захищеності критичних інформаційних систем (КІС) держави. Експериментальне дослідження методу реалізується за допомогою представлених у [21] етапів, що включає ідентифікацію загроз, формування сценаріїв їх реалізації, оцінювання ризиків, надійності та стійкості КІС з подальшим визначенням інтегрального показника рівня її захищеності. Це забезпечує можливість об’єктивно перевірити ефективність методу на практиці та порівняти стан системи до і після впровадження заходів підвищення безпеки згідно з [22-23].

Верифікація 1

Автоматизована система управління повітряним рухом

Для експериментального дослідження було обрано КІС транспортного сектору – автоматизовану систему управління повітряним рухом (АС УПР), яка забезпечує навігаційне та диспетчерське обслуговування польотів у повітряному просторі України. Вибір цієї системи зумовлений її стратегічною роллю для національної безпеки, а також високим рівнем критичності наслідків можливих відмов або кібервтручань. Особливо актуальним є дослідження стійкості та захищеності АС УПР в умовах воєнного стану, коли цивільний повітряний простір України з 2022 року переважно закритий для комерційних польотів, а система використовується у обмеженому режимі, виконуючи функції забезпечення перельотів державної, гуманітарної, евакуаційної та військової авіації. Це супроводжується зміною профілю загроз, зростанням актуальності кібератак та радіоелектронних

впливів, необхідністю підтримання працездатності під час бойових дій, пошкодження інфраструктури та нестабільності енергосистеми [24-27].

Етап 1. Визначення множини потенційних загроз КІС

Відповідно до запропонованого методу, розглянемо приклад формування загального переліку потенційних загроз АС УПР на основі аналізу нормативних документів ICAO, EASA, EUROCONTROL, NOTAM [24-27]. При $n = 5$ з урахуванням (1) визначимо множину типів потенційних загроз АС УПР таким чином:

$$\mathbf{H} = \{\bigcup_{k=1}^{5} H_k\} = \{H_1, H_2, H_3, H_4, H_5\},$$

де H_1 – кібератаки на сервери, навігаційні комплекси та радіолокаційні системи, H_2 – відмова або порушення роботи каналів зв'язку АТС–пілот/АТС–АТС, H_3 – технічний збій, аварія або деградація обладнання ЦОВ/радари/сервери, H_4 – людський фактор (помилки диспетчера, стресові умови, перевантаження), H_5 – зовнішні впливи: пошкодження інфраструктури, перебої енергоживлення, РЕБ, бойові дії, згідно [21-27].

Етап 2. Визначення множини сценаріїв, що характеризують потенційні загрози певної КІС

Для визначеного на попередньому етапі переліку потенційну загрозу H_k, при $n = 5$ та $p = 5$ з урахуванням (2) представимо множину сценаріїв, у наступному вигляді:

$$\mathbf{\Omega} = \{\bigcup_{p=1}^{5} \Omega_p\} = \{\Omega_1, \Omega_2, \Omega_3, \Omega_4, \Omega_5\},$$

де Ω_1 – множина сценаріїв кібервпливу на АС УПР, Ω_2 – множина сценаріїв деградації або порушення каналів зв'язку АТС, Ω_3 – множина сценаріїв

технічних відмов радарів/ серверів/ ЦОВ, Ω_4 – множина сценаріїв, пов'язаних із людським фактором, Ω_5 – множина сценаріїв зовнішніх впливів (енергетичних, РЕБ, бойових).

Для представлення відповідного сценарію Ω_{kp}, що характеризує реалізацію конкретної загрози H_k, з урахуванням (3), представимо кортеж ω_{kp}, який враховує комбінацію типу загрози, умов середовища та часу її реалізації у наступному вигляді:

$$\Omega_1 = \{\omega_{11}, \omega_{12}\}, \omega_{11} = \langle H_1, cond_{11}, t_{11} \rangle, \omega_{12} = \langle H_1, cond_{12}, t_{12} \rangle,$$

де $cond_{11}$ – відсутність сегментації мережі та вразливість серверів, t_{11} – період пікового навантаження або оновлення систем, $cond_{12}$ – наявність відкритих портів та недостатній контроль IDS/IPS, t_{12} – в момент зовнішньої інформаційної атаки, DDoS.

$$\Omega_2 = \{\omega_{21}, \omega_{22}\}, \omega_{21} = \langle H_2, cond_{21}, t_{21} \rangle, \omega_{22} = \langle H_2, cond_{22}, t_{22} \rangle,$$

де $cond_{21}$ – пошкодження наземних каналів або втрата VHF-зв'язку, t_{21} – у період погіршених погодних умов, $cond_{22}$ – деградація SATCOM/ADS-B сигналів, t_{22} – під час воєнних завад або РЕБ.

$$\Omega_3 = \{\omega_{31}, \omega_{32}\}, \omega_{31} = \langle H_3, cond_{31}, t_{31} \rangle, \omega_{32} = \langle H_3, cond_{32}, t_{32} \rangle,$$

де $cond_{31}$ – зношеність обладнання або відсутність резервування, t_{31} – у пікові години або під час оновлення ПЗ, $cond_{32}$ – збій бази даних або аварія сервера, t_{32} – при переході на резервний сегмент.

$$\Omega_4 = \{\omega_{41}, \omega_{42}\}, \omega_{41} = \langle H_4, cond_{41}, t_{41} \rangle, \omega_{42} = \langle H_4, cond_{42}, t_{42} \rangle,$$

де $cond_{41}$ – втома персоналу або інформаційне перевантаження, t_{41} – при високій щільності трафіку або НС, $cond_{42}$ – помилка при передачі команд, t_{42} – у критичних ситуаціях або під час стрес-фактора.

$$\Omega_5 = \{\omega_{51}, \omega_{52}\}, \omega_{51} = \langle H_5, cond_{51}, t_{51} \rangle, \omega_{52} = \langle H_5, cond_{52}, t_{52} \rangle,$$

де $cond_{51}$ – перебої енергоживлення або відсутність генератора, t_{51} – під час обстрілів або масованих атак, $cond_{52}$ – вплив РЕБ або глушіння GNSS, t_{52} – у критичний період польотних операцій.

Базові налаштування програмного застосунку, що реалізують етапи формування множини загроз та сценаріїв їх реалізації (етапи 1-2 методу), наведено на рис. 4.8.

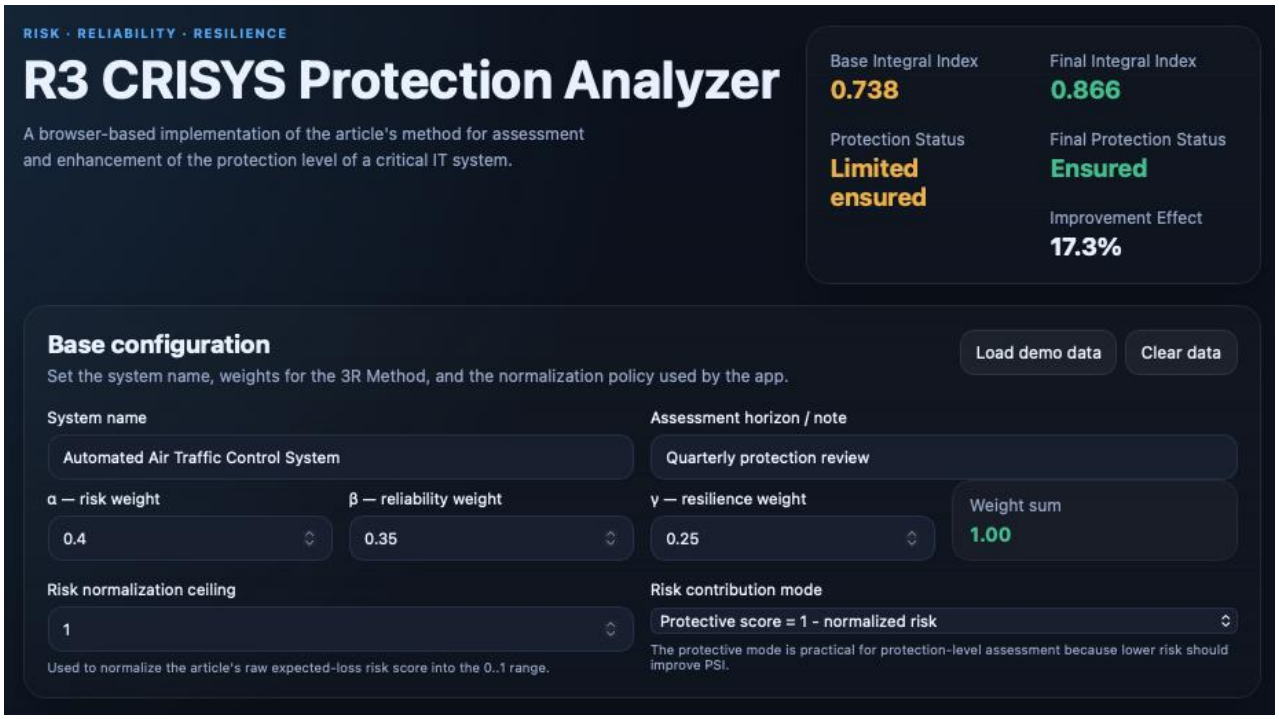

Рис. 4.8. Інтерфейс програмного застосунку для реалізації етапів 1–2 методу

На рис. 4.8 представлено інтерфейс програмного застосунку, який забезпечує формування множини загроз та відповідних сценаріїв їх реалізації.

Етап 3. Оцінка ризиків елемента КІС

З урахуванням визначених множин Ω_k та кортежів ω_{kp} сформуємо експериментальні дані для розрахунку ризику. Для випадку АС УПР у рамках експерименту використаємо дві категорії наслідків: $d=1$ – безпекові , вага $w_1=0.7,\ d=2$ – економічні наслідки , вага $w_2=0.3$.

Для кожного сценарію, відповідно до виразу (4), задаємо параметри сценаріїв ризику для АС УПР у вигляді Табл. 4.28.

Таблиця 4.28

Параметри сценаріїв ризику для АС УПР

Загроза H_k	Сценарій ω_{kp}	Ймовірність реалізації P_{ikp}	Рівень вразливості V_{ikp}	Наслідки $C^{(1)}$	Наслідки $C^{(2)}$
H_1	ω_{11}	0.10	0.80	0.95	0.85
	ω_{12}	0.12	0.75	0.90	0.80
H_2	ω_{21}	0.06	0.70	0.85	0.60
	ω_{22}	0.05	0.65	0.80	0.55
H_3	ω_{31}	0.04	0.85	0.95	0.70
	ω_{32}	0.07	0.60	0.75	0.50
H_4	ω_{41}	0.10	0.50	0.70	0.45
	ω_{42}	0.08	0.55	0.65	0.40
H_5	ω_{51}	0.05	0.60	0.80	0.65
	ω_{52}	0.07	0.70	0.85	0.55

Далі представимо результати розрахунку ризику для кожної загрози:

1) Загроза H_1: кібератаки

$$R_1 = \left(0.7 \cdot 0.10 \cdot 0.8 \cdot 0.95 + 0.3 \cdot 0.10 \cdot 0.8 \cdot 0.85\right) +$$
$$+\left(0.7 \cdot 0.12 \cdot 0.75 \cdot 0.9 + 0.3 \cdot 0.12 \cdot 0.75 \cdot 0.80\right) = 0.1519$$

2) Загроза H_2: порушення каналів зв'язку

$$R_2 = \left(0.7 \cdot 0.06 \cdot 0.7 \cdot 0.85 + 0.3 \cdot 0.06 \cdot 0.70 \cdot 0.60\right) +$$
$$+\left(0.7 \cdot 0.05 \cdot 0.65 \cdot 0.80 + 0.3 \cdot 0.05 \cdot 0.65 \cdot 0.55\right) = 0.0561$$

3) Загроза H_3: технічний збій обладнання

$$R_3 = \left(0.7 \cdot 0.04 \cdot 0.85 \cdot 0.95 + 0.3 \cdot 0.04 \cdot 0.85 \cdot 0.70\right) +$$
$$+\left(0.7 \cdot 0.07 \cdot 0.60 \cdot 0.75 + 0.3 \cdot 0.07 \cdot 0.60 \cdot 0.50\right) = 0.0581$$

4) Загроза H_4: людський фактор

$$R_4 = \left(0.7 \cdot 0.10 \cdot 0.50 \cdot 0.70 + 0.3 \cdot 0.10 \cdot 0.50 \cdot 0.45\right) +$$
$$+\left(0.7 \cdot 0.08 \cdot 0.55 \cdot 0.65 + 0.3 \cdot 0.08 \cdot 0.55 \cdot 0.40\right) = 0.0566$$

5) Загроза H_4: зовнішні впливи (енергія, РЕБ, бойові дії)

$$R_5 = \left(0.7 \cdot 0.05 \cdot 0.60 \cdot 0.80 + 0.3 \cdot 0.05 \cdot 0.60 \cdot 0.65\right) +$$
$$+\left(0.7 \cdot 0.07 \cdot 0.70 \cdot 0.85 + 0.3 \cdot 0.07 \cdot 0.70 \cdot 0.55\right) = 0.0599$$

Загальний ризик елемента АС УПР відповідно до (4):

$$RISK_i = R_1 + R_2 + R_3 + R_4 + R_5 =$$
$$= 0.1519 + 0.0561 + 0.0581 + 0.0566 + 0.0599 = 0.3826 \approx 0.383$$

Результати оцінювання ризиків елементів КІС з використанням програмного застосунку наведено на рис. 4.9.

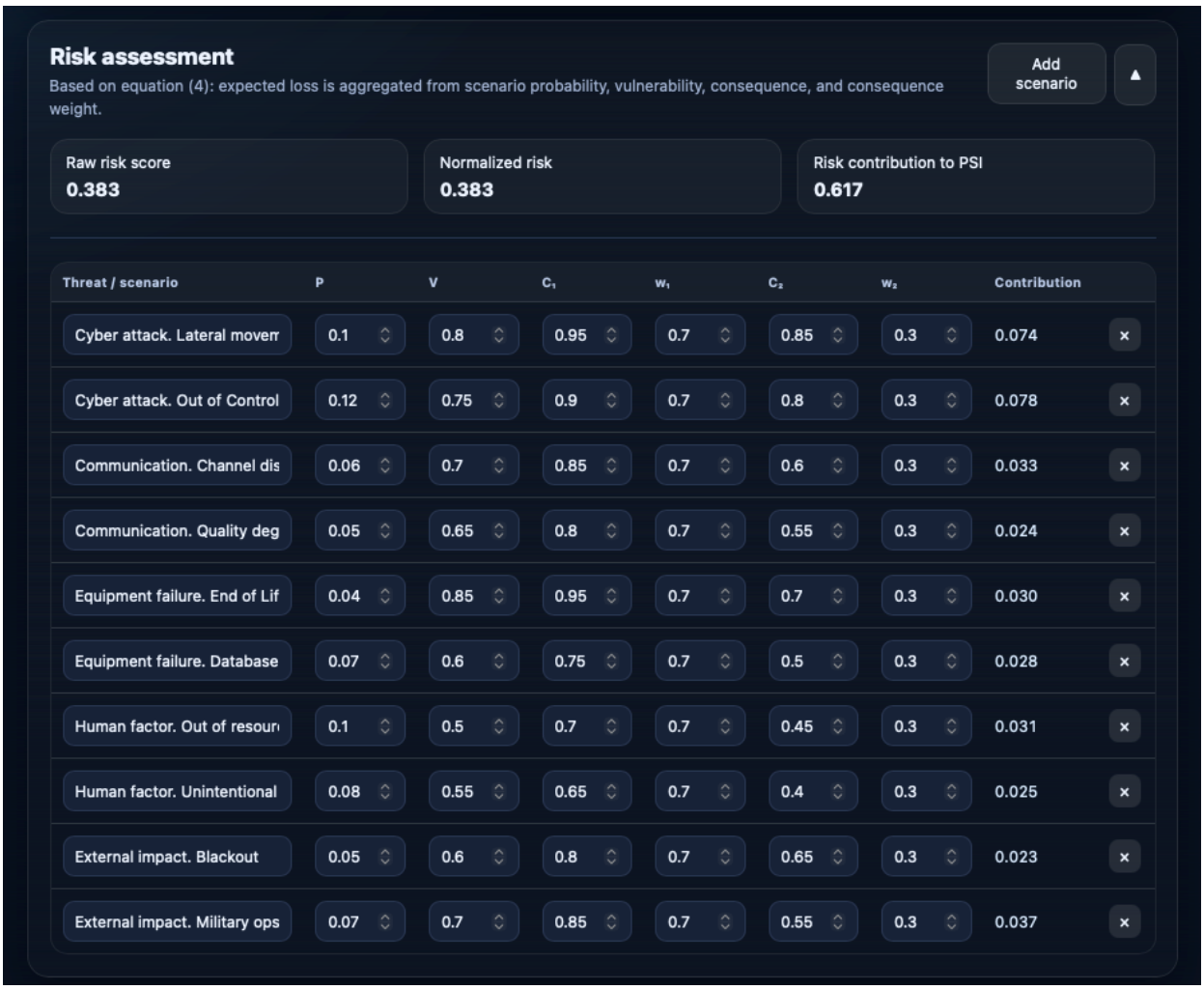

Рис. 4.9. Інтерфейс програмного застосунку при оцінюванні ризиків КІС

На рис. 4.9 представлено результати оцінювання ризиків, що враховують ймовірність реалізації загроз, рівень вразливості та можливі наслідки.

Етап 4. Оцінка надійності елемента КІС

У межах експерименту приймемо показники роботи критичного елемента АС УПР (наприклад, серверного вузла або радіолокаційної підсистеми): за період 3 років спостережень зафіксовано: $N_{fail,i} = 3$ відмови, загальний час роботи за цей період: $T_{obs,i} = 3 \cdot 8760 = 26280$ год.

$$\lambda_i = \frac{N_{fail,i}}{T_{obs,i}} = \frac{3}{26280} \approx 1.14 \cdot 10^{-4}.$$

Для розрахунку імовірності безвідмовної роботи, врахуємо річний інтервал $t = 8760$ годин, враховуючи (5), отримаємо $R_i(t) = e^{-\lambda_i t} = e^{-1.14 \cdot 10^{-4} \cdot 8760} \approx e^{-0.999} \approx 0.368$.

Отже, імовірність того, що елемент АС УПР працюватиме безвідмовно протягом року, становить 0.368.

Деякі елементи АС УПР можуть підтримувати автономний перезапуск або ізольований режим роботи (наприклад, резервні радари, дублюючі сервери). Розширену надійність обчислюємо відповідно до (7), враховуючи, що $B_s = 0.85$ (ймовірність успішного автоматичного відновлення роботи), $R_{island} = 0.90$.

$$R_i^* = R_i + (1 - R_i) \cdot B_s \cdot R_{island} = 0.368 + (1 - 0.368) \cdot 0.85 \cdot 0.90 = 0.851.$$

Результати оцінювання надійності елемента КІС з використанням програмного застосунку наведено на рис. 4.10.

Рис. 4.10. Інтерфейс програмного застосунку при оцінюванні надійності КІС

На рис. 4.10 представлено результати оцінювання імовірності безвідмовної роботи елементів КІС з урахуванням можливості їх відновлення.

Етап 5. Оцінка стійкості елемента КІС

Для експериментального дослідження визначимо типовий цикл роботи АС УПР протягом 12 год після дестабілізуючого впливу (наприклад, втрати каналу зв'язку чи технічного збою) та виділимо три характерні етапи функціонування системи:

- етап порушення роботи (0-2 год) – система працює у режимі зниженої ефективності, продуктивність становить $P(t)/P_{пот}=0.40$ від номінального значення;

- етап часткового відновлення (2-6 год) – після проведення коригувальних заходів працездатність підвищується до $P(t)/P_{пот}=0.70$;

- етап стабілізації (6-12 год) – система повертається до майже нормального функціонування, демонструючи продуктивність $P(t)/P_{пот}=0.95$ від номінальної.

Розрахунок індексу стійкості відповідно до (8):

$$RI_i=\frac{1}{T}\int_0^T\frac{P(t)}{P_{пот}}dt=\frac{1}{12}\left(\int_0^2 0.40\,dt+\int_2^6 0.70\,dt+\int_6^{12}0.95\,dt+\right)=$$

$$=\frac{1}{12}(0.8+2.8+5.7)=0.775,$$

Для складних систем АС УПР стійкість формується на кількох рівнях:

- технологічному (сервери, мережеве обладнання),

$$RI^{(\ell)}=0.78 \text{ та } \beta_\ell=0.5;$$

- інформаційному (цілісність та актуальність даних),

$$RI^{(\ell)}=0.80 \text{ та } \beta_\ell=0.3;$$

- організаційному (процедури, людський фактор),

$$RI^{(\ell)} = 0.72 \text{ та } \beta_\ell = 0.2.$$

Отже визначимо інтегральний показник стійкості як зважену сума часткових індексів, відповідно до (9), у наступному вигляді:

$$RI_{sys} = \sum_{\ell} \beta_\ell \cdot RI^{(\ell)} = 0.5 \cdot 0.78 + 0.3 \cdot 0.80 + 0.2 \cdot 0.72 = 0.774 .$$

Результати оцінювання стійкості елемента КІС з використанням програмного застосунку наведено на рис. 4.11.

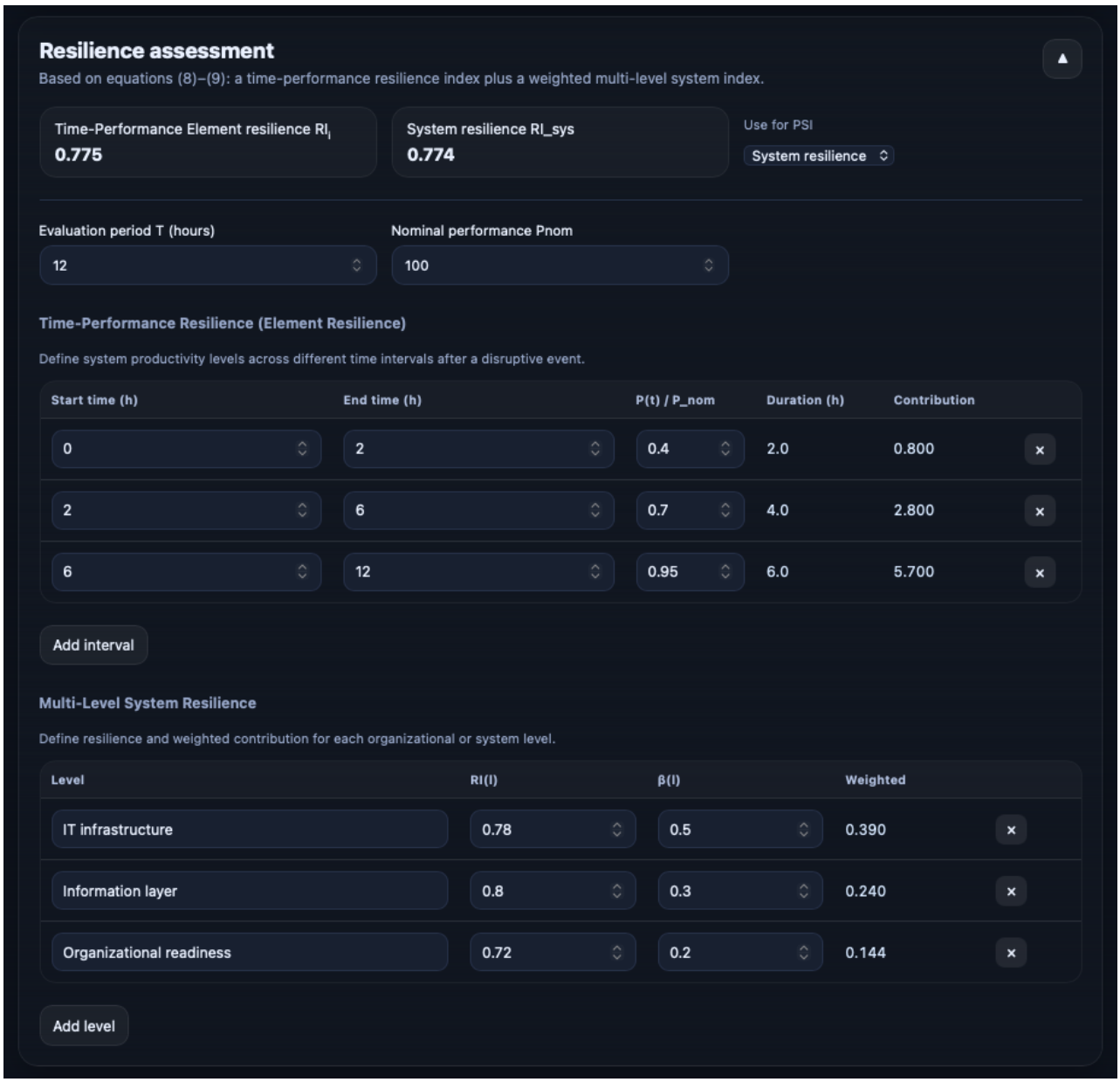

Рис. 4.11. Інтерфейс програмного застосунку при оцінюванні стійкості КІС

На рис. 4.11 представлено результати оцінювання стійкості, що відображають здатність системи відновлювати функціонування після дестабілізуючих впливів.

Етап 6. Інтегральна оцінка рівня захищеності КІС

На цьому етапі здійснюється об'єднання результатів трьох складових методу, а саме $RISK_i, R_i, RI_{sys}$ та вагових коефіцієнтів $\alpha = 0.4, \beta = 0.35, \gamma = 0.25$ у єдиний інтегральний показник рівня захищеності КІС. Крім того слід зазначити, що результати оцінювання ризику, надійності та стійкості елемента КІС приводяться до порівнянного вигляду шляхом нормування,

$$RISK_i = 1 - RISK_i = 1 - 0.383 = 0.617,\ R_i = R_i = 0.851,\ RI_i = RI_{sys} = 0.774.$$

$$PSI_i^{(0)} = \alpha \cdot RISK_i + \beta \cdot R_i + \gamma \cdot RI_i = 0.4 \cdot 0.617 + 0.35 \cdot 0.851 + 0.25 \cdot 0.774 = 0.738,$$

відповідно до Табл. 3.1 рівень значущості за $0,65 < PSI_i^{(0)} \le 0,85$ визначається як «обмежено забезпечує».

Результати оцінювання інтегральної оцінка рівня захищеності КІС з використанням програмного застосунку наведено на рис. 4.12.

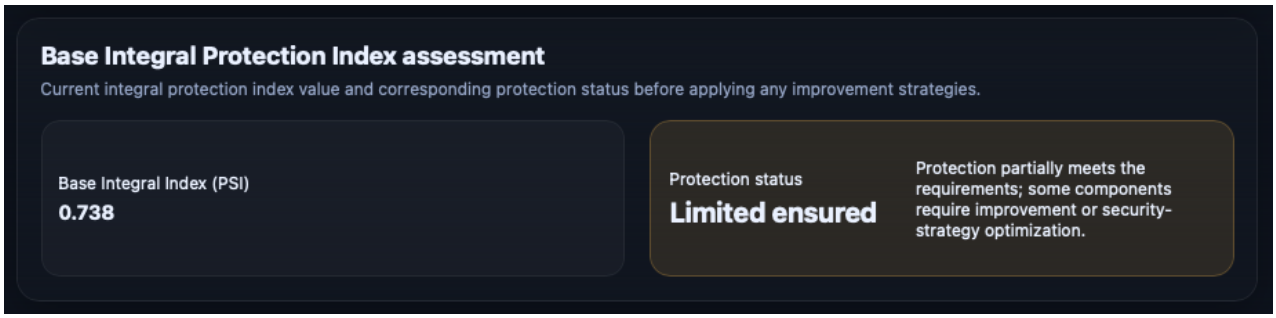

Рис. 4.12. Інтерфейс програмного застосунку при оцінюванні інтегральної оцінки рівня захищеності КІС

На рис. 4.12 представлено інтегральний показник рівня захищеності КІС, отриманий на основі узагальнення показників ризику, надійності та стійкості.

Етап 7. Оптимізація стратегій захищеності КІС

Для визначення оптимального набору стратегій, необхідно забезпечити відповідність елемента КІС нормативним критеріям надійності та стійкості. Відповідно до вимог ICAO та EUROCONTROL для критичних систем АС УПР, мінімально допустима імовірність безвідмовного функціонування повинна становити не менше $R_{\min} = 0.90$, а мінімально допустимий рівень стійкості $RI_{\min} = 0.80$. Отримані на попередніх етапах значення для елемента АС УПР: $R_i^* = 0.851 < 0.89$, $RI_{sys} = 0.774 < 0.80$, свідчать про невідповідність системи нормативним вимогам та необхідність впровадження коригувальних стратегій.

Доступний бюджет для реалізації заходів $B = 800$ тис. грн. У межах експериментального дослідження сформовано п’ять потенційних стратегій підвищення захищеності АС УПР. Кожна з них має певний вплив на показники ризику, надійності або стійкості (Табл. 4.29).

Таблиця 4.29

Стратегії підвищення захищеності АС УПР

Стратегія s_k	Опис заходу	Очікуваний вплив			Вартість C_k тис. грн
		RISK	R	RI	
s_1	Модернізація серверів АС УПР	0.02	0.12	0.04	1000
s_2	Резервування каналів зв’язку АТС	0.01	0.08	0.06	600
s_3	Впровадження автоматизованих процедур реагування	0.04	0.03	0.06	350
s_4	Захист мережевої інфраструктури від кібератак	0.05	0.08	0.03	500
s_5	Підвищення обізнаності персоналу	0.04	0	0.01	100
s_6	Організація сегментації шляхом впро-вадження рішення класу Zero-Trust	0.12	0.02	0.05	450

s_7	Впровадження архітектури високої доступності, інтегрованої в системи моніторингу та гарячого резервування	0.06	0.14	0.15	2000
s_8	Проведення заходів з перевірки ефективності систем та процедур реагування на кіберінциденти (Penetration Test, Red Teaming, Purple Teaming)	0.05	0.02	0.06	200
s_9	Розгортання платформи незмінного резервного копіювання	0.1	0.04	0.11	900

Вплив на показники ризику, надійності та стійкості.

У межах доступного бюджету визначено стратегії, які дозволяють досягти підвищення показників з максимальною ефективністю. В даному випадку це стратегії s_5, s_6, s_8.

Стратегії s_5, s_6, s_8 забезпечують зміну показників ризику, надійності та стійкості. Підвищення обізнаності персоналу, впровадження рішення Zero-Trust та проведення заходів з перевірки ефективності реагування на інциденти зменшує ризик впливу загроз на систему на $\triangle RISK_i = +0.04 + 0.12 + 0.05,$ а після її реалізації $RISK_i^*(s_5, s_6, s_8) = 0.617 + 0.21 = 0.827 \geq RISK_{\min},$ а також підвищує відповідно надійність $\triangle R_i = +0.02 + 0.02,$ $R_i^*(s_5, s_6, s_8) = 0.851 + 0.04 = 0.891 \geq R_{\min}$ та стійкість системи $\triangle RI_{sys} = +0.01 + 0.05 + 0.06,$ $RI_{sys}^*(s_5, s_6, s_8) = 0.774 + 0.12 = 0.894 \geq RI_{\min}.$

Таким чином, мінімально необхідний набір стратегій – це стратегії s_5, s_6, s_8. Перевірка бюджетних можливостей $C_{s_5} + C_{s_6} + C_{s_8} = 100 + 450 + 200 = 750 \leq B.$ Отже, обрана комбінація вкладається у доступний бюджет.

Інші стратегії є менш раціональними з точки зору впливу на показники або знаходяться поза межами доступного бюджету.

Далі повторно визначається об’єднання результатів трьох складових методу, а саме $RISK_i, R_i, RI_{sys}$ та вагових коефіцієнтів $\alpha = 0.4, \beta = 0.35, \gamma = 0.25$ у єдиний інтегральний показник рівня захищеності КІС.

Після впровадження стратегій оновлений інтегральний показник рівня захищеності дорівнює:

$$PSI_i^{(1)} = \alpha \cdot RISK_i + \beta \cdot R_i + \gamma \cdot RI_i = 0.4 \cdot 0.827 + 0.35 \cdot 0.891 + 0.25 \cdot 0.894 = 0.866,$$

відповідно до Табл. 3.1 рівень значущості за $0{,}85 < PSI_i^{(0)} \le 1{,}00$ визначається як «забезпечує».

Результати оптимізації стратегій захищеності КІС з використанням програмного застосунку наведено на рис. 4.13.

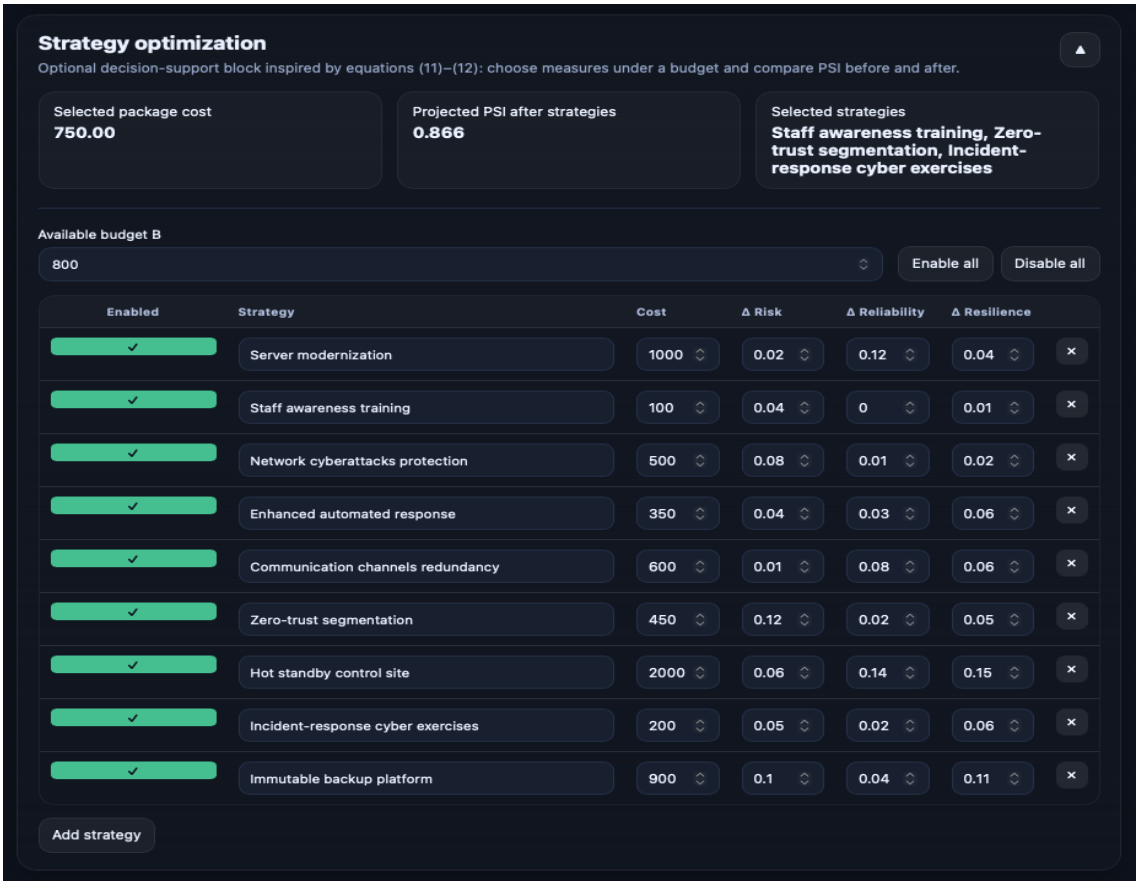

Рис. 4.13. Інтерфейс програмного застосунку при оптимізації стратегій захищеності КІС

На рис. 4.13 представлено результати оптимізації стратегій захищеності, що дозволяють обрати їх раціональну комбінацію з урахуванням бюджетних обмежень та впливу на показники системи.

Етап 8. Оцінка ефекту підвищення захищеності КІС

На цьому етапі визначається ефект підвищення рівня захищеності КІС у результаті реалізації оптимальних стратегій.

$$E_i = \frac{PSI_i^{(1)} - PSI_i^{(0)}}{PSI_i^{(0)}} \cdot 100\% = \frac{0.866 - 0.738}{0.738} \cdot 100\% = 17.3\%.$$

Результати оцінки ефекту підвищення захищеності КІС з використанням програмного застосунку наведено на рис. 4.14.

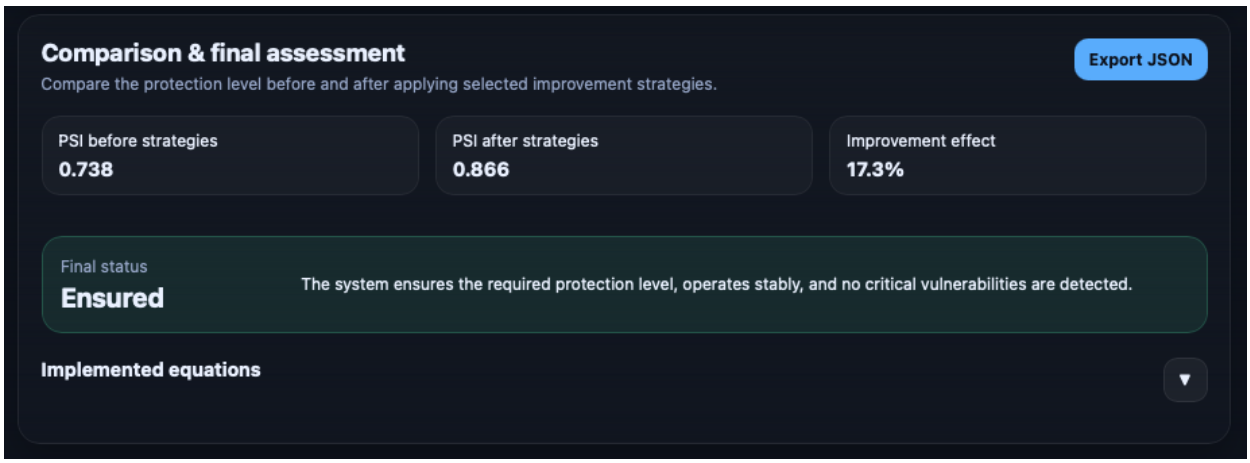

Рис. 4.14. Інтерфейс програмного застосунку при оцінці ефекту підвищення захищеності КІС

На рис. 4.14 представлено результати оцінювання ефекту підвищення рівня захищеності КІС після реалізації обраних стратегій.

Проведене експериментальне дослідження підтвердило ефективність запропонованого методу підвищення рівня захищеності КІС. На основі інтегральної оцінки ризику, надійності та стійкості визначено поточний стан системи та обґрунтовано потребу у впровадженні коригувальних заходів. Оптимізація стратегій дозволила обрати їх раціональну комбінацію, що забезпечує досягнення нормативних порогів та ефективне використання ресурсів.

Отримане підвищення інтегрального показника після реалізації стратегій підтверджує результативність запропонованого підходу. Розроблений метод забезпечує можливість кількісного оцінювання стану захищеності, прогнозування впливу загроз та вибору оптимальних заходів підвищення стійкості в умовах обмежених ресурсів.

З метою розширення області застосування та підтвердження універсальності запропонованого методу проведено додаткові експериментальні дослідження з використанням розробленого програмного застосунку для інших ОКІ транспортної галузі.

У межах дослідження здійснено верифікацію методу для системи управління безпекою залізничного руху (верифікація 2) [28-30] та міської автоматизованої системи керування рухом автотранспорту (верифікація 3) [31-35], що дозволило оцінити його ефективність у різних умовах функціонування систем.

Верифікація 2

Система управління безпекою залізничного руху

Результати Верифікації 2 для системи управління безпекою залізничного руху з використанням застосунку наведено на рис. 4.15-4.17 [28-30].

Рис. 4.15. Інтерфейс програмного застосунку для Верифікації 2 (частина 1)

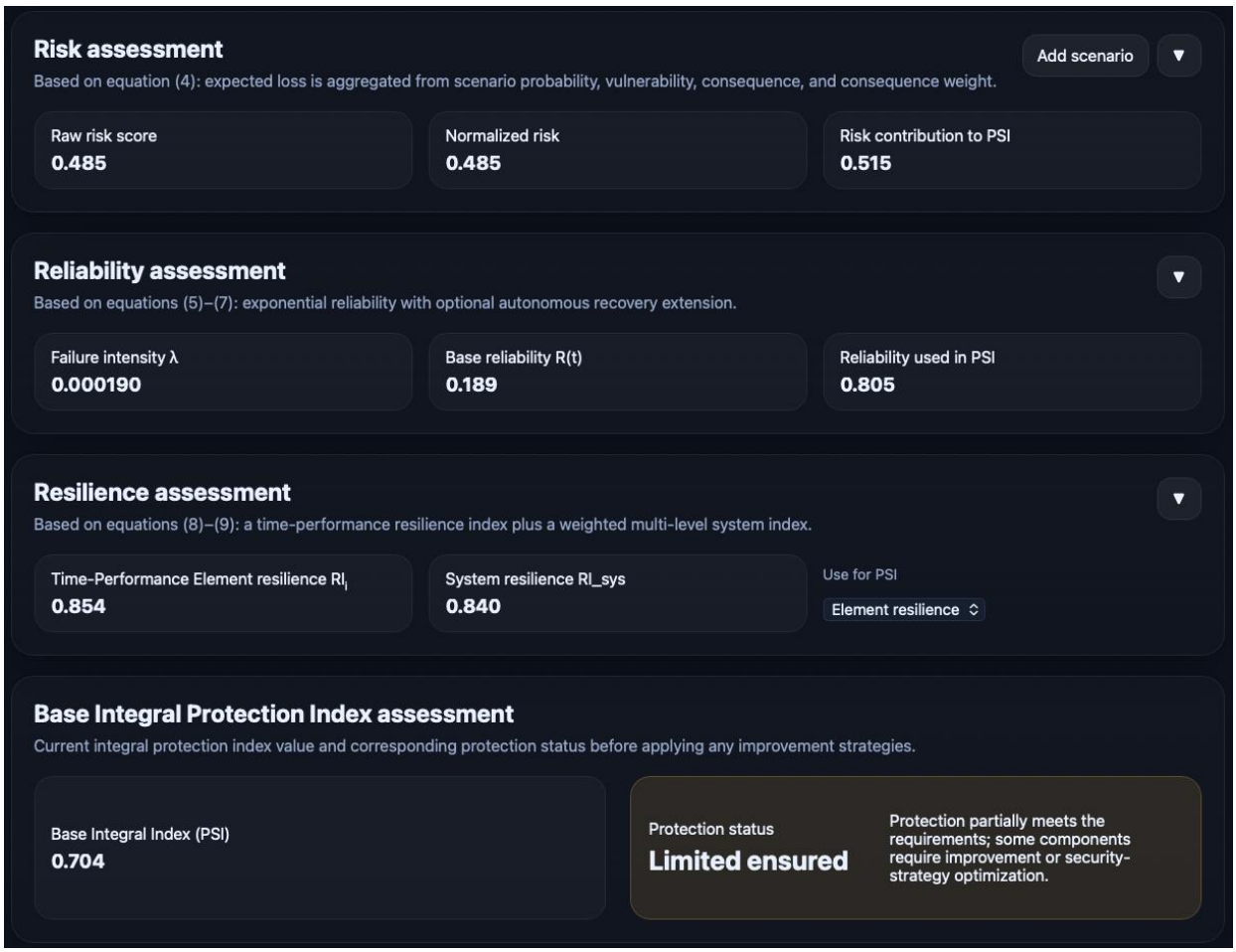

Рис. 4.16. Інтерфейс програмного застосунку для Верифікації 2 (частина 2)

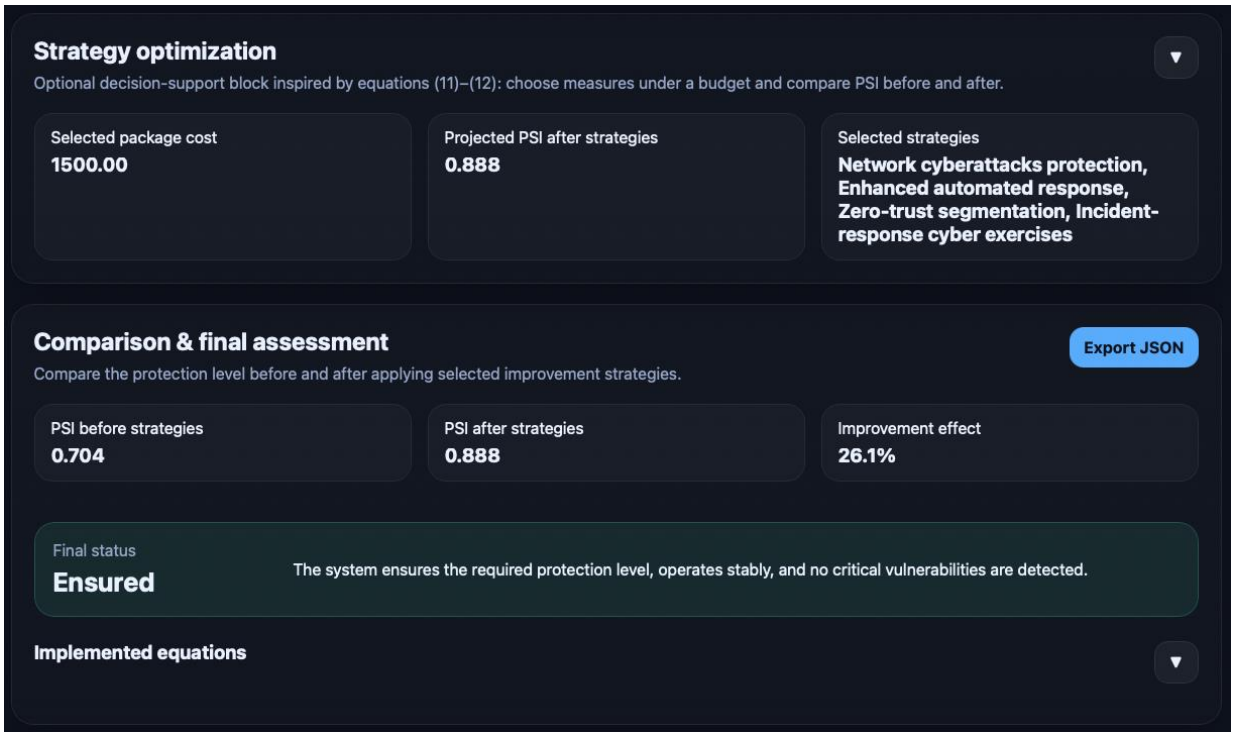

Рис. 4.17. Інтерфейс програмного застосунку для Верифікації 2 (частина 3)

На рис. 4.15-4.17 представлено результати верифікації методу для системи управління безпекою залізничного руху з використанням розробленого програмного застосунку. Отримані результати підтверджують можливість застосування запропонованого методу для оцінювання стану захищеності складних транспортних систем, що функціонують в умовах підвищених вимог до безпеки, надійності та стійкості. Встановлено, що врахування параметрів ризику, надійності, адаптивності та ресурсної забезпеченості дозволяє кількісно оцінювати зміну інтегрального показника захищеності системи, а також обґрунтовувати вибір раціональних стратегій реагування на дестабілізуючі впливи.

Верифікація 3

Міська автоматизована система керування рухом автотранспорту

Результати Верифікації 3 для міської автоматизованої системи керування рухом автотранспорту з використанням програмного застосунку наведено на рис. 4.18-4.20 [31-35].

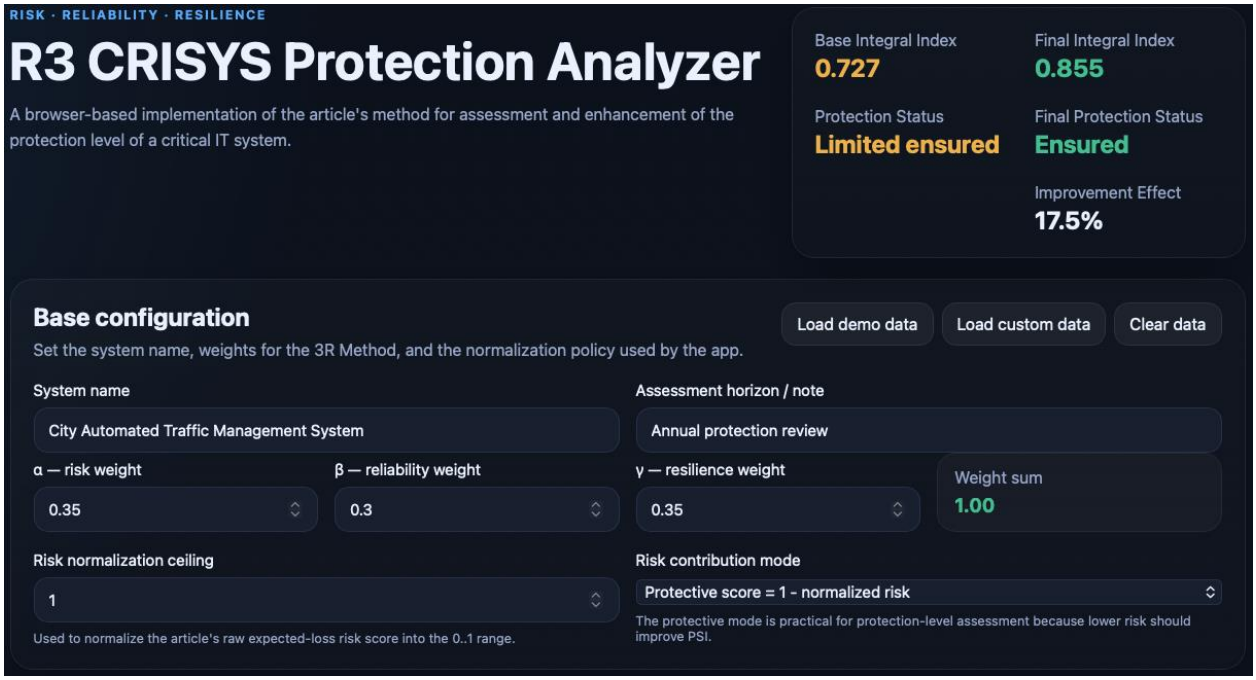

Рис. 4.18. Інтерфейс програмного застосунку для Верифікації 3 (частина 1)

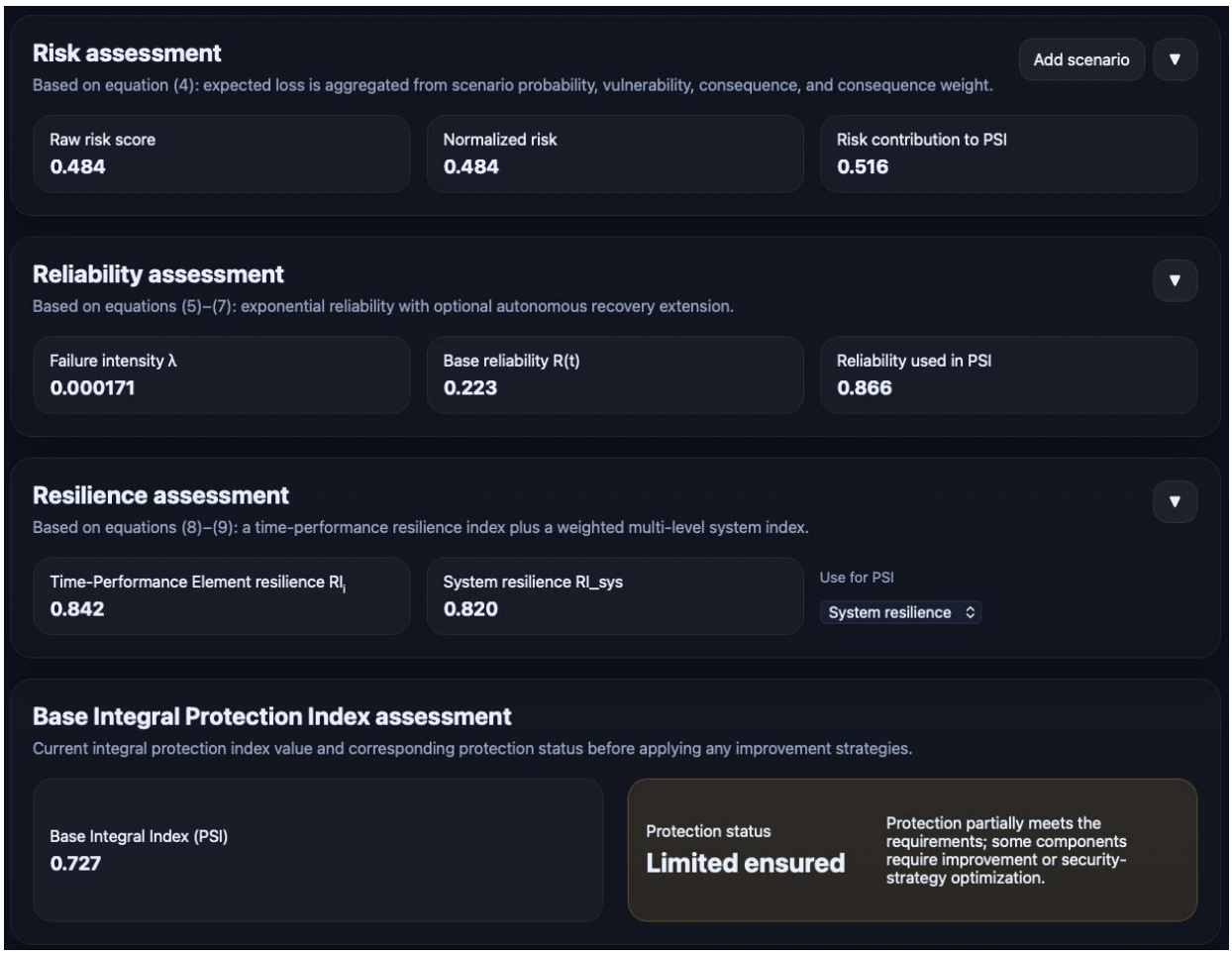

Рис. 4.19. Інтерфейс програмного застосунку для Верифікації 3 (частина 2)

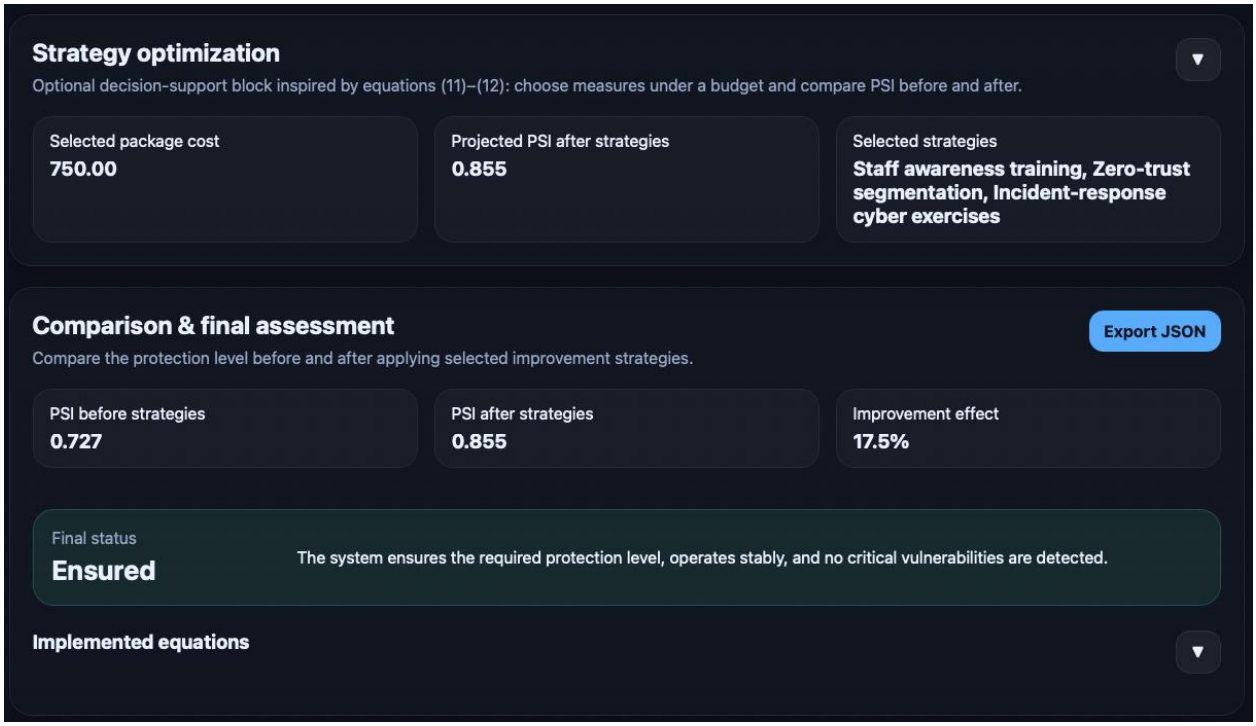

Рис. 4.20. Інтерфейс програмного застосунку для Верифікації 3 (частина 3)

На рис. 4.18-4.20 представлено результати верифікації методу для міської автоматизованої системи керування рухом автотранспорту. Отримані результати свідчать про можливість застосування запропонованого методу для оцінювання стану захищеності розподілених ІКС, функціонування яких залежить від динамічних зовнішніх умов та значної кількості взаємопов'язаних елементів. Встановлено, що врахування зміни параметрів функціонування системи, інтенсивності інцидентів та структурних взаємозалежностей дозволяє оцінювати зміну інтегрального показника захищеності та прогнозувати реакцію системи на дестабілізуючі впливи.

Проведена верифікація підтверджує ефективність запропонованого методу оцінювання впливу інцидентів на рівень захищеності ІКС КІ. Метод забезпечує можливість кількісного оцінювання впливу інцидентів на стан функціонування системи, аналізу сценаріїв розвитку подій та обґрунтування рішень щодо вибору заходів реагування і підвищення стійкості системи.

Загальні висновки за результатами Верифікації 1-3

У табл. 4.30 узагальнено результати верифікації запропонованого методу підвищення рівня захищеності КІС за трьома експериментальними сценаріями [21-35]. Порівняння значень інтегрального показника захищеності до та після реалізації стратегій дозволяє оцінити ефективність методу та результативність його застосування.

Таблиця 4.30

Результати верифікації методу підвищення рівня захищеності КІС

	Верифікація 1	**Верифікація 2**	**Верифікація 3**
КІС транспортного сектору	АС управління повітряним рухом	АС безпеки залізничного руху	АС керування рухом автотранспорту
Значення $PSI^{(0)}$	0.738	0.704	0.727

Рівень захищеності $PSI^{(0)}$	обмежено забезпечує	обмежено забезпечує	обмежено забезпечує
Значення $PSI^{(1)}$	0.866	0.888	0.855
Рівень захищеності $PSI^{(1)}$	забезпечує	забезпечує	забезпечує
Ефект підвищення, E_i	**17.3%**	**26.1%**	**17.5%**

Розроблене ПЗ забезпечує комплексне оцінювання стану ІКС, прогнозування впливу загроз та підтримку вибору раціональної сукупності організаційних і технічних заходів забезпечення захищеності ОКІІ.

Результати верифікацій 1-3, наведені в табл. 4.30, підтвердили працездатність та ефективність запропонованого методу підвищення рівня захищеності КІС для різних типів транспортних систем. Встановлено, що застосування методу забезпечує підвищення інтегрального показника захищеності на 17–26 %, що підтверджує результативність запропонованих стратегій та обґрунтованість рішень щодо розподілу ресурсів.

Проведене експериментальне дослідження також підтвердило універсальність запропонованого підходу щодо його застосування до КІС із різною топологією взаємозв’язків, характеристиками загроз та умовами функціонування, що свідчить про можливість його використання для підтримки прийняття рішень у задачах підвищення захищеності ОКІ.

Практичні рекомендації щодо вибору раціональної сукупності організаційних і технічних заходів захисту об’єктів КІІ

За результатами експериментальної апробації ***сформовано практичні рекомендації*** щодо вибору раціональної сукупності організаційних і технічних заходів захисту об’єктів КІІ (рис. 4.21).

Практичні рекомендації передбачають:

– поетапне впровадження заходів з урахуванням критичності функцій та рівня ризику;

– пріоритизацію інвестицій у заходи, що забезпечують максимальне зниження інтегрального ризику при мінімальних ресурсних витратах;

– поєднання технічних рішень (резервування, модернізація інфраструктури, посилення кіберзахисту) з організаційними заходами (регламентація процедур реагування, підготовка персоналу);

– забезпечення адаптивності системи захисту до зміни умов середовища та характеру загроз.

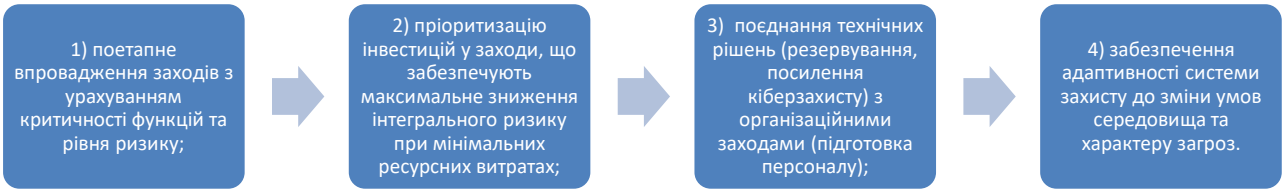

Рис. 4.21. Практичні рекомендації щодо вибору раціональної сукупності організаційних і технічних заходів захисту об’єктів КІІ

Сформовані рекомендації можуть бути використані операторами КІІ для обґрунтованого прийняття управлінських рішень щодо вибору раціональних стратегій підвищення рівня захищеності в умовах воєнних і гібридних загроз.

4.4. Висновки до четвертого розділу

Таким чином, у четвертому розділі на основі запропонованих методик та розробленого спеціалізованого програмного застосунку проведено експериментальне дослідження та верифіковано розроблені у роботі методи: оцінювання ефективності функціонування систем безпеки взаємозалежних

критичних інфраструктур, оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем, а також підвищення рівня захищеності критичних інформаційних систем. Отримані результати підтвердили їх працездатність, адекватність та ефективність при аналізі функціонування систем у різних умовах.

4.5. Список літератури до другого розділу

1. Гнатюк С.О., Сидоренко В.М., Березовий І.Р., Сидоренко С.Ю., Тараненко К.О. Модель оцінювання ефективності функціонування систем інформаційної безпеки взаємозалежних критичних інфраструктур. Проблеми інформатизації та управління. 2022. Т. 4. № 72. С. 17-25. DOI: https://doi.org/10.18372/2073-4751.72.17457.

2. Lutskyi M., Sydorenko V., Polozhentsev A., Apenko N., Sydorenko S. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures. CEUR Workshop Proceedings. 2023. Vol. 3421. P. 214-222. URL: https://ceur-ws.org/Vol-3421/short7.pdf

3. Limnios N., Oprisan G. Semi-Markov Processes and Reliability. Boston: Birkhäuser, 2001.

4. Nozick L., Turnquist M., Jones D., Davis J., Lawton C. Assessing the Performance of Interdependent Infrastructures and Optimizing Investment. Proceedings of the 37th Hawaii International Conference on System Sciences. 2004.

5. Xu N., Nozick L. K., Turnquist M. A., Jones D. A. Optimizing Investment for Recovery in Interdependent Infrastructure. Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS’07). Waikoloa, HI, USA, 2007. P. 112–112. DOI: 10.1109/HICSS.2007.413.

6. Boyer S. A. SCADA: Supervisory Control and Data Acquisition. 4th ed. USA: ISA – International Society of Automation, 2010. 179 p.

7. Abbas H. A., Mohamed A. M. Review in the design of web-based SCADA systems based on OPC DA protocol. International Journal of Computer Networks. 2011. Vol. 2, No. 6. P. 266–277.

8. Gürkan G., Ozge Y., Robinson S. Sample Path Optimization in Simulation. Proceedings of the 1994 Winter Simulation Conference. 1994. P. 247-254.

9. Law A. M. *Simulation Modeling and Analysis.* 5th ed. New York: McGraw-Hill, 2015. 784 p.

10. Rubinstein R. Y., Kroese D. P. *Simulation and the Monte Carlo Method.* 3rd ed. Hoboken, NJ: Wiley, 2016. 398 p.

11. Banks J., Carson J. S., Nelson B. L., Nicol D. M. *Discrete-Event System Simulation.* 5th ed. Upper Saddle River, NJ: Pearson, 2010. 640 p.

12. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів IT-інцидентів на об'єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління. 2024. Т. 2. №78. С. 104-114. DOI: https://doi.org/10.18372/2073-4751.78.18967.

13. Gnatyuk S., Sydorenko V., Polozhentsev A., Sydorenko S. Experimental Study of the Method for Cyber Incidents Management in Aviation Critical Infrastructure. In: Ostroumov, I., Marais, K., Zaliskyi, M. (eds) Advances in Civil Aviation Systems Development. ACASD 2025. Lecture Notes in Networks and Systems, Vol. 1418. P. 74–91, Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-91992-3_6.

14. Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Смірнова Т.В., Сидоренко С.Ю. Модель визначення критичності галузевих інформаційно-телекомунікаційних систем. Проблеми інформатизації та управління. 2022. Т. 2. № 70. С. 28-37. DOI: https://doi.org/10.18372/2073-4751.70.16844.

15. Жигаревич О.К., Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю. Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи». Кіберзахист особи, суспільства і держави: наук.-практ. конф., с. Велятино, 24-27 січня 2024 р.: тези доп., Київ: НАУ, 2024. С. 14-15.

16. IEC 62443-3-3:2013. Security for Industrial Automation and Control Systems – System Security Requirements and Security Levels. Geneva: International Electrotechnical Commission, 2013.

17. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82 Rev.

3). Gaithersburg, MD: National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.SP.800-82r3.

18. Panteli, M., Mancarella, P. The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. IEEE Power & Energy Magazine. 2015. Vol. 13, No. 3. P. 58–66.

19. Nosal K., Solecka K. Application of AHP Method for Multi-Criteria Evaluation of Variants of the Integration of Urban Public Transport. Transportation Research Procedia. 2014. Vol. 3. P. 269–278. DOI: 10.1016/j.trpro.2014.10.006.

20. Saaty T. L. Decision Making with the Analytic Hierarchy Process. International Journal of Services Sciences. 2008. Vol. 1, No. 1. P. 83–98. DOI: 10.1504/IJSSCI.2008.017590.

21. Сидоренко В. М., Сидоренко С. Ю. Метод підвищення рівня захищеності критичних інформаційних систем держави. Кібербезпека: освіта, наука, техніка. 2025. Т. 2. № 30. С. 500–510. DOI: https://doi.org/10.28925/2663-4023.2025.30.988.

22. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20.

23. Кабінет Міністрів України. «Деякі питання забезпечення безпеки та стійкості критичної інфраструктури». Постанова від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2021-п.

24. ICAO. Annex 17 to the Convention on International Civil Aviation — Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference. Montreal: ICAO, latest ed.

25. EUROCONTROL. European Air Traffic Management Master Plan / Guidelines for ATM Cybersecurity. Brussels: EUROCONTROL.

26. EASA. Easy Access Rules for Air Traffic Management / Air Navigation Services (ATM/ANS), including cybersecurity provisions. Cologne: European Union Aviation Safety Agency.

27. ICAO. Procedures for Air Navigation Services — Air Traffic Management (Doc 4444).

28. EN 50126-1:2017. Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Brussels: CENELEC, 2017.

29. European Union Agency for Railways. Cybersecurity in the Railway Sector. Luxembourg: Publications Office of the European Union, 2020.

30. ERTMS Users Group. ETCS System Requirements Specification (Subset-026). Brussels, latest ed.

31. ISO 14813-1:2015. Intelligent Transport Systems — Reference Model Architecture(s) for the ITS Sector. Geneva: International Organization for Standardization, 2015.

32. ENISA. Cybersecurity and Resilience of Smart Cars and Intelligent Transport Systems.

33. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82 Rev. 3). Gaithersburg, MD: National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.SP.800-82r3.

34. Panteli, M., Mancarella, P. The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. IEEE Power & Energy Magazine. 2015. Vol. 13, No. 3. P. 58–66.

35. Nosal K., Solecka K. Application of AHP Method for Multi-Criteria Evaluation of Variants of the Integration of Urban Public Transport. Transportation Research Procedia. 2014. Vol. 3. P. 269–278. DOI: 10.1016/j.trpro.2014.10.006.

ВИСНОВКИ

Результатом виконаної дисертаційної роботи є розв’язання актуальної та важливої науково-технічної задачі розроблення методів оцінювання ефективності та захищеності інформаційно-комунікаційних систем критичної інфраструктури держави.

У процесі виконання дисертаційної роботи отримані такі наукові та практичні результати:

1. Проведено аналіз сучасних підходів до оцінювання ефективності функціонування систем безпеки ВКІ, який показав, що існуючі методи базуються на теорії надійності, ризик-аналізі, оптимізації та стохастичному моделюванні, однак лише частково враховують взаємозалежності об’єктів критичної інфраструктури, що не забезпечує комплексного урахування динаміки функціонування систем і обґрунтованого розподілу ресурсів. Аналіз підходів до оцінювання впливу інцидентів показав, що існуючі рішення орієнтовані на оцінювання ризиків і пріоритизацію інцидентів, однак не забезпечують формалізованого взаємозв’язку між їх характеристиками та станом системи і обмежують інтегроване врахування їх впливу. Аналіз підходів до підвищення рівня захищеності показав, що сучасні дослідження зосереджені на окремих складових (ризику, надійності, стійкості), однак не забезпечують комплексного врахування їх взаємозв’язків та оптимізації стратегій захисту в умовах обмежених ресурсів. Проведений аналіз дозволив сформулювати завдання дисертаційного дослідження щодо розроблення та вдосконалення відповідних методів оцінювання та підвищення захищеності інформаційно-комунікаційних систем критичної інфраструктури держави.

2. Удосконалено метод оцінювання ефективності функціонування систем безпеки взаємозалежних критичних інфраструктур, за рахунок використання графового подання взаємозалежностей об’єктів, марківських і

напівмарківських процесів моделювання станів, забезпечує оцінювання ймовірнісних характеристик функціонування системи та обґрунтування розподілу інвестицій у забезпечення безпеки об’єктів критичної інфраструктури. Крім того, сформовано практичні рекомендації щодо раціонального розподілу інвестицій та ресурсів з урахуванням наявних обмежень. Отримані результати експериментального дослідження показали, що значення ймовірності забезпечення заданого рівня ефективності варіюється в межах P_{sat}=0.39–0.78 залежно від структури взаємозв’язків та рівня резервування, при цьому приріст показника становить ΔP=0.16–0.22.

3. Удосконалено метод оцінювання впливу інцидентів на рівень захищеності інформаційно-комунікаційних систем критичної інфраструктури, який за рахунок формалізації взаємозв’язку між характеристиками інцидентів та параметрами стану системи, а також використання вагових коефіцієнтів їх впливу, дозволяє кількісно враховувати вплив інцидентів на інтегральний показник захищеності та оцінювати загальний стан функціонування системи. На основі розробленого методу сформовано методику оцінювання впливу інцидентів, що дозволяє враховувати їх наслідки при прийнятті рішень щодо управління функціонуванням інформаційно-комунікаційних систем.

4. Отримав подальшого розвитку метод підвищення рівня захищеності КІС, який завдяки формалізації взаємозв’язків між ризиком, надійністю та стійкістю, використанню інтегрального показника рівня захищеності та врахуванню технічних і організаційних факторів, дає можливість здійснювати комплексне оцінювання стану системи, прогнозування впливу загроз і оптимізацію стратегій підвищення стійкості в умовах обмежених ресурсів. Розроблено програмне забезпечення, яке забезпечує комплексне оцінювання стану інформаційно-комунікаційних систем, прогнозування впливу загроз, а також сформовано практичні рекомендації щодо вибору раціональної сукупності організаційних і

технічних заходів функціонування об’єктів критичної інформаційної інфраструктури. Отримані результати експериментального дослідження показали, що застосування методу забезпечує підвищення рівня захищеності КІС транспортного сектору на 17–26%, що підтверджує ефективність методу та обґрунтованість обраних стратегій підвищення захищеності.

5. На основі запропонованих методик та розробленого спеціалізованого програмного забезпечення проведено експериментальне дослідження та верифіковано розроблені у роботі методи. Результати дисертації впроваджені і використовуються у діяльності ТОВ «AxxonSoft» (акт про впровадження від 13.03.2026) та у НДЛ протидії кіберзагрозам авіаційної галузі КАІ (акт про впровадження від 14.04.2026) для вирішення прикладних завдань забезпечення сталого функціонування інформаційно-комунікаційних систем.

Додаток А

Документи, що підтверджують впровадження результатів дисертації

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «АККСОН СОФТ»
Адреса для листування:
04119, Україна, м. Київ, вул. Дегтярівська, буд. 25-А, корп. 1, оф. 414
Код ЄДРПОУ 37818589
IBAN UA053348510000000026008260738,
в АТ «ПУМБ» м. Київ, МФО 334851
https://ua.axxonsoft.com/
тел.+38044 333-71-90, моб. +38 068 333 71 90

АКТ ВПРОВАДЖЕННЯ

результатів дисертаційної роботи **Сидоренка Сергія Юрійовича** на тему: «Методи оцінювання ефективності та захищеності інформаційно-комунікаційних систем критичної інфраструктури держави» подану на здобуття наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології», за спеціальністю 122 «Комп'ютерні науки»

Результати наукового дослідження впроваджені у діяльність ТОВ «АККСОН СОФТ». У практичній діяльності підприємства використано метод підвищення рівня захищеності критичних інформаційних систем. Запропонований метод базується на формалізації взаємозв'язків між ризиком, надійністю та стійкістю і забезпечує інтегральну кількісну оцінку стану безпеки.

Використання методу забезпечує інтегральну кількісну оцінку стану безпеки та оптимізацію стратегій підвищення стійкості в умовах обмежених ресурсів. Крім того, сформовано практичні рекомендації щодо вибору раціональної сукупності заходів захисту об'єктів критичної інформаційної інфраструктури.

Директор
ТОВ «АККСОН СОФТ» **Курінний О.В.**

ЗАТВЕРДЖУЮ
Проректор з наукових досліджень та
трансферу технологій
Державного університету
«Київський авіаційний інститут»
_____ С.О. Гнатюк
«14» 04 2026 року

АКТ
впровадження у науково-дослідну діяльність
результатів дисертаційної роботи Сидоренка Сергія Юрійовича
«Методи оцінювання ефективності та захищеності інформаційно-комунікаційних систем критичної інфраструктури держави» на здобуття наукового ступеня доктора філософії

Комісія у складі: голова – провідний науковий співробітник Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі к.т.н., ст. дослідник Охріменко Т.О., науковий співробітник, PhD, Положенцев А.А., молодший науковий співробітник Поліщук Ю.Я., склали даний акт про те, що результати дисертаційної роботи Сидоренка Сергія Юрійовича, впроваджені у науково-дослідну діяльність та використовуються в Науково-дослідній лабораторії протидії кіберзагрозам в авіаційній галузі за темою «Методи, моделі та програмні засоби управління інцидентами кібербезпеки в критичній інфраструктурі держави» (держ. реєстр. №0125U000624).

№ з/п	Назва роботи, що впроваджується	Форма впровадження	Ефективність від впровадження
	1	2	3
1.	Метод оцінювання ефективності функціонування систем інформаційної безпеки взаємозалежних критичних інфраструктур	Методичні матеріали та математичний апарат, використані при виконанні етапів НДР №0125U000624	Забезпечує оцінювання ймовірнісних характеристик функціонування системи та обґрунтування розподілу інвестицій у забезпечення безпеки об'єктів критичної інфраструктури.
2.	Практичні рекомендації щодо раціонального розподілу інвестицій та ресурсів з урахуванням наявних обмежень.	Наукові результати, впроваджені у межах НДР	Сформовані рекомендації можуть бути використані операторами КІ для раціонального розподілу інвестицій та ресурсів у системах інформаційної безпеки взаємозалежних критичних інфраструктур.

Голова комісії,

к.т.н., ст. дослідник
п.н.с. НДЛ протидії кіберзагрозам
в авіаційній галузі Тетяна ОХРІМЕНКО

Члени комісії:

PhD, н.с НДЛ протидії кіберзагрозам
в авіаційній галузі Артем ПОЛОЖЕНЦЕВ

м.н.с НДЛ протидії кіберзагрозам
в авіаційній галузі Юлія ПОЛІЩУК

Додаток Б

Лістинги (код) програмного забезпечення

App.js

```
// R3 CRISYS Protection Analyzer
//version 1.0.3

const thresholds = [
  {
    minExclusive: 0.85,
    maxInclusive: 1.0,
    label: 'Ensured',
    className: 'good',
    description:
      'The system ensures the required protection level, operates stably, and no critical vulnerabilities are detected.',
  },
  {
    minExclusive: 0.65,
    maxInclusive: 0.85,
    label: 'Limited ensured',
    className: 'medium',
    description:
      'Protection partially meets the requirements; some components require improvement or security-strategy optimization.',
  },
  {
    minExclusive: -Infinity,
    maxInclusive: 0.65,
    label: 'Not ensured',
    className: 'bad',
    description:
      'The protection level is insufficient; the system has significant vulnerabilities and requires additional resilience measures.',
  },
];

const demoData = {
```

```
  systemName: 'Automated Air Traffic Control System',
  assessmentNote: 'Quarterly protection review',
  alpha: 0.4,
  beta: 0.35,
  gamma: 0.25,
  riskCeiling: 1,
  riskMode: 'protective',
  failures: 3,
  observationTime: 26280,
  targetTime: 8760,
  blackStart: 0.85,
  islandReliability: 0.9,
  useExtendedReliability: 'yes',
  nominalPerformance: 100,
  evaluationPeriod: 12,
  resilienceMode: 'system',
  budget: 800,
  objectWeight: 1,
  resilienceIntervals: [
    { start: 0, end: 2, productivity: 0.40 },
    { start: 2, end: 6, productivity: 0.70 },
    { start: 6, end: 12, productivity: 0.95 },
  ],
  riskRows: [
    { name: 'Cyber attack. Lateral movement', p: 0.1, v: 0.8, c1: 0.95, c2: 0.85, w1: 0.7,
w2: 0.3 },
    { name: 'Cyber attack. Out of Control', p: 0.12, v: 0.75, c1: 0.9, c2: 0.8, w1: 0.7, w2:
0.3 },
    { name: 'Communication. Channel disruption', p: 0.06, v: 0.70, c1: 0.85, c2: 0.60, w1:
0.7, w2: 0.3 },
    { name: 'Communication. Quality degradation', p: 0.05, v: 0.65, c1: 0.80, c2: 0.55, w1:
0.7, w2: 0.3 },
    { name: 'Equipment failure. End of Life/Support', p: 0.04, v: 0.85, c1: 0.95, c2: 0.70,
w1: 0.7, w2: 0.3 },
    { name: 'Equipment failure. Database crash', p: 0.07, v: 0.60, c1: 0.75, c2: 0.50, w1:
0.7, w2: 0.3 },
    { name: 'Human factor. Out of resources', p: 0.10, v: 0.50, c1: 0.70, c2: 0.45, w1: 0.7,
w2: 0.3 },
```

```
    { name: 'Human factor. Unintentional mistake', p: 0.08, v: 0.55, c1: 0.65, c2: 0.40, w1:
0.7, w2: 0.3 },
    { name: 'External impact. Blackout', p: 0.05, v: 0.60, c1: 0.80, c2: 0.65, w1: 0.7, w2:
0.3 },
    { name: 'External impact. Military ops', p: 0.07, v: 0.70, c1: 0.85, c2: 0.55, w1: 0.7, w2:
0.3 },

  ],
  resilienceRows: [
    { name: 'IT infrastructure', score: 0.78, weight: 0.5 },
    { name: 'Information layer', score: 0.8, weight: 0.3 },
    { name: 'Organizational readiness', score: 0.72, weight: 0.2 },
  ],
  strategyRows: [
    { name: 'Server modernization', cost: 1000, risk: 0.02, reliability: 0.12, resilience: 0.04
},
    { name: 'Staff awareness training', cost: 100, risk: 0.04, reliability: 0.0, resilience: 0.01
},
    { name: 'Network cyberattacks protection', cost: 500, risk: 0.08, reliability: 0.01,
resilience: 0.02 },
    { name: 'Enhanced automated response', cost: 350, risk: 0.04, reliability: 0.03,
resilience: 0.06 },
    { name: 'Communication channels redundancy', cost: 600, risk: 0.01, reliability: 0.08,
resilience: 0.06 },
    { name: 'Zero-trust segmentation', cost: 450, risk: 0.12, reliability: 0.02, resilience:
0.05 },
    { name: 'Hot standby control site', cost: 2000, risk: 0.06, reliability: 0.14, resilience:
0.15 },
    { name: 'Incident-response cyber exercises', cost: 200, risk: 0.05, reliability: 0.02,
resilience: 0.06 },
    { name: 'Immutable backup platform', cost: 900, risk: 0.10, reliability: 0.04, resilience:
0.11 },
  ],
};

const els = {
  systemName: document.getElementById('systemName'),
  assessmentNote: document.getElementById('assessmentNote'),
```

```
alpha: document.getElementById('alpha'),
beta: document.getElementById('beta'),
gamma: document.getElementById('gamma'),
riskCeiling: document.getElementById('riskCeiling'),
riskMode: document.getElementById('riskMode'),
failures: document.getElementById('failures'),
observationTime: document.getElementById('observationTime'),
targetTime: document.getElementById('targetTime'),
blackStart: document.getElementById('blackStart'),
islandReliability: document.getElementById('islandReliability'),
useExtendedReliability: document.getElementById('useExtendedReliability'),
currentPerformance: document.getElementById('currentPerformance'),
nominalPerformance: document.getElementById('nominalPerformance'),
evaluationPeriod: document.getElementById('evaluationPeriod'),
budget: document.getElementById('budget'),
objectWeight: document.getElementById('objectWeight'),
weightSum: document.getElementById('weightSum'),
rawRiskValue: document.getElementById('rawRiskValue'),
normalizedRiskValue: document.getElementById('normalizedRiskValue'),
riskContributionValue: document.getElementById('riskContributionValue'),
lambdaValue: document.getElementById('lambdaValue'),
baseReliabilityValue: document.getElementById('baseReliabilityValue'),
usedReliabilityValue: document.getElementById('usedReliabilityValue'),
elementResilienceValue: document.getElementById('elementResilienceValue'),
systemResilienceValue: document.getElementById('systemResilienceValue'),
resilienceMode: document.getElementById('resilienceMode'),
psiValue: document.getElementById('psiValue'),
psiLabel: document.getElementById('psiLabel'),
psiEffect: document.getElementById('psiEffect'),
finalPsiValue: document.getElementById('finalPsiValue'),
finalPsiLabel: document.getElementById('finalPsiLabel'),
currentPsiValue: document.getElementById('currentPsiValue'),
currentStatusLabel: document.getElementById('currentStatusLabel'),
currentResultBand: document.getElementById('currentResultBand'),
currentBandDescription: document.getElementById('currentBandDescription'),
projectedPsiValue: document.getElementById('projectedPsiValue'),
selectedCostValue: document.getElementById('selectedCostValue'),
selectedStrategiesValue: document.getElementById('selectedStrategiesValue'),
```

```
  beforePsiValue: document.getElementById('beforePsiValue'),
  afterPsiValue: document.getElementById('afterPsiValue'),
  improvementEffectValue: document.getElementById('improvementEffectValue'),
  finalResultBand: document.getElementById('finalResultBand'),
  finalBandLabel: document.getElementById('finalBandLabel'),
  finalBandDescription: document.getElementById('finalBandDescription'),
  bandLabel: document.getElementById('bandLabel'),
  bandDescription: document.getElementById('bandDescription'),
  resultBand: document.getElementById('resultBand'),
  riskTableBody: document.getElementById('riskTableBody'),
  resilienceIntervalTableBody: document.getElementById('resilienceIntervalTableBody'),
  resilienceTableBody: document.getElementById('resilienceTableBody'),
  strategyTableBody: document.getElementById('strategyTableBody'),
  loadSampleBtn: document.getElementById('loadSampleBtn'),
  loadCustomDataBtn: document.getElementById('loadCustomDataBtn'),
  clearDataBtn: document.getElementById('clearDataBtn'),
  importJsonInput: document.getElementById('importJsonInput'),
  addRiskRowBtn: document.getElementById('addRiskRowBtn'),
  addResilienceIntervalBtn: document.getElementById('addResilienceIntervalBtn'),
  addResilienceRowBtn: document.getElementById('addResilienceRowBtn'),
  addStrategyRowBtn: document.getElementById('addStrategyRowBtn'),
  enableAllStrategiesBtn: document.getElementById('enableAllStrategiesBtn'),
  disableAllStrategiesBtn: document.getElementById('disableAllStrategiesBtn'),
  downloadJsonBtn: document.getElementById('downloadJsonBtn'),
};

const templates = {
  risk: document.getElementById('riskRowTemplate'),
  resilienceInterval: document.getElementById('resilienceIntervalTemplate'),
  resilience: document.getElementById('resilienceRowTemplate'),
  strategy: document.getElementById('strategyRowTemplate'),
};

function numberValue(input, fallback = 0) {
  if (!input) {
    return fallback;
  }
  const value = parseFloat(input.value);
```

```
  return Number.isFinite(value) ? value : fallback;
}

function clamp(value, min = 0, max = 1) {
  return Math.min(Math.max(value, min), max);
}

function formatNumber(value, digits = 3) {
  return Number.isFinite(value) ? value.toFixed(digits) : '0.000';
}

function formatPercent(value, digits = 1) {
  return `${formatNumber(value, digits)}%`;
}

function autoResizeStrategyName(textarea) {
  textarea.style.height = 'auto';
  textarea.style.height = (textarea.scrollHeight) + 'px';
}

function createRow(type, values = {}) {
  const fragment = templates[type].content.cloneNode(true);
  const row = fragment.querySelector('tr');

  if (type === 'risk') {
    row.querySelector('.risk-name').value = values.name ?? 'Scenario';
    row.querySelector('.risk-p').value = values.p ?? 0.25;
    row.querySelector('.risk-v').value = values.v ?? 0.30;
    row.querySelector('.risk-c1').value = values.c1 ?? 0.60;
    row.querySelector('.risk-w1').value = values.w1 ?? 0.50;
    row.querySelector('.risk-c2').value = values.c2 ?? 0.60;
    row.querySelector('.risk-w2').value = values.w2 ?? 0.50;
    els.riskTableBody.appendChild(row);
  }

  if (type === 'resilienceInterval') {
    row.querySelector('.interval-start').value = values.start ?? 0;
    row.querySelector('.interval-end').value = values.end ?? 2;
```

```
  row.querySelector('.interval-productivity').value = values.productivity ?? 0.5;
  els.resilienceIntervalTableBody.appendChild(row);
}

if (type === 'resilience') {
  row.querySelector('.resilience-name').value = values.name ?? 'IT infrastructure';
  row.querySelector('.resilience-score').value = values.score ?? 0.88;
  row.querySelector('.resilience-weight').value = values.weight ?? 0.34;
  els.resilienceTableBody.appendChild(row);
}

if (type === 'strategy') {
  row.querySelector('.strategy-enabled').checked = values.enabled !== false;
  const nameTextarea = row.querySelector('.strategy-name');
  nameTextarea.textContent = values.name ?? 'Strategy';
  nameTextarea.value = values.name ?? 'Strategy';

  // Set up auto-resize on input
  nameTextarea.addEventListener('input', function() {
    autoResizeStrategyName(this);
    recalculate();
  });

  // Initial resize
  autoResizeStrategyName(nameTextarea);

  row.querySelector('.strategy-cost').value = values.cost ?? 50;
  row.querySelector('.strategy-risk').value = values.risk ?? 0.05;
  row.querySelector('.strategy-reliability').value = values.reliability ?? 0.03;
  row.querySelector('.strategy-resilience').value = values.resilience ?? 0.04;
  els.strategyTableBody.appendChild(row);
}

row.addEventListener('input', recalculate);
row.querySelector('.remove-row-btn').addEventListener('click', () => {
  row.remove();
  recalculate();
});
```

```
}

function getRiskRows() {
  return [...els.riskTableBody.querySelectorAll('tr')].map((row) => ({
    row,
    name: row.querySelector('.risk-name').value.trim(),
    p: clamp(numberValue(row.querySelector('.risk-p'))),
    v: clamp(numberValue(row.querySelector('.risk-v'))),
    c1: clamp(numberValue(row.querySelector('.risk-c1'))),
    w1: clamp(numberValue(row.querySelector('.risk-w1'))),
    c2: clamp(numberValue(row.querySelector('.risk-c2'))),
    w2: clamp(numberValue(row.querySelector('.risk-w2'))),
  }));
}

function getResilientIntervalRows() {
  return [...els.resilienceIntervalTableBody.querySelectorAll('tr')].map((row) => ({
    row,
    start: Math.max(0, numberValue(row.querySelector('.interval-start'))),
    end: Math.max(0, numberValue(row.querySelector('.interval-end'))),
    productivity: clamp(numberValue(row.querySelector('.interval-productivity'))),
  }));
}

function getResilienceRows() {
  return [...els.resilienceTableBody.querySelectorAll('tr')].map((row) => ({
    row,
    name: row.querySelector('.resilience-name').value.trim(),
    score: clamp(numberValue(row.querySelector('.resilience-score'))),
    weight: clamp(numberValue(row.querySelector('.resilience-weight'))),
  }));
}

function getStrategyRows() {
  return [...els.strategyTableBody.querySelectorAll('tr')].map((row, index) => ({
    index,
    row,
    name: row.querySelector('.strategy-name').value.trim() || `Strategy ${index + 1}`,
```

```
    enabled: row.querySelector('.strategy-enabled').checked,
    cost: Math.max(0, numberValue(row.querySelector('.strategy-cost'))),
    risk: clamp(numberValue(row.querySelector('.strategy-risk'))),
    reliability: clamp(numberValue(row.querySelector('.strategy-reliability'))),
    resilience: clamp(numberValue(row.querySelector('.strategy-resilience'))),
  }));
}

function classifyPsi(psi) {
  return thresholds.find((item) => psi > item.minExclusive && psi <= item.maxInclusive) ||
thresholds[2];
}

function solveStrategySelection(strategies, budget, baseState, weights) {
  // The article presents a constrained maximization problem. For a client-side browser
app,
  // we implement an exhaustive subset search, which is exact for the small strategy
tables
  // that such decision-support screens usually contain.
  const n = strategies.length;
  let best = {
    names: [],
    cost: 0,
    psiAfter: baseState.psi,
    weightedObjective: baseState.psi,
  };

  for (let mask = 0; mask < 2 ** n; mask += 1) {
    let totalCost = 0;
    let deltaRisk = 0;
    let deltaReliability = 0;
    let deltaResilience = 0;
    const names = [];

    for (let i = 0; i < n; i += 1) {
      if (mask & (1 << i)) {
        const item = strategies[i];
        totalCost += item.cost;
```

```
        deltaRisk += item.risk;
        deltaReliability += item.reliability;
        deltaResilience += item.resilience;
        names.push(item.name);
      }
    }

    if (totalCost > budget) continue;

    const psiAfter =
      weights.alpha * clamp(baseState.riskContribution + deltaRisk) +
      weights.beta * clamp(baseState.reliability + deltaReliability) +
      weights.gamma * clamp(baseState.resilience + deltaResilience);

    const weightedObjective = psiAfter;

    if (
      weightedObjective > best.weightedObjective ||
      (weightedObjective === best.weightedObjective && totalCost < best.cost)
    ) {
      best = { names, cost: totalCost, psiAfter, weightedObjective };
    }
  }

  return best;
}

function recalculate() {
  const alpha = numberValue(els.alpha);
  const beta = numberValue(els.beta);
  const gamma = numberValue(els.gamma);
  const weightSum = alpha + beta + gamma;
  els.weightSum.textContent = formatNumber(weightSum, 2);
  els.weightSum.style.color = Math.abs(weightSum - 1) < 0.001 ? 'var(--success)' : 'var(-
-danger)';

  const riskRows = getRiskRows();
  let rawRisk = 0;
```

```
  riskRows.forEach((item) => {
    const contribution = item.p * item.v * (item.c1 * item.w1 + item.c2 * item.w2);
    rawRisk += contribution;
    item.row.querySelector('.row-output').textContent = formatNumber(contribution, 3);
  });
  const normalizedRisk = clamp(rawRisk / Math.max(numberValue(els.riskCeiling, 1),
0.0001));

  // Implementation note:
  // Equation (10) in the article adds a normalized risk term positively into PSI.
  // For a protection-level app, a lower raw risk should improve protection.
  // Therefore the default mode converts expected loss into a protective score: 1 -
normalizedRisk.
  const riskContribution =
    els.riskMode.value === 'direct' ? normalizedRisk : clamp(1 - normalizedRisk);

  els.rawRiskValue.textContent = formatNumber(rawRisk, 3);
  els.normalizedRiskValue.textContent = formatNumber(normalizedRisk, 3);
  els.riskContributionValue.textContent = formatNumber(riskContribution, 3);

  const failures = Math.max(0, numberValue(els.failures));
  const observationTime = Math.max(numberValue(els.observationTime, 1), 0.0001);
  const targetTime = Math.max(numberValue(els.targetTime, 1), 0.0001);
  const lambda = failures / observationTime;
  const baseReliability = Math.exp(-lambda * targetTime);
  const blackStart = clamp(numberValue(els.blackStart));
  const islandReliability = clamp(numberValue(els.islandReliability));
  const extendedReliability = clamp(baseReliability + (1 - baseReliability) * blackStart *
islandReliability);
  const reliabilityUsed = els.useExtendedReliability.value === 'yes' ? extendedReliability
: baseReliability;

  els.lambdaValue.textContent = formatNumber(lambda, 6);
  els.baseReliabilityValue.textContent = formatNumber(baseReliability, 3);
  els.usedReliabilityValue.textContent = formatNumber(reliabilityUsed, 3);

  const nominalPerformance = Math.max(numberValue(els.nominalPerformance, 1),
0.0001);
```

```
  const evaluationPeriod = Math.max(numberValue(els.evaluationPeriod, 1), 0.0001);

  // Calculate element resilience from time-performance intervals
  // RI_i = (1/T) * Σ(productivity * duration) for each interval
  const intervals = getResilientIntervalRows();
  let integralSum = 0;
  intervals.forEach((item) => {
    const duration = Math.max(0, item.end - item.start);
    const contribution = item.productivity * duration;
    integralSum += contribution;
    const outputs = item.row.querySelectorAll('.row-output');
    if (outputs.length >= 2) {
      outputs[0].textContent = formatNumber(duration, 1);
      outputs[1].textContent = formatNumber(contribution, 3);
    }
  });

  const elementResilience = clamp(integralSum / evaluationPeriod);

  const resilienceRows = getResilienceRows();
  let systemResilience = 0;
  resilienceRows.forEach((item) => {
    const contribution = item.score * item.weight;
    systemResilience += contribution;
    item.row.querySelector('.row-output').textContent = formatNumber(contribution, 3);
  });
  systemResilience = clamp(systemResilience || elementResilience);

  els.elementResilienceValue.textContent = formatNumber(elementResilience, 3);
  els.systemResilienceValue.textContent = formatNumber(systemResilience, 3);

  // Select which resilience value to use based on mode
  const resilienceUsed = els.resilienceMode.value === 'element' ? elementResilience :
systemResilience;

  const psi = alpha * riskContribution + beta * reliabilityUsed + gamma * resilienceUsed;
  const classification = classifyPsi(psi);
```

```
  els.psiValue.textContent = formatNumber(psi, 3);
  els.psiValue.className = classification.className;
  els.psiLabel.textContent = classification.label;
  els.psiLabel.className = classification.className;

  // Populate Base PSI Assessment section (Section 5)
  els.currentPsiValue.textContent = formatNumber(psi, 3);
  els.currentStatusLabel.textContent = classification.label;
  els.currentBandDescription.textContent = classification.description;
  els.currentResultBand.className = `result-band assessment-result-band
${classification.className}`;

  const strategies = getStrategyRows();
  const enabledStrategies = strategies.filter((s) => s.enabled);
  const selected = solveStrategySelection(
    enabledStrategies,
    Math.max(0, numberValue(els.budget)),
    {
      psi,
      riskContribution,
      reliability: reliabilityUsed,
      resilience: resilienceUsed,
    },
    { alpha, beta, gamma }
  );

  const effect = psi > 0 ? ((selected.psiAfter - psi) / psi) * 100 : 0;
  els.projectedPsiValue.textContent = formatNumber(selected.psiAfter, 3);
  els.selectedCostValue.textContent = formatNumber(selected.cost, 2);
  els.selectedStrategiesValue.textContent = selected.names.length ?
selected.names.join(', ') : 'None';
  els.psiEffect.textContent = formatPercent(effect, 1);

  // Populate Comparison & Final Assessment section (Section 7)
  els.beforePsiValue.textContent = formatNumber(psi, 3);
  els.afterPsiValue.textContent = formatNumber(selected.psiAfter, 3);
  els.improvementEffectValue.textContent = formatPercent(effect, 1);
```

```
  const finalClassification = classifyPsi(selected.psiAfter);
  els.finalBandLabel.textContent = finalClassification.label;
  els.finalBandDescription.textContent = finalClassification.description;
  els.finalResultBand.className = `result-band ${finalClassification.className}`;

  // Update hero metrics with final values
  els.finalPsiValue.textContent = formatNumber(selected.psiAfter, 3);
  els.finalPsiValue.className = finalClassification.className;
  els.finalPsiLabel.textContent = finalClassification.label;
  els.finalPsiLabel.className = finalClassification.className;
}

function exportState() {
  const state = {
    systemName: els.systemName.value,
    assessmentNote: els.assessmentNote.value,
    alpha: numberValue(els.alpha),
    beta: numberValue(els.beta),
    gamma: numberValue(els.gamma),
    riskCeiling: numberValue(els.riskCeiling),
    riskMode: els.riskMode.value,
    failures: numberValue(els.failures),
    observationTime: numberValue(els.observationTime),
    targetTime: numberValue(els.targetTime),
    blackStart: numberValue(els.blackStart),
    islandReliability: numberValue(els.islandReliability),
    useExtendedReliability: els.useExtendedReliability.value,
    nominalPerformance: numberValue(els.nominalPerformance),
    evaluationPeriod: numberValue(els.evaluationPeriod),
    resilienceMode: els.resilienceMode.value,
    budget: numberValue(els.budget),
    objectWeight: numberValue(els.objectWeight, 1),
    riskRows: getRiskRows().map(({ name, p, v, c1, c2, w1, w2 }) => ({ name, p, v, c1,
c2, w1, w2 })),
    resilienceIntervals: getResilientIntervalRows().map(({ start, end, productivity }) => ({
start, end, productivity })),
    resilienceRows: getResilienceRows().map(({ name, score, weight }) => ({ name,
score, weight })),
```

```
    strategyRows: getStrategyRows().map(({ name, enabled, cost, risk, reliability,
resilience }) => ({
      name,
      enabled,
      cost,
      risk,
      reliability,
      resilience,
    })),
  };

  const blob = new Blob([JSON.stringify(state, null, 2)], { type: 'application/json' });
  const url = URL.createObjectURL(blob);
  const link = document.createElement('a');
  link.href = url;
  link.download = 'cis-protection-assessment.json';
  link.click();
  URL.revokeObjectURL(url);
}

function applyAssessmentData(data) {
  const normalizedData = {
    systemName: '',
    assessmentNote: '',
    alpha: '',
    beta: '',
    gamma: '',
    riskCeiling: '',
    riskMode: 'protective',
    failures: '',
    observationTime: '',
    targetTime: '',
    blackStart: '',
    islandReliability: '',
    useExtendedReliability: 'yes',
    nominalPerformance: '',
    evaluationPeriod: '',
    resilienceMode: 'system',
```

```
    budget: '',
    ...data,
    riskRows: Array.isArray(data?.riskRows) ? data.riskRows : [],
    resilienceIntervals: Array.isArray(data?.resilienceIntervals) ? data.resilienceIntervals :
[],
    resilienceRows: Array.isArray(data?.resilienceRows) ? data.resilienceRows : [],
    strategyRows: Array.isArray(data?.strategyRows) ? data.strategyRows : [],
  };

  Object.entries(normalizedData).forEach(([key, value]) => {
    if (els[key] && !Array.isArray(value)) {
      els[key].value = value;
    }
  });

  els.riskTableBody.innerHTML = '';
  normalizedData.riskRows.forEach((item) => createRow('risk', item));

  els.resilienceIntervalTableBody.innerHTML = '';
  normalizedData.resilienceIntervals.forEach((item) => createRow('resilienceInterval',
item));

  els.resilienceTableBody.innerHTML = '';
  normalizedData.resilienceRows.forEach((item) => createRow('resilience', item));

  els.strategyTableBody.innerHTML = '';
  normalizedData.strategyRows.forEach((item) => createRow('strategy', item));

  recalculate();
}

function importAssessmentData(file) {
  if (!file) {
    return;
  }

  const reader = new FileReader();
```

```
  reader.onload = () => {
    try {
      const parsed = JSON.parse(reader.result);
      applyAssessmentData(parsed);
    } catch (error) {
      console.error('Failed to import assessment JSON:', error);
      alert('Could not import the file. Please choose a valid JSON export from this app.');
    } finally {
      els.importJsonInput.value = '';
    }
  };

  reader.onerror = () => {
    alert('Could not read the selected file. Please try again.');
    els.importJsonInput.value = '';
  };

  reader.readAsText(file);
}

function clearData() {
  // Clear all input fields
  els.systemName.value = '';
  els.assessmentNote.value = '';
  els.alpha.value = '';
  els.beta.value = '';
  els.gamma.value = '';
  els.riskCeiling.value = '';
  els.riskMode.value = 'protective';
  els.failures.value = '';
  els.observationTime.value = '';
  els.targetTime.value = '';
  els.blackStart.value = '';
  els.islandReliability.value = '';
  els.useExtendedReliability.value = 'yes';
  els.nominalPerformance.value = '';
  els.evaluationPeriod.value = '';
  els.budget.value = '';
```

```
  els.resilienceMode.value = 'system';

  // Clear all tables
  els.riskTableBody.innerHTML = '';
  els.resilienceIntervalTableBody.innerHTML = '';
  els.resilienceTableBody.innerHTML = '';
  els.strategyTableBody.innerHTML = '';

  recalculate();
}

[
  els.systemName,
  els.assessmentNote,
  els.alpha,
  els.beta,
  els.gamma,
  els.riskCeiling,
  els.riskMode,
  els.failures,
  els.observationTime,
  els.targetTime,
  els.blackStart,
  els.islandReliability,
  els.useExtendedReliability,
  els.nominalPerformance,
  els.evaluationPeriod,
  els.budget,
  // els.objectWeight, // Removed from equations - not impacting optimization
].forEach((element) => element.addEventListener('input', recalculate));

els.resilienceMode.addEventListener('change', recalculate);

els.loadSampleBtn.addEventListener('click', () => applyAssessmentData(demoData));
els.loadCustomDataBtn.addEventListener('click', () => els.importJsonInput.click());
els.clearDataBtn.addEventListener('click', clearData);
els.downloadJsonBtn.addEventListener('click', exportState);
els.importJsonInput.addEventListener('change', (event) => {
```

```
  importAssessmentData(event.target.files?.[0]);
});
els.enableAllStrategiesBtn.addEventListener('click', () => {
  els.strategyTableBody.querySelectorAll('.strategy-enabled').forEach((checkbox) => {
    checkbox.checked = true;
  });
  recalculate();
});
els.disableAllStrategiesBtn.addEventListener('click', () => {
  els.strategyTableBody.querySelectorAll('.strategy-enabled').forEach((checkbox) => {
    checkbox.checked = false;
  });
  recalculate();
});
els.addRiskRowBtn.addEventListener('click', () => {
  createRow('risk');
  recalculate();
});
els.addResilienceIntervalBtn.addEventListener('click', () => {
  createRow('resilienceInterval');
  recalculate();
});
els.addResilienceRowBtn.addEventListener('click', () => {
  createRow('resilience');
  recalculate();
});
els.addStrategyRowBtn.addEventListener('click', () => {
  createRow('strategy');
  recalculate();
});

// Listen for strategy checkbox changes to trigger recalculation
els.strategyTableBody.addEventListener('change', (e) => {
  if (e.target.classList.contains('strategy-enabled')) {
    recalculate();
  }
});
```

```
// Toggle collapsible sections
document.querySelectorAll('.toggle-section').forEach((btn) => {
  btn.addEventListener('click', () => {
    const targetId = btn.getAttribute('data-target');
    const targetElement = document.getElementById(targetId);
    if (targetElement) {
      const isHidden = targetElement.style.display === 'none';
      targetElement.style.display = isHidden ? 'block' : 'none';
      btn.setAttribute('aria-expanded', isHidden ? 'true' : 'false');
    }
  });
});

// Populate the interface with the bundled sample dataset on first load.
applyAssessmentData(demoData);
```

Index.html

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>R3 CRISYS Protection Analyzer</title>
  <link rel="stylesheet" href="styles.css" />
</head>
<body>
  <header class="hero">
    <div>
      <p class="eyebrow">Risk · Reliability · Resilience</p>
      <h1>R3 CRISYS Protection Analyzer</h1>
      <p class="subtitle">
        A browser-based implementation of the article's method for assessment and
enhancement of the protection level
        of a critical IT system.
      </p>
    </div>
```

```
    <div class="hero-metrics card" style="display: grid; grid-template-columns: 1fr 1fr;
gap: 2rem;">
      <div style="display: flex; flex-direction: column; gap: 1.5rem;">
        <div>
          <span class="metric-label">Base Integral Index</span>
          <strong id="psiValue">0.000</strong>
        </div>
        <div>
          <span class="metric-label">Protection Status</span>
          <strong id="psiLabel">Not ensured</strong>
        </div>
      </div>
      <div style="display: flex; flex-direction: column; gap: 1.5rem;">
        <div>
          <span class="metric-label">Final Integral Index</span>
          <strong id="finalPsiValue">0.000</strong>
        </div>
        <div>
          <span class="metric-label">Final Protection Status</span>
          <strong id="finalPsiLabel">Not ensured</strong>
        </div>
        <div>
          <span class="metric-label">Improvement Effect</span>
          <strong id="psiEffect">0.0%</strong>
        </div>
      </div>
    </div>
  </header>

  <main class="layout">
    <section class="card section">
      <div class="section-head">
        <div>
          <h2>Base configuration</h2>
          <p>Set the system name, weights for the 3R Method, and the normalization
policy used by the app.</p>
        </div>
        <div style="display: flex; gap: 8px;">
```

```
        <button id="loadSampleBtn" class="ghost-btn">Load demo data</button>
        <button id="loadCustomDataBtn" class="ghost-btn">Load custom data</button>
        <button id="clearDataBtn" class="ghost-btn">Clear data</button>
        <input id="importJsonInput" type="file" accept=".json,application/json" hidden />
      </div>
    </div>
    <div class="grid-2">
      <label>
        <span>System name</span>
        <input id="systemName" type="text" value="National Energy Dispatch Platform"
/>
      </label>
      <label>
        <span>Assessment horizon / note</span>
        <input id="assessmentNote" type="text" value="Quarterly protection review" />
      </label>
    </div>

    <div class="weights-grid">
      <label>
        <span>α — risk weight</span>
        <input id="alpha" type="number" min="0" max="1" step="0.01" value="0.34" />
      </label>
      <label>
        <span>β — reliability weight</span>
        <input id="beta" type="number" min="0" max="1" step="0.01" value="0.33" />
      </label>
      <label>
        <span>γ — resilience weight</span>
        <input id="gamma" type="number" min="0" max="1" step="0.01" value="0.33" />
      </label>
      <div class="badge-box">
        <span class="muted">Weight sum</span>
        <strong id="weightSum">1.00</strong>
      </div>
    </div>

    <div class="grid-2 top-gap">
```

```
        <label>
          <span>Risk normalization ceiling</span>
          <input id="riskCeiling" type="number" min="0.01" step="0.01" value="1" />
          <small>Used to normalize the article's raw expected-loss risk score into the 0..1
range.</small>
        </label>
        <label>
          <span>Risk contribution mode</span>
          <select id="riskMode">
            <option value="protective" selected>Protective score = 1 - normalized
risk</option>
            <option value="direct">Direct normalized risk</option>
          </select>
          <small>
            The protective mode is practical for protection-level assessment because lower
risk should improve PSI.
          </small>
        </label>
      </div>
    </section>

    <section class="card section">
      <div class="section-head">
        <div>
          <h2>Risk assessment</h2>
          <p>
            Based on equation (4): expected loss is aggregated from scenario probability,
vulnerability,
            consequence, and consequence weight.
          </p>
        </div>
        <div style="display: flex; gap: 8px;">
          <button id="addRiskRowBtn" class="ghost-btn">Add scenario</button>
          <button class="toggle-section ghost-btn" data-target="risk-details" title="Toggle
details">▼</button>
        </div>
      </div>
      <div class="summary-grid">
```

```
    <div class="summary-box">
      <span>Raw risk score</span>
      <strong id="rawRiskValue">0.000</strong>
    </div>
    <div class="summary-box">
      <span>Normalized risk</span>
      <strong id="normalizedRiskValue">0.000</strong>
    </div>
    <div class="summary-box">
      <span>Risk contribution to PSI</span>
      <strong id="riskContributionValue">0.000</strong>
    </div>
  </div>
  <div id="risk-details" class="section-details" style="display: none;">
    <div class="table-wrap">
      <table class="risk-table">
        <thead>
          <tr>
            <th>Threat / scenario</th>
            <th>P</th>
            <th>V</th>
            <th>C₁</th>
            <th>w₁</th>
            <th>C₂</th>
            <th>w₂</th>
            <th>Contribution</th>
            <th></th>
          </tr>
        </thead>
        <tbody id="riskTableBody"></tbody>
      </table>
    </div>
  </div>
</section>

<section class="card section">
  <div class="section-head">
    <div>
```

```
        <h2>Reliability assessment</h2>
        <p>
          Based on equations (5)–(7): exponential reliability with optional autonomous recovery extension.
        </p>
      </div>
      <button class="toggle-section ghost-btn" data-target="reliability-details" title="Toggle details">▼</button>
    </div>
    <div class="summary-grid">
      <div class="summary-box">
        <span>Failure intensity λ</span>
        <strong id="lambdaValue">0.000300</strong>
      </div>
      <div class="summary-box">
        <span>Base reliability R(t)</span>
        <strong id="baseReliabilityValue">0.806</strong>
      </div>
      <div class="summary-box">
        <span>Reliability used in PSI</span>
        <strong id="usedReliabilityValue">0.917</strong>
      </div>
    </div>
    <div id="reliability-details" class="section-details" style="display: none;">
      <div class="grid-3">
        <label>
          <span>Observed failures Nfail</span>
          <input id="failures" type="number" min="0" step="1" value="3" />
        </label>
        <label>
          <span>Observation time Tobs</span>
          <input id="observationTime" type="number" min="0.01" step="0.01" value="10000" />
        </label>
        <label>
          <span>Target operating time t</span>
          <input id="targetTime" type="number" min="0.01" step="0.01" value="720" />
        </label>
```

```
      </div>
      <div class="grid-3 top-gap">
       <label>
        <span>Autonomous restart probability Bs</span>
        <input id="blackStart" type="number" min="0" max="1" step="0.01" value="0.70"
/>
       </label>
       <label>
        <span>Island / isolated mode reliability</span>
        <input id="islandReliability" type="number" min="0" max="1" step="0.01"
value="0.82" />
       </label>
       <label>
        <span>Use extended reliability</span>
        <select id="useExtendedReliability">
         <option value="yes" selected>Yes</option>
         <option value="no">No</option>
        </select>
       </label>
      </div>
     </div>
    </section>

    <section class="card section">
     <div class="section-head">
      <div>
       <h2>Resilience assessment</h2>
       <p>
        Based on equations (8)–(9): a time-performance resilience index plus a
weighted multi-level system index.
       </p>
      </div>
      <button class="toggle-section ghost-btn" data-target="resilience-details"
title="Toggle details">▼</button>
     </div>
     </div>
     <div class="summary-grid top-gap-small">
      <div class="summary-box">
```

```
        <span>Time-Performance Element resilience RIi</span>
        <strong id="elementResilienceValue">0.880</strong>
      </div>
      <div class="summary-box">
        <span>System resilience RI_sys</span>
        <strong id="systemResilienceValue">0.876</strong>
      </div>
      <div style="display: flex; align-items: center; gap: 0.5rem;">
        <label style="margin: 0;">
          <span style="color: var(--muted); font-size: 0.9rem;">Use for PSI</span>
          <select id="resilienceMode" style="margin-top: 0.4rem;">
            <option value="system" selected>System resilience</option>
            <option value="element">Element resilience</option>
          </select>
        </label>
      </div>
    </div>

    <div id="resilience-details" class="section-details" style="display: none;">
      <div class="grid-3" style="margin-bottom: 2rem;">
        <label>
          <span>Evaluation period T (hours)</span>
          <input id="evaluationPeriod" type="number" min="0.01" step="0.01" value="12"
/>
        </label>
        <label>
          <span>Nominal performance Pnom</span>
          <input id="nominalPerformance" type="number" min="0.01" step="0.01"
value="100" />
        </label>
      </div>

      <div style="margin-bottom: 2rem;">
        <h4 style="margin-top: 0; color: var(--muted);">Time-Performance Resilience
(Element Resilience)</h4>
        <p style="font-size: 0.9rem; color: var(--muted); margin-bottom: 1rem;">
          Define system productivity levels across different time intervals after a disruptive
event.
```

```
        </p>
        <div class="table-wrap">
          <table>
            <thead>
              <tr>
                <th>Start time (h)</th>
                <th>End time (h)</th>
                <th>P(t) / P_nom</th>
                <th>Duration (h)</th>
                <th>Contribution</th>
                <th></th>
              </tr>
            </thead>
            <tbody id="resilienceIntervalTableBody"></tbody>
          </table>
        </div>
        <div style="margin-top: 1.5rem;">
          <button id="addResilienceIntervalBtn" class="ghost-btn">Add interval</button>
        </div>
      </div>

      <div>
        <h4 style="margin-top: 0; color: var(--muted);">Multi-Level System
Resilience</h4>
        <p style="font-size: 0.9rem; color: var(--muted); margin-bottom: 1rem;">
          Define resilience and weighted contribution for each organizational or system
level.
        </p>
        <div class="table-wrap">
          <table class="resilience-level-table">
            <thead>
              <tr>
                <th>Level</th>
                <th>RI(l)</th>
                <th>β(l)</th>
                <th>Weighted</th>
                <th></th>
              </tr>
```

```
            </thead>
            <tbody id="resilienceTableBody"></tbody>
          </table>
        </div>
        <div style="margin-top: 1.5rem;">
          <button id="addResilienceRowBtn" class="ghost-btn">Add level</button>
        </div>
      </div>
    </div>
  </section>

  <section class="card section">
    <div class="section-head">
      <div>
        <h2>Base Integral Protection Index assessment</h2>
        <p>Current integral protection index value and corresponding protection status
before applying any improvement strategies.</p>
      </div>
    </div>
    <div class="assessment-summary-grid">
      <div class="summary-box assessment-summary-box">
        <span>Base Integral Index (PSI)</span>
        <strong id="currentPsiValue">0.000</strong>
      </div>
      <div class="result-band assessment-result-band" id="currentResultBand">
        <div>
          <span>Protection status</span>
          <h3 id="currentStatusLabel">Not ensured</h3>
        </div>
        <p id="currentBandDescription"></p>
      </div>
    </div>
  </section>

  <section class="card section">
    <div class="section-head">
      <div>
        <h2>Strategy optimization</h2>
```

```
        <p>
          Optional decision-support block inspired by equations (11)–(12): choose measures under a budget and compare PSI before and after.
        </p>
      </div>
      <button class="toggle-section ghost-btn" data-target="strategy-details" title="Toggle details">▼</button>
    </div>
    <div class="summary-grid top-gap-small">
      <div class="summary-box">
        <span>Selected package cost</span>
        <strong id="selectedCostValue">0.00</strong>
      </div>
      <div class="summary-box">
        <span>Projected PSI after strategies</span>
        <strong id="projectedPsiValue">0.000</strong>
      </div>
      <div class="summary-box">
        <span>Selected strategies</span>
        <strong id="selectedStrategiesValue">—</strong>
      </div>
    </div>
    <div id="strategy-details" class="section-details" style="display: none;">
      <div style="display: grid; grid-template-columns: 1fr auto; gap: 1rem; align-items: end;">
        <label>
          <span>Available budget B</span>
          <input id="budget" type="number" min="0" step="5" value="250" />
        </label>
        <div style="display: flex; gap: 8px;">
          <button id="enableAllStrategiesBtn" class="ghost-btn">Enable all</button>
          <button id="disableAllStrategiesBtn" class="ghost-btn">Disable all</button>
        </div>
      </div>
      <!-- Object importance weight wᵢ field removed - not impacting equations -->
      <div class="table-wrap top-gap">
        <table>
          <thead>
```

```
            <tr>
              <th style="width: 40px; text-align: center;">Enabled</th>
              <th>Strategy</th>
              <th>Cost</th>
              <th>Δ Risk</th>
              <th>Δ Reliability</th>
              <th>Δ Resilience</th>
              <th></th>
            </tr>
          </thead>
          <tbody id="strategyTableBody"></tbody>
        </table>
      </div>
      <div style="display: flex; gap: 8px; margin-top: 1rem;">
        <button id="addStrategyRowBtn" class="ghost-btn">Add strategy</button>
      </div>
    </div>
  </section>

  <section class="card section results-section">
    <div class="section-head">
      <div>
        <h2>Comparison & final assessment</h2>
        <p>Compare the protection level before and after applying selected improvement
strategies.</p>
      </div>
      <button id="downloadJsonBtn" class="primary-btn">Export JSON</button>
    </div>
    <div class="summary-grid top-gap-small">
      <div class="summary-box">
        <span>PSI before strategies</span>
        <strong id="beforePsiValue">0.000</strong>
      </div>
      <div class="summary-box">
        <span>PSI after strategies</span>
        <strong id="afterPsiValue">0.000</strong>
      </div>
      <div class="summary-box">
```

```
        <span>Improvement effect</span>
        <strong id="improvementEffectValue">0.0%</strong>
       </div>
      </div>
      <div class="result-band" id="finalResultBand">
       <div>
        <span class="muted">Final status</span>
        <h3 id="finalBandLabel">Not ensured</h3>
       </div>
       <p id="finalBandDescription">
        The protection level is insufficient; the system has significant vulnerabilities and
requires additional resilience measures.
       </p>
      </div>
      <div class="section-head" style="margin-top: 1.5rem;">
       <h3>Implemented equations</h3>
       <button class="toggle-section ghost-btn" data-target="equations-details"
title="Toggle equations">▼</button>
      </div>
      <div id="equations-details" class="section-details" style="display: none;">
       <div class="formula-panel">
        <ul>
         <li><code>Risk_raw = Σ(w × P × V × C)</code></li>
         <li><code>λ = Nfail / Tobs</code></li>
         <li><code>R(t) = e^(−λt)</code></li>
         <li><code>R* = R + (1 − R) × Bs × R_island</code></li>
         <li><code>RIᵢ = (1 / T) × ∫[0..T] P(t)/Pnom dt</code><!-- → discrete
implementation uses average performance ratio--></li>
         <li><code>RI_sys = Σ(β(I) × RI(I))</code></li>
         <li><code>PSI = α × Risk_component + β × Reliability + γ ×
Resilience</code></li>
         <li><code>Effect = ((PSI_after − PSI_before) / PSI_before) × 100%</code></li>
        </ul>
       </div>
      </div>
     </section>
    </main>
```

```
 <footer class="footer">
  <p>
   Source: EXPERIMENTAL STUDY OF A METHOD FOR ENHANCING THE
PROTECTION OF CRITICAL GOVERNMENT INFORMATION SYSTEMS (article by
V.Sydorenko and S.Sydorenko).
   The app includes a documented engineering interpretation for risk normalization.
The integral indicator can be used as a protection score.
  </p>
 </footer>

 <template id="riskRowTemplate">
  <tr>
   <td><input type="text" class="risk-name" value="Scenario" /></td>
   <td><input type="number" class="risk-p" min="0" max="1" step="0.01" value="0.25"
/></td>
   <td><input type="number" class="risk-v" min="0" max="1" step="0.01" value="0.30"
/></td>
   <td><input type="number" class="risk-c1" min="0" max="1" step="0.01"
value="0.60" /></td>
   <td><input type="number" class="risk-w1" min="0" max="1" step="0.01"
value="0.50" /></td>
   <td><input type="number" class="risk-c2" min="0" max="1" step="0.01"
value="0.60" /></td>
   <td><input type="number" class="risk-w2" min="0" max="1" step="0.01"
value="0.50" /></td>
   <td class="row-output">0.023</td>
   <td><button class="icon-btn remove-row-btn" title="Remove row">×</button></td>
  </tr>
 </template>

 <template id="resilienceIntervalTemplate">
  <tr>
   <td><input type="number" class="interval-start" min="0" step="0.1" value="0"
/></td>
   <td><input type="number" class="interval-end" min="0" step="0.1" value="2" /></td>
   <td><input type="number" class="interval-productivity" min="0" max="1" step="0.01"
value="0.40" /></td>
   <td class="row-output">2.0</td>
```

```
      <td class="row-output">0.800</td>
      <td><button class="icon-btn remove-row-btn" title="Remove row">×</button></td>
    </tr>
  </template>

  <template id="resilienceRowTemplate">
    <tr>
      <td><input type="text" class="resilience-name" value="IT infrastructure" /></td>
      <td><input type="number" class="resilience-score" min="0" max="1" step="0.01"
value="0.88" /></td>
      <td><input type="number" class="resilience-weight" min="0" max="1" step="0.01"
value="0.34" /></td>
      <td class="row-output">0.299</td>
      <td><button class="icon-btn remove-row-btn" title="Remove row">×</button></td>
    </tr>
  </template>

  <template id="strategyRowTemplate">
    <tr>
      <td style="text-align: center;"><input type="checkbox" class="strategy-enabled"
checked /></td>
      <td><textarea class="strategy-name">Strategy</textarea></td>
      <td><input type="number" class="strategy-cost" min="0" step="0.01" value="50"
/></td>
      <td><input type="number" class="strategy-risk" min="0" max="1" step="0.01"
value="0.05" /></td>
      <td><input type="number" class="strategy-reliability" min="0" max="1" step="0.01"
value="0.03" /></td>
      <td><input type="number" class="strategy-resilience" min="0" max="1" step="0.01"
value="0.04" /></td>
      <td><button class="icon-btn remove-row-btn" title="Remove row">×</button></td>
    </tr>
  </template>

  <script src="app.js"></script>
</body>
</html>
```

Додаток В

Список публікацій здобувача

Статті у наукових фахових виданнях України:

1. Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Смірнова Т.В., Сидоренко С.Ю. Модель визначення критичності галузевих інформаційно-телекомунікаційних систем. *Проблеми інформатизації та управління.* 2022. Т. 2. № 70. С. 28-37. DOI: https://doi.org/10.18372/2073-4751.70.16844

2. Гнатюк С.О., Сидоренко В.М., Березовий І.Р., Сидоренко С.Ю., Тараненко К.О. Модель оцінювання ефективності функціонування систем інформаційної безпеки взаємозалежних критичних інфраструктур. *Проблеми інформатизації та управління.* 2022. Т. 4.№ 72. С. 17-25. DOI: https://doi.org/10.18372/2073-4751.72.17457

3. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об’єктах критичної інформаційної інфраструктури держави. *Проблеми інформатизації та управління*. 2024. Т. 2. №78. С. 104-114. DOI: https://doi.org/10.18372/2073-4751.78.18967

4. Сидоренко В.М., Сидоренко С.Ю. Метод підвищення рівня захищеності критичних інформаційних систем держави. *Кібербезпека: освіта, наука, техніка.* 2025. Т.2. №30. С. 500-510. DOI: https://doi.org/10.28925/2663-4023.2025.30.988

Статті в іноземних виданнях:

5. Gnatyuk S., Sydorenko V., Polozhentsev A., Sydorenko S. Experimental Study of the Method for Cyber Incidents Management in Aviation

Critical Infrastructure. In: Ostroumov, I., Marais, K., Zaliskyi, M. (eds) Advances in Civil Aviation Systems Development. ACASD 2025. *Lecture Notes in Networks and Systems*, Vol. 1418. P. 74–91, Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-91992-3_6. (*Scopus*) Q4, ISSN 2367-3370.

6. Lutskyi M., Sydorenko V., Polozhentsev A., Apenko N., Sydorenko S. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures. *CEUR Workshop Proceedings.* 2023. Vol. 3421. P. 214-222. URL: https://ceur-ws.org/Vol-3421/short7.pdf (*Scopus*) Q4, ISSN 1613-0073.

Публікації, які додатково відображають наукові результати дисертації:

7. Жигаревич О.К., Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю. Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи». *Кіберзахист особи, суспільства і держави*: наук.-практ. конф., с. Велятино, 24-27 січня 2024 р.: тези доп., Київ: НАУ, 2024. С. 14-15.