КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.988
УДК 004.056.53:351.853

Сидоренко Вікторія Миколаївна
к.т.н., доц., доцент кафедри комп'ютерних інформаційних технологій
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Сидоренко Сергій Юрійович
аспірант факультету комп'ютерних наук та технологій
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0002-7170-123X
serh.sydorenko@gmail.com

МЕТОД ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ДЕРЖАВИ

Анотація. У сучасних умовах зростання кількості кіберзагроз і ускладнення технологічних систем забезпечення захищеності критичних інформаційних систем (КІС) є одним із ключових завдань національної безпеки держави. Існуючі підходи до оцінювання стану безпеки КІС переважно орієнтовані на окремі технічні або організаційні аспекти, що не забезпечує комплексного урахування взаємозв'язків між ризиком, надійністю та стійкістю. У статті представлено метод підвищення рівня захищеності КІС, який передбачає формалізацію взаємозв'язків між цими параметрами у вигляді системи математичних виразів і введення інтегрального показника рівня захищеності. Запропонований підхід дозволяє кількісно оцінювати поточний стан безпеки КІС, прогнозувати вплив потенційних загроз і визначати оптимальні стратегії підвищення стійкості з урахуванням обмежених ресурсів. Розроблений метод забезпечує об'єктивне прийняття рішень щодо управління ризиками та підвищення ефективності захисту КІС, а також сприяє формуванню адаптивної національної системи кібербезпеки. Подальші дослідження передбачають експериментальну перевірку та верифікацію запропонованого методу на прикладах функціонування об'єктів критичної інфраструктури (ОКІ) різних галузей для оцінки його ефективності, універсальності та можливості практичного впровадження.

Ключові слова: критична інфраструктура, об'єкти критичної інфраструктури, критичні інформаційні системи, загрози, захищеність, рівень захищеності, стійкість, забезпечення стійкості, ефективність, ризик, надійність, управління ризиками, оптимізація стратегій.

ВСТУП

Забезпечення належного рівня захищеності ОКІ є стратегічним пріоритетом державної політики України, оскільки від стабільності їх функціонування залежать ефективність державного управління, економічна стійкість, енергетична безпека та обороноздатність країни. Особливу роль серед них відіграють КІС – це сукупність взаємопов'язаних інформаційних, комунікаційних і технологічних компонентів, від безперебійного функціонування яких залежить стабільність роботи ОКІ, а також безпека, економічна стійкість і життєдіяльність держави [1]. До складу КІС належать інформаційні ресурси, засоби обробки, передавання та зберігання даних, програмне забезпечення, комунікаційні мережі та елементи кіберфізичних систем, що забезпечують управління технологічними процесами у ключових секторах – енергетичному, транспортному, фінансовому, оборонному, медичному тощо. Сучасні загрози для КІС мають комплексний характер, поєднуючи кібернетичні, техногенні, фізичні та організаційні чинники. Уразливість таких систем може призвести до

порушення роботи ОКІ, збоїв у ланцюгах постачання, витоку конфіденційних даних та значних економічних втрат.

Нормативно-правове забезпечення сфери захисту критичної інфраструктури (КІ) в Україні базується на Законі України «Про критичну інфраструктуру» [2], який визначає принципи функціонування системи її безпеки та стійкості. Важливе значення мають також постанови Кабінету Міністрів України № 1109 «Деякі питання забезпечення безпеки та стійкості критичної інфраструктури» [3] і № 518 «Про затвердження критеріїв віднесення об'єктів до категорій критичності» [4], що регламентують підходи до класифікації, управління ризиками та взаємодії суб'єктів у сфері захисту КІ. Крім того, на практичному рівні для оцінювання стану захищеності ОКІ використовується Методика оцінки стану захищеності об'єктів критичної інфраструктури [5], затверджена наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 17 від 14.01.2025 р. Вона встановлює порядок визначення рівня захищеності ОКІ за низкою критеріїв і шкалою оцінювання, що дозволяє здійснювати базову діагностику безпеки КІ.

Однак чинні нормативні підходи здебільшого зосереджені на окремих складових безпеки без урахування їх взаємного впливу та динамічної взаємозалежності. Така фрагментарність ускладнює формування комплексного бачення рівня захищеності КІС, які потребують інтегрованих методів оцінювання та управління. В умовах зростання інтенсивності кібератак, гібридних загроз і міжгалузевих залежностей виникає потреба у нових методологічних підходах, які дозволяють комплексно оцінювати стан захищеності систем та підвищувати їх стійкість у динамічному середовищі ризику.

Актуальність дослідження зумовлена потребою у створенні інтегрованого підходу до оцінювання рівня захищеності КІС, який поєднає технічні, організаційні та аналітичні аспекти й може бути використаний для підтримки прийняття рішень на державному та галузевому рівнях.

Постановка проблеми. Попри наявність законодавчих та методичних засад у сфері захисту КІ, актуальним залишається питання комплексного оцінювання рівня захищеності КІС. Існуючі методики, зокрема [5], забезпечують лише базову діагностику стану безпеки, не враховуючи взаємозв'язків між ризиком, надійністю та стійкістю. Такий підхід не дозволяє повною мірою оцінити динамічний характер впливу загроз, взаємозалежність компонентів системи та ефективність застосованих заходів із підвищення захищеності.

Складність проблеми полягає у багатовимірності самої природи захищеності, що охоплює технічні, організаційні, аналітичні та людські чинники, які взаємодіють у мінливому середовищі загроз. Крім того, ризики для КІС мають нелінійний і динамічний характер, що ускладнює їх кількісну оцінку та прогнозування. Відсутність єдиного інтегрованого підходу до аналізу та управління такими ризиками призводить до фрагментарності оцінювання, коли різні аспекти безпеки розглядаються ізольовано. У цих умовах постає необхідність у створенні науково обґрунтованого методу, який дозволить інтегрувати взаємопов'язані параметри ризику, надійності та стійкості у єдину математично формалізовану методологію для підвищення рівня захищеності КІС держави.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Забезпечення належного рівня захищеності КІС є одним із ключових завдань держави, оскільки від їх стійкого функціонування залежить національна безпека, економічна стабільність та обороноздатність країни. Сучасні виклики, пов'язані з кіберзагрозами, фізичними та технологічними ризиками, зумовлюють необхідність застосування комплексних підходів до підвищення рівня захищеності таких систем. Водночас попередній

аналіз наукових джерел свідчить, що ефективним напрямом розвитку є інтеграція існуючих концепцій, які дозволяє поєднати різноманітні оцінки ризиків, надійності та стійкості в єдину методологічну основу. Для вирішення завдань пов'язаних з забезпеченням захищеності КІС проведемо аналіз сучасних публікацій, опишемо існуючі підходи до визначення захищеності та проведемо їх порівняльний аналіз.

У роботі [6] Мурасов Р. та Мельник Я. розглядається підхід до оцінювання захищеності кіберпростору ОКІ України, який базується на системному аналізі ризиків, уразливостей та потенційних наслідків реалізації кіберзагроз. Автори пропонують методику, що враховує особливості функціонування інформаційних систем об’єктів КІ та передбачає використання сучасних інструментів моніторингу та тестування безпеки.

У аналітичній доповіді [7] Суходоля 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 [8] Шевченко Н. І. та Плахотнюк 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 стійкість систем, та розробляють багатокритеріальну модель оцінки з інтегральним показником стійкості.

У дослідженні [9] Кириленко С. П. та Тищенко В. В. розглянуто формалізовані моделі оцінювання ризиків для ОКІ в умовах збройного конфлікту. Автори пропонують математичний апарат для кількісної оцінки ризику, що враховує ймовірність реалізації загрози, рівень уразливості та очікувані наслідки.

У роботі [10] Третьяков О. В. та ін. запропоновано підхід до кількісної оцінки 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.

У статті [11] Mahmood Y., Afrin T. та ін. обґрунтовано системний підхід до сталого розвитку інфраструктур на основі концепції 3R (Risk–Reliability–Resilience). Запропоновано фундаментальну та взаємопов’язану матрицю, що відображає взаємозв’язки між ризиками, надійністю та стійкістю систем, дозволяючи формалізувати їх у єдину модель оцінювання.

У публікації [12] Mohd Safari M.A., Masseran N. та ін. представлено робастний і ефективний метод оцінювання параметрів надійності технічних систем, що ґрунтується на експоненційному розподілі часу безвідмовної роботи. Запропонований підхід дозволяє мінімізувати вплив аномальних даних і підвищити точність визначення інтенсивності відмов.

У статті [13] Kong J., Zhang C. та ін. запропоновано підхід до оптимізації стійкості взаємопов’язаних інфраструктур шляхом поєднання технічних і організаційних заходів підвищення безпеки. Автори застосували багатокритеріальну оптимізацію для визначення найефективнішого набору рішень з урахуванням обмежень ресурсів, часу та рівня ризику, що в свою чергу, дозволяє оцінювати зміну рівня резильєнтності систем унаслідок впровадження певних стратегій.

У статті [14] 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 частиною її резильєнтності.

У роботі [15] 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 показник resilience. Автори наголошують на важливості врахування взаємозалежностей між різними типами загроз і адаптивних можливостей системи.

У Табл. 1, враховуючи попередні дослідження [1-16], систематизовано та представлено детальний аналіз підходів до оцінювання рівня захищеності КІС за такими 8 критеріями (запропоновані авторами):

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 інформаційних систем 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

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 порівняльний аналіз підходів до оцінювання рівня захищеності КІС показав, що найбільш повно вивченими критеріями є рівень ризику реалізації загроз (RR), надійність елементів системи (RF) та стійкість інформаційних потоків (RI). Ці аспекти є

центральними у більшості проаналізованих праць, зокрема зарубіжних, що ґрунтуються на принципах 3R. Водночас адаптивність систем (RA), ресурсна забезпеченість заходів захисту (RC) та оперативність реагування (RRs) залишаються менш розробленими, особливо в контексті українських досліджень, що свідчить про необхідність подальшої розробки інтегрованих моделей управління захищеністю. Отримані результати підтверджують доцільність розробки нового підходу для комплексного оцінювання та підвищення ефективності функціонування КІС в умовах обмежених ресурсів і високої динаміки загроз. Отже, **метою статті** є розробка методу підвищення рівня захищеності КІС держави.

ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ МЕТОДУ

Математичний опис методу підвищення рівня захищеності КІС, з урахуванням [11-15], реалізується за допомогою наступних етапів:

Етап 1. Визначення множини потенційних загроз КІС

Для визначення загального переліку потенційних загроз КІС введемо множину **H** у наступному вигляді:

$$\mathbf{H} = \{\bigcup_{k=1}^{n} H_k\} = \{H_1, H_2, \ldots, H_n\}, \quad (1)$$

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:

$$\mathbf{\Omega}_k = \{\bigcup_{p=1}^{m_k} \Omega_{kp}\} = \{\Omega_{k1}, \Omega_{k2}, \ldots, \Omega_{km_k}\}, \quad (2)$$

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 [11], представимо кортеж ω_{kp}, який враховує комбінацію типу загрози, умов середовища та часу її реалізації у наступному вигляді:

$$\omega_{kp} = \{< h_k, cond_{kp}, t_{kp} > \mid h_k \in H_k\}, \quad (3)$$

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:

$$RISK_i = \sum_{k=1}^{n} \sum_{p=1}^{m_k} \sum_{d=1}^{D} w_d \cdot P_{ikp} \cdot V_{ikp} \cdot C_{kd}^{(p)}, \quad (4)$$

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:

$$R_i(t) = e^{-\lambda_i t}, \quad (5)$$

де $R_i(t)$ – імовірність безвідмовної роботи елемента i у часі t, λ_i – інтенсивність відмов елемента i [11]. Інтенсивність відмов λ_i визначається згідно з [12] за емпіричними даними або статистикою експлуатації, відповідно до виразу:

$$\lambda_i = \frac{N_{fail,i}}{T_{obs,i}}, \quad (6)$$

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 [11], у наступному вигляді:

$$R_i^* = R_i + (1 - R_i) \cdot B_s \cdot R_{island}, \quad (7)$$

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:

$$RI_i = \frac{1}{T} \int_0^T \frac{P(t)}{P_{nom}} dt, \quad (8)$$

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 [10], як зважена сума часткових індексів:

$$RI_{sys} = \sum_{l} \beta_l \cdot RI^{(l)}, \sum_{l} \beta_l = 1, \quad (9)$$

де RI_{sys} – інтегральний індекс стійкості всієї системи, $RI^{(l)}$ – частковий показник стійкості l -го рівня (наприклад, 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 [11]. Для цього використовується нормована лінійна модель:

$$PSI_i^{(0)} = \alpha \cdot \widehat{RISK}_i + \beta \cdot \hat{R}_i + \gamma \cdot \widehat{RI}_i, \quad \alpha + \beta + \gamma = 1 \quad (10)$$

де $PSI_i^{(0)}$ – інтегральний показник базового рівня захищеності КІС, $\widehat{RISK}_i$, $\hat{R}_i$, $\widehat{RI}_i$ – 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 [5], наведена у Табл. 2.

Таблиця 2

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. 2, 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» [5].

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 [11, 13], введемо вираз у наступному вигляді:

$$\max_{\{s_k\}} \sum_i w_i \cdot PSI_i^{(0)}(s_k), \text{ за умов } \sum_k C_k \cdot s_k \le B, \quad R_i^* \ge R_{\min}, \quad RI_{sys} \ge R_{\min}, \quad (11)$$

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:

$$E_i = \frac{PSI_i^{(1)} - PSI_i^{(0)}}{PSI_i^{(0)}} \cdot 100\%, \tag{12}$$

де E_i – ефект підвищення рівня захищеності КІС, виражений у відсотках, $PSI_i^{(0)}$ – початкове значення інтегрального показника рівня захищеності, визначене за допомогою (10), $PSI_i^{(1)}$ – інтегральний показник після реалізації оптимальних стратегій.

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 дозволяє кількісно оцінювати стан безпеки, прогнозувати вплив потенційних загроз та визначати оптимальні стратегії підвищення стійкості з урахуванням обмежених ресурсів і умов функціонування в державі.

ВИСНОВКИ

У роботі було проведено комплексний аналіз сучасних підходів до оцінювання рівня захищеності КІС. В результаті якого встановлено, що наявні підходи не забезпечують комплексного урахування взаємозв'язків між ризиком, надійністю та стійкістю. Більшість досліджень орієнтована переважно на технічні або організаційні аспекти без врахування їх інтегрального впливу на загальний рівень безпеки критичної системи. Це свідчить про наявність важливого наукового завдання щодо розробки інтегрованого методу, який дозволяє поєднати кількісне оцінювання ризиків, показників надійності та характеристик стійкості у єдиний узгоджений підхід.

Було розроблено метод підвищення рівня захищеності КІС, який забезпечує комплексне оцінювання стану безпеки шляхом формалізації взаємозв'язків між ризиком, надійністю та стійкістю. Запропонований підхід передбачає використання інтегрального показника рівня захищеності, що дозволяє кількісно оцінювати поточний стан безпеки системи та прогнозувати вплив потенційних загроз. На відміну від відомих методів, у запропонованому підході враховано як технічні, так і організаційні фактори, а також введено механізм оптимізації стратегій підвищення стійкості з урахуванням обмежених ресурсів.

Продовженням даного дослідження стане експериментальна перевірка та верифікація запропонованого методу підвищення рівня захищеності КІС. Крім того, планується проведення апробації методу на практичних прикладах функціонування ОКІ різних галузей з метою доведення його ефективності, достовірності розрахунків та можливості адаптації до різних умов експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сидоренко, В., & Максимець, А. (2025). Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. Електронне фахове наукове видання *«Кібербезпека: освіта, наука, техніка»,* 3(27), 560–571. https://doi.org/10.28925/2663-4023.2025.27.779.
2. Закон України «Про критичну інфраструктуру» (2021). №1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20.
3. Кабінет Міністрів України. (2021). Постанова №1109 «Деякі питання забезпечення безпеки та стійкості критичної інфраструктури» від 09.10.2021. https://zakon.rada.gov.ua/laws/show/1109-2021-%D0%BF.
4. Кабінет Міністрів України. (2022). Постанова №518 «Про затвердження критеріїв віднесення об'єктів до категорій критичності» від 13.05.2022. https://zakon.rada.gov.ua/laws/show/518-2022-%D0%BF.
5. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2025). Методика оцінки стану захищеності об'єктів критичної інфраструктури (Наказ № 17 від 14.01.2025). https://zakon.rada.gov.ua/laws/show/z0375-25#Text
6. 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.
7. 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.
8. 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.
9. Кириленко, С. П., Тищенко, В. В. (2023). Моделі оцінювання ризиків для критичної інфраструктури в умовах збройного конфлікту. *Безпека життєдіяльності*, 3(9), 74–88.
10. 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.
11. 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
12. 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
13. 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
14. 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.
15. 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
16. 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

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Viktoriia Sydorenko
PhD, Associate Professor,
Associate Professor of the Department of Computer Information Technologies
State University «Kyiv Aviation Institute», Kyiv, Ukraine
ORCID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Serhii Sydorenko
PhD Student of the Faculty of Computer Science and Technology
State University «Kyiv Aviation Institute», Kyiv, Ukraine
ORCID: 0000-0002-7170-123X
serh.sydorenko@gmail.com

METHOD FOR ENHANCING THE SECURITY LEVEL OF THE STATE'S CRITICAL INFORMATION SYSTEMS

Abstract. In today's conditions of increasing cyber threats and the complexity of technological systems, ensuring the security of critical information systems (CIS) is one of the key tasks of national security of the state. Existing approaches to assessing the state of CIS security are mainly focused on individual technical or organizational aspects, which does not provide comprehensive consideration of the relationships between risk, reliability and stability. The article presents a method for increasing the level of CIS security, which involves formalizing the relationships between these parameters in the form of a system of mathematical expressions and introducing an integral indicator of the level of security. The proposed approach allows quantitatively assessing the current state of CIS security, predicting the impact of potential threats and determining optimal strategies for increasing stability, taking into account limited resources. The developed method ensures objective decision-making on risk management and increasing the effectiveness of CIS protection and contributes to the formation of an adaptive national cybersecurity system. Further research involves experimental testing and verification of the proposed method on examples of the functioning of critical infrastructure objects of various industries to assess its effectiveness, versatility and possibility of practical implementation.

Keywords: critical infrastructure, critical infrastructure objects, critical information systems, threats, security, level of security, stability, ensuring stability, efficiency, risk, reliability, risk management, optimization of strategies.

REFERENCES

1. Sydorenko, V., & Maksymets, A. (2025). Model for ensuring the stability of critical information systems under the influence of internal and external destabilizing factors. Electronic professional scientific publication *«Cybersecurity: education, science, technology»,* 3(27), 560–571. https://doi.org/10.28925/2663-4023.2025.27.779.
2. Law of Ukraine «On Critical Infrastructure» (2021). No. 1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20.
3. Cabinet of Ministers of Ukraine. (2021). Resolution No. 1109 «Some issues of ensuring the security and stability of critical infrastructure» dated 09.10.2021. https://zakon.rada.gov.ua/laws/show/1109-2021-%D0%BF.
4. Cabinet of Ministers of Ukraine. (2022). Resolution No. 518 «On Approval of Criteria for Assigning Objects to Criticality Categories» dated 05/13/2022. https://zakon.rada.gov.ua/laws/show/518-2022-%D0%BF.
5. Administration of the State Service for Special Communications and Information Protection of Ukraine. (2025). Methodology for Assessing the Security Status of Critical Infrastructure Objects (Order No. 17 dated 01/14/2025). https://zakon.rada.gov.ua/laws/show/z0375-25#Text
6. Murasov, R., Melnyk, Ya. (2023). Assessment of Cyberspace Security of Critical Infrastructure Objects of Ukraine. *Modern Information Technologies*, (3), 98–112. https://sit.nuou.org.ua/article/view/280288.
7. Sukhodolya, O. (2022). Sustainability of critical energy infrastructure and community life. Analytical report of the National Institute of Energy and Infrastructure, 72 p. https://chtyvo.org.ua/.../Stiikist_krytychnoi_enerhetychnoi_infrastruktury_ta_zhyttiediialnosti_hromad

8. Shevchenko, N. I., Plahotniuk, R. V. (2024). Methodological approaches to assessing the sustainability of critical infrastructure facilities in a special period of the functioning of the Ukrainian economy. *Economic Reform and Innovative Development Strategies*, 14(2), 112–126. https://reicst.com.ua/pmtl/article/view/2024-14-02-08.
9. Kyrylenko, S. P., Tyshchenko, V. V. (2023). Risk assessment models for critical infrastructure in armed conflict. *Life Safety*, 3(9), 74–88.
10. Tretyakov, O. V., Khalmuradov, B. D., Kichata, N. M., & Remska, A. V. (2025). An approach to quantitative assessment of the stability of critical infrastructure facilities. *Control, Navigation and Communication Systems*, 1(79), 178–183. https://doi.org/10.26906/SUNZ.2025.1.178-183.
11. 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
12. 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
13. 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
14. 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.
15. 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
16. Sydorenko, V. (2025). Method for assessing the stability of objects of critical information infrastructure of the state. Electronic professional scientific publication *«Cybersecurity: education, science, technology»,* 1(29), 837–853. https://doi.org/10.28925/2663-4023.2025.29.944