УДК 331.1:331.45:355.58:519.2:614.8:614.89
DOI: 10.30838/UJCEA.0333.270526.16.1239

ОБМЕЖЕННЯ ЧИННОГО РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

БЄЛІКОВ А. С.[1], *докт. техн. наук, проф.,*
МАЦУК З. М.[2*], *канд. техн. наук, доц.,*
РУДЕНКО В. П.[3], *асп.,*
АТАНЕСЯН А. А.[4], *асп.*

[1] Кафедра охорони праці, цивільної та екологічної безпеки, Український державний університет науки і технологій, ННІ «Придніпровська державна академія будівництва та архітектури», вул. Архітектора Олега Петрова, 24-а, 49005, Дніпро, Україна, тел. + 38 (0562) 47-03-25, e-mail: belikov@pdaba.edu.ua, https://orcid.org/0000-0001-5822-9682
[2*] Кафедра охорони праці, цивільної та екологічної безпеки, Український державний університет науки і технологій, ННІ «Придніпровська державна академія будівництва та архітектури», вул. Архітектора Олега Петрова, 24-а, 49005, Дніпро, Україна, тел. +38 (067) 731-52-26, e-mail: matsuk.zachar@pdaba.edu.ua, https://orcid.org/0000-0001-6114-9536
[3] Кафедра охорони праці, цивільної та екологічної безпеки, Український державний університет науки і технологій, ННІ «Придніпровська державна академія будівництва та архітектури», вул. Архітектора Олега Петрова, 24-а, 49005, Дніпро, Україна, тел. +38 (099) 655-57-55, e-mail: v.p.rudenko@ust.edu.ua, https://orcid.org/0009-0002-0221-2640
[4] Кафедра охорони праці, цивільної та екологічної безпеки, Український державний університет науки і технологій, ННІ «Придніпровська державна академія будівництва та архітектури», вул. Архітектора Олега Петрова, 24-а, 49005, Дніпро, Україна, тел. +38 (099) 359-44-58, e-mail: atanesian.aram@365.pdaba.edu.ua, https://orcid.org/0009-0005-9159-0775

Анотація. ***Постановка проблеми.*** Критична інфраструктура (надалі – КІ) є основою стійкого функціонування держави. В умовах зростання техногенної складності, цифровізації та гібридних загроз питання забезпечення безпеки КІ виходить за межі класичних підходів до ризик-менеджменту, оскільки відмова або компрометація окремого елемента системи може ініціювати каскадні ефекти з порушенням міжсекторальних залежностей. Традиційно управління безпекою спирається на ризик-орієнтовану парадигму, в межах якої загрози інтерпретуються через ймовірність реалізації небажаних подій і тяжкість наслідків, а ризик розглядається як вплив невизначеності на цілі. Однак застосування базових підходів виявляє системні обмеження, пов'язані з невизначеністю у прийнятті рішень, нелінійністю природи ризику, адаптивною поведінкою суб'єктів загроз, динамічною зміною конфігурацій фізичних і кіберфізичних систем, що є проблемою. Це формує потребу у переосмисленні меж застосовності відомих моделей ризик-менеджменту та розробленні нових удосконалених рамок, які врахують ризик, стійкість та сценарну невизначеність. ***Мета статті*** – обґрунтувати межі застосовності відомих ризик-орієнтованих підходів у КІ, запропонувати критерій валідності ризик-оцінювання та концептуальну модель формалізації ефективності заходів безпеки. ***Висновок.*** Обґрунтовано, що ключове обмеження чинних ризик-орієнтованих підходів полягає у методологічній асиметрії: ймовірність загроз оцінюється, тоді як ймовірність ефективності заходів безпеки не є обов'язковим елементом оцінювання безпеки. Обґрунтовано, що в практичних реалізаціях ризик-орієнтованого підходу ймовірнісна природа заходів безпеки часто не враховується, як у процедурах оцінювання ризику, так і при встановленні рівня безпеки. Запропоновано використання принципу адекватності ймовірностей як метакритерію валідності ризик-оцінювання, як основу формалізації динамічного балансу загроз і контрзаходів, для підвищення керованості безпеки КІ.

Ключові слова: *критична інфраструктура; менеджмент ризиків; оцінювання ризику; методологічна асиметрія; принцип адекватності ймовірностей; ймовірність ефективності контрзаходів; прогнозне оцінювання; залишковий ризик; стійкість*

LIMITATIONS OF THE CURRENT RISK-ORIENTED APPROACH TO ENSURING CRITICAL INFRASTRUCTURE SECURITY

BIELIKOV A.S.[1], *Dr. Sc. (Tech.), Prof.,*
MATSUK Z.M.[2*], *Cand. Sc. (Tech.), Assoc. Prof.,*
RUDENKO V.P.[3], *Postgrad. Stud.,*
ATANESIAN A.A.[4], *Postgrad. Stud.*

[1] Department of Labour Protection, Civil and Ecological Safety, Ukrainian State University of Science and Technologies, ESI "Prydniprovska State Academy of Civil Engineering and Architecture", 24-a, Architect Oleh Petrov St., Dnipro, 49005, Ukraine, tel. +38 (0562) 47-03-25, e-mail: belicov@pdaba.edu.ua, https://orcid.org/0000-0001-5822-9682

[2*] Department of Labour Protection, Civil and Ecological Safety, Ukrainian State University of Science and Technologies,

ESI "Prydniprovska State Academy of Civil Engineering and Architecture", 24-a, Architect Oleh Petrov St., Dnipro, 49005, Ukraine, tel. +38 (067) 731-52-26, e-mail: matsuk.zachar@pdaba.edu.ua, https://orcid.org/0000-0001-6114-9536
[3] Department of Labor Protection, Civil and T Ecological Safety, Ukrainian State University of Science and Technologies, ESI "Prydniprovska State Academy of Civil Engineering and Architecture", 24-a, Architect Oleh Petrov St., Dnipro, 49005, Ukraine, tel. +38 (099) 655-57-55, e-mail: v.p.rudenko@ust.edu.ua, https://orcid.org/0009-0002-0221-2640
[4] Department of Labor Protection, Civil and Ecological Safety, Ukrainian State University of Science and Technologies, ESI "Prydniprovska State Academy of Civil Engineering and Architecture", 24-a, Architect Oleh Petrov St., Dnipro, 49005, Ukraine, tel. +38 (099) 359-44-58, e-mail: atanesian.aram@365.pdaba.edu.ua, https://orcid.org/0009-0005-9159-0775

Abstract. ***Problem statement.*** Critical infrastructure (hereinafter referred to as CI) constitutes the foundation of the state's resilient functioning. Under conditions of increasing technological complexity, digitalization, and hybrid threats, ensuring CI security extends beyond classical risk management approaches, since the failure or compromise of an individual system element may initiate cascading effects accompanied by disruptions of intersectoral dependencies. Traditionally, security management has relied on a risk-oriented paradigm, within which threats are interpreted in terms of the probability of occurrence of undesirable events and the severity of their consequences, while risk is understood as the effect of uncertainty on objectives. However, the application of these baseline approaches reveals systemic limitations associated with decision-making uncertainty, the nonlinear nature of risk, the adaptive behavior of threat actors, and the dynamic reconfiguration of physical and cyber-physical systems. This, in turn, creates a need to reconsider the applicability boundaries of established risk management models and to develop new, enhanced frameworks that account for risk, resilience, and scenario-based uncertainty simultaneously. ***The purpose of the article*** is to justify the boundaries of applicability of currently established risk-based (risk-oriented) approaches in critical infrastructure, to propose a validity criterion for risk assessment procedures, and to develop a conceptual model for the formalization of security measure effectiveness. ***Conclusions.*** The principal limitation inherent in current risk-based approaches has been substantiated: they exhibit methodological asymmetry, whereby threat probabilities are quantified while the probabilities of security measure effectiveness remain non-mandatory elements of safety assessment. It is shown that practical realizations of risk-oriented methodologies commonly neglect the stochastic character of protective measures, both in the risk evaluation process and in the establishment of target safety levels. The principle of probability adequacy is advanced as a meta-criterion of risk assessment validity. This principle provides the conceptual foundation for formalizing the dynamic balance between threats and countermeasures, ultimately improving the controllability (governance) of critical infrastructure safety.

Keywords: *critical infrastructure; risk management; risk assessment; methodological asymmetry; probability adequacy principle; probability of control effectiveness; ex ante assessment; residual risk; resilience*

Постановка проблеми. Сучасна практика управління ризиками [1-7] враховує ймовірності реалізації загроз, однак не вимагає проведення обов'язкової ймовірнісної оцінки ефективності заходів безпеки. Це формує принциповий розрив між декларованими та фактично досягнутими показниками зниження ризику (як показника підвищення рівня безпеки системи), внаслідок чого втрачається основна управлінська функція ризик-менеджменту: система стає такою, що здатна описувати ризики, але не забезпечує доказовості та адекватності прогнозу зниження ризику.

У межах даного дослідження терміни тлумачаться наступним чином: небезпека (hazard) – джерело/умова з потенціалом завдання шкоди; загроза (threat) – подія/дія або особа (актор), здатні ініціювати реалізацію небезпеки; ризик (risk) – ефект невизначеності на цілі безпеки та стійкості системи, що формується у конкретних сценаріях.

Загальноприйнята логіка у сучасній практиці ризик-менеджменту ґрунтується на наступних базових припущеннях:

– реалізація небезпек через загрози має ймовірнісний характер і підлягає оцінюванню;

– захід безпеки трактується як детермінований фактор зниження ризику, без моделювання ймовірності його успіху/відмови.

Зрозуміло, що в сучасних умовах функціонування критичної інфраструктури ці припущення є методологічно неповними, тому що заходи безпеки, як і загрози, також мають ймовірнісну природу.

У контексті даного дослідження під ймовірністю ефективності заходу безпеки розуміється умовна ймовірність того, що за заданого контексту, режиму функціонування та часових обмежень відповідний захід забезпечує досягнення запланованого ризик-знижувального ефекту щодо визначеного сценарію небезпеки.

Такий ефект може проявлятися у зменшенні ймовірності ініціювання

небезпечної події, обмеженні масштабів її ескалації або зниженні тяжкості наслідків, при цьому сама ефективність заходу розглядається як величина, чутлива до невизначеності, деградації та змін умов експлуатації.

Отже, у парадигмі сучасної безпеки заходи не гарантують зниження ризику, їх ефективність не оцінюється через ймовірність «успіху» та розподіл ефективності і при цьому вони все ж впроваджуються, що становить проблему.

Розглянуті обмеження не залежать від галузі КІ та притаманні широкому класу кіберфізичних і соціотехнічних систем.

Мета дослідження – обґрунтувати межі застосовності відомих ризик-орієнтованих підходів у КІ, запропонувати критерій валідності ризик-оцінювання та концептуальну модель формалізації ефективності заходів безпеки.

Методологічною основою дослідження є системний та ризик-орієнтований підходи. Застосовано нормативно-структурний і логіко-структурний аналіз міжнародних та національних вимог з управління ризиками безпеки критичної інфраструктури. Узагальнення результатів здійснено шляхом концептуального моделювання контурів ризик-менеджменту та формулювання критеріальних положень щодо адекватності ризик-орієнтованого підходу в умовах невизначеності та динаміки загроз.

Результати досліджень. Сучасна дискусія у сфері ризик-менеджменту розгортається у трьох взаємопов’язаних площинах:

1. методична – нездатність моделей оцінювати реальне зниження ризику («до/після» впровадження заходів);

2. аналітична (оцінювальна) – переважання показників звітності над показниками, що відображають вплив заходів на ризик;

3. управлінська – масове впровадження заходів без попередньої оцінки їх ефективності.

Наприклад, за оглядами консалтингових і аналітичних звітів, практики повномасштабної кількісної оцінки ризиків інформаційної безпеки залишаються обмеженими, що інтерпретується як недостатня зрілість підходів [8].

З методологічної точки зору такі показники як кількість сповіщень про загрози, обсяги охоплення перевірками, а також показник середнього часу виявлення загроз і реагування на них, поза контекстом реальної ідентифікованої небезпеки, є переважно показниками процесу, а не показниками результативності. Такий підхід декларує керованість діяльності, проте не дає відповіді, чи зменшилися очікувані втрати, частота інцидентів, ймовірність реалізації небезпечного сценарію або масштаб наслідків. У галузевих публікаціях це явище описують як феномен імітації безпеки, коли показники оцінки ризику створюють видимість контролю, але слабо пов’язані з реальним зниженням ризику та фактичним рівнем уразливості систем [9].

Для об’єктів КІ така ситуація є особливо гострою, оскільки зростання «інтенсивності робіт» супроводжується погіршенням прогнозу профілю ризику через зміну (модифікацію) загроз, старіння обладнання, пропорційного зниження ефективності заходів безпеки, накопичення інших прихованих відмов (відхилень) тощо.

Поєднання невизначеності щодо реального зниження ризику та домінування показників «для звітності» створює сприятливі умови для поширення такого підходу, коли заходи розробляються і впроваджуються насамперед задля виконання формальних вимог законодавства. Як наслідок, організації масштабно закуповують товари, послуги, приймають організаційні рішення тощо без верифікованої оцінки їхньої дієвості з позицій прогнозного зниження ризику.

В оглядових матеріалах галузевих видань підкреслюється потреба визначати пріоритетність заходів на основі прогнозу зниження ризику, а не на основі декларативних заяв аудиторів (експертів) або тиску з боку формальної необхідності [10].

Разом з цим, у трендах провідних аналітичних компаній акцентується, що взаємозалежності, регуляторні зміни та динаміка загроз вимагають переходу від типових заходів безпеки до управління

стійкістю та наслідками, тобто до логіки результативності, а не активності [11].

Відомо, що будь-яка діяльність завжди описується як процес із входами, виходами, ресурсами, власником процесу та показниками результативності.

Відповідно, у безпеці це коли**:**

– небезпека «вбудована» в процес;

– керуємо параметрами процесу;

– рішення перевірені і відтворювані.

Відомо, що менеджмент ризиків включає наступні процеси [2]:

1. Комунікація та консультації.
2. Встановлення сфери застосування, контексту і критеріїв.
3. Оцінювання ризику, яке включає:

– ідентифікацію ризику;

– аналіз ризику;

– оцінювання ризику;

4. Оброблення ризику.
5. Моніторинг і аналіз процесів
6. Документування і звітність.

Вивчення стандарту [2] дозволяє зробити висновок, що цей стандарт не містить посилань на методику, яка б прямо встановлювала, як саме кількісно визначати ефективність заходів безпеки до їх впровадження. Стандарт задає принцип: обрати опції оброблення ризику, спланувати їх, а потім оцінити ефективність після реалізації (ex post) і прийняти рішення щодо залишкового ризику. Водночас прогноз ефективності до впровадження заходів (ex ante) у стандарті не формалізовано як обов’язковий елемент.

Таким чином, у чинній рамці ризик-менеджменту відсутній механізм перевірки адекватності очікуваного зниження ризику до реалізації заходів безпеки.

Тобто стандарт [2] є рамковим документом, який не дає інструментарію для доказового прогнозування ефективності заходів безпеки (до/після), відповідно не забезпечує адекватну оцінку рівня безпеки. Стандарт [3] також не встановлює конкретної галузевої процедури оцінювання ефективності заходів безпеки та залишає її вибір за організацією.

Мінімальною вимогою раціональності у межах [2; 3] є недопущення впровадження заходів безпеки, сукупний ризик внаслідок упровадження яких перевищує ризик, що підлягає зменшенню.

У рамках [2] за використанням технік [3] ефективність заходів безпеки до впровадження визначається як прогнозна зміна параметрів сценаріїв і бар’єрів у моделі ризику.

Водночас, відомо, що у реальних умовах експлуатації об’єктів КІ відсутність репрезентативних даних та унікальність аварійних комбінацій істотно обмежують якість оцінок. За цих умов оцінювання ефективності заходів безпеки зводиться до припущень, доповнених експертними судженнями, які самі є джерелом невизначеності, а отже не забезпечують доказового підтвердження ризику до реалізації заходів.

Стандарт [3] передбачає верифікацію і валідацію результатів оцінювання ризику, перевірку критичних припущень та аналіз чутливості, а також доведення наявності невизначеності до осіб, які ухвалюють рішення. Однак за відсутності емпіричних даних ці процедури забезпечують переважно логічну узгодженість моделей, але не гарантують адекватності ймовірнісних параметрів, що є критичним обмеженням сучасних ризик-орієнтованих підходів у КІ.

Постають питання: якщо небезпека має ймовірнісну природу, а ризик, пов'язаний з її реалізацією, підлягає оцінюванню та обробці, чому в практиці не враховується ймовірнісна природа ефективності заходів безпеки?

Чому ймовірність позитивного (ризик-знижувального) впливу заходів безпеки не підлягає ані оцінюванню, ані подальшій обробці в контурі ризик-менеджменту?

Україна не стала винятком. Відповідно до вимог абзацу другого частини першої статті 22 Закону України «Про критичну інфраструктуру» [12], 1 квітня 2025 року Кабінет Міністрів України затвердив «Вимоги щодо управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності» [13] (далі – Вимоги).

Під час проведення досліджень нами визначено обмеження вітчизняного ризик-орієнтованого підходу до забезпечення безпеки КІ, а саме (рис. 1).

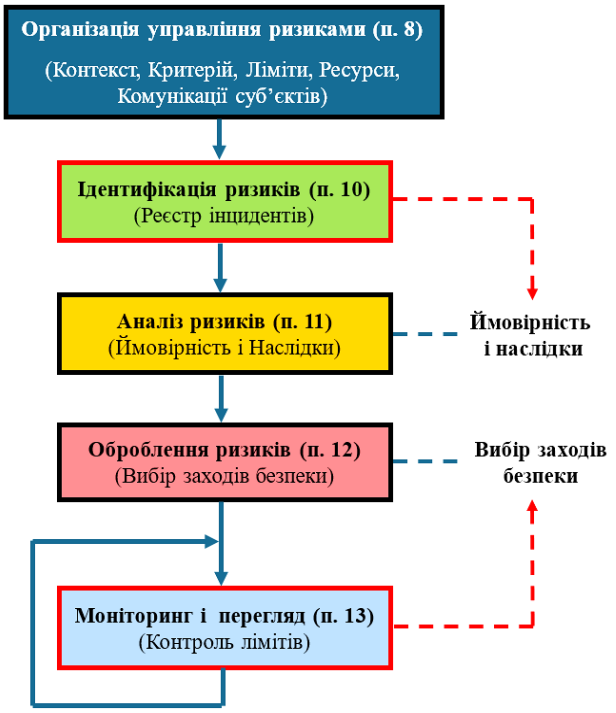

Рис. 1. Поточний контур ризик-орієнтованого підходу до безпеки КІ (І категорії)

Виявлені обмеження доцільно розглядати у двох взаємопов'язаних, але принципово різних площинах: нормативно-методологічній та практично-операційній.

Нормативно-методологічні обмеження зумовлені рамковим характером чинних стандартів і регуляторних документів та полягають у відсутності формалізованих вимог щодо обов'язкового прогнозного (ex ante) ймовірнісного оцінювання ефективності заходів безпеки.

Практично-операційні обмеження пов'язані з особливостями впровадження ризик-орієнтованого підходу в реальних умовах експлуатації об'єктів КІ та проявляються у домінуванні процесних і звітних показників над показниками фактичного зниження ризику, обмеженій доступності репрезентативних даних і високій залежності оцінок від експертних суджень.

Подальший аналіз обмежень вимог [13] здійснюється з урахуванням зазначеного розмежування.

Пункт 8 [13].

Статичний контекст при динамічній природі загроз.

Вихідні дані фактично задають «паспортну» модель об'єкта і загроз, але не описують темп змін, деградацію захистів, старіння обладнання, а також еволюцію загроз. У промисловості це критично, бо частота відмов, режимні порушення та «дрейф» процедур системно змінюють ризик у часі.

У документі наявна логічна недосконаліть організації рівнів аналізу: національний/секторальний/об'єктовий.

Проєктні загрози трьох рівнів подані як одне поле даних, але не визначено механізм узгодження масштабів: макрорівневі ризики погано транслюються в параметри HAZOP/FMEA, а мікрорівневі відмови не агрегуються коректно на рівень сектора. Це формує несумісність моделей і «розриви» при переході між рівнями.

Документ не містить явної вимоги до моделювання залежностей і каскадності процесів.

Є фраза про «зв'язок об'єкта з іншою інфраструктурою», але без інструментів (байєсівські мережі, мережеві моделі, системна динаміка) ця вимога лишається декларативною. Для КІ це породжує недооцінку каскадних відмов і ефектів доміно.

Пункт 9 [13].

Послідовність «ідентифікація → аналіз → оброблення» є коректною логікою, але у тексті постанови відсутня окрема пряма стадія «оцінювання ефективності контрзаходів» та їх оброблення до впровадження, які є обов'язковими.

Пункт 10 [13].

Ключова проблема тут наступна: ідентифікація визначає інциденти та показники, але не задає причинно-наслідкову модель, не вимагає:

- сценарної структури;
- моделі бар'єрів безпеки;
- опису людського чинника як окремого механізму (HEP/HRA), а не як «фактору».

Пункт 11 [13].

Ймовірність визначається, але не перевіряється на адекватність.

Документ дозволяє кількісні, якісні та комбіновані показники, але не встановлює вимоги до:

- калібрування експертних оцінок;
- обліку похибок вимірювань;
- моделювання невизначеності.

В умовах експлуатації КІ ймовірності часто оцінюються з неповних даних або за аналогіями, тому без спеціальних методів, нечіткої логіки або інтервальних моделей, на виході, оператори отримують «точні числа з неточних припущень».

Водночас ранжування ризиків, як визначення і процес, підміняє керування ризиками. Ранжування (визначення вагомості) тут зручне, але:

- воно не гарантує оптимальності розподілу ресурсів;
- ігнорує взаємозалежність ризиків;
- часто стимулює локальну оптимізацію замість підвищення системної стійкості.

Для КІ це породжує типову помилку: оператори обирають заходи проти «найбільшого» ризику, але не проти найбільш системно небезпечного сценарію з каскадною ескалацією.

Також, у документі, деградація бар'єрів не параметризована.

У тексті постанови немає вимоги щодо моделювання:

- зниження надійності бар'єрів у часі;
- прихованих відмов захисту;
- залежних відмов.

Отже, аналіз ймовірності інцидентів стає історично-статистичним, тоді як безпека в промисловості є динамічною характеристикою системи.

Пункт 12 [13].

Відомо, що «вузьке» місце ризик-орієнтованих підходів, це впровадження заходів безпеки без прогнозу їх ефективності з оцінкою постфактум.

В тексті постанови вказано на «визначення найбільш ефективного заходу», але не встановлено процедури оцінювання його ефективності до впровадження.

У результаті рішення може бути прийняте на основі:

- експертної думки;
- звички («так прийнято»);
- перевірочних листів, без кількісного зв'язку з ризиком.

Для промислових КІ це створює ілюзію керованості, коли ризик зменшується «на папері», але не зменшується в реальному процесі.

На додаток, рамкою підходу постанови «супутні ризики» згадано, але також без вимог щодо їх інструментів оцінювання.

Законодавець вказує на супутні ризики від заходів, але не вимагає застосування методів їх аналізу та моделювання.

Тому існує ризик ідентифікувати супутні ризики і не врахувати їх вплив на вибір заходів безпеки для усієї системи.

Пункт 13 [13].

Моніторинг і перегляд актуальності не рідше 1 разу на рік – недостатньо для КІ.

Вимога «не рідше одного разу на рік» на практиці означає – один раз на рік.

Такий цикл перегляду не відповідає реальній змінності умові/модифікації ризиків КІ. Для динамічних загроз потрібне оновлення ризику з частотою, співрозмірною темпу зміни режимів/загроз і мінімум 3 горизонти моніторингу:

- оперативний (дні/тижні),
- тактичний (місяці/квартали),
- стратегічний (рік).

Для багатьох промислових об'єктів КІ параметри процесу можуть змінюватися щогодинно, а деградація бар'єрів має нелінійний характер. Інциденти КІ можуть розгортатися за хвилини. Тому «раз на рік» створює структурне запізнення у контурі ризик-менеджменту КІ .

Далі. Законодавець говорить про «контроль наближення ризику до лімітів», але не вимагає оцінки:

- показників працездатності бар'єрів;
- провідних індикаторів та верифікації фактичного зниження ризику після впровадження заходів.

Таким чином, моніторинг ризику перетворюється на моніторинг документації.

Отже, ризик-орієнтований підхід є методологічно неадекватним, якщо в оцінюванні враховується ймовірність реалізації загроз, але не враховується ймовірність досягнення запланованого ефекту заходів безпеки.

Оновлений контур ризик-менеджменту КІ України, з урахуванням зняття існуючих обмежень, пропонується такий як наведено на рисунку 2.

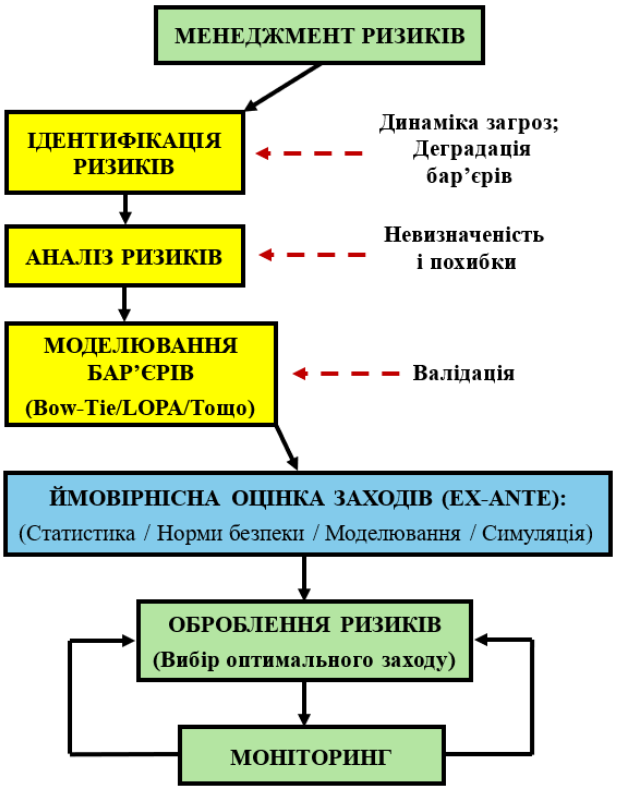

Рис. 2. Цільовий контур ризик-менеджменту КІ

Отже, у базовому підході відбувається асиметрія ймовірностей, яка породжує систематичне зміщення оцінки рівня ризику.

Нормативна рамка, визначена [2; 13]. формує контур, що оптимізує відповідність і ранжування, але не забезпечує доказового прогнозу результативності заходів безпеки та адекватності залишкового ризику в умовах деградації й еволюції загроз.

Вочевидь, виникає потреба у розробленні нових, цільових, галузевих, об'єктово-орієнтованих методологій ризик-менеджменту, адаптованих до КІ на базі оновлених стандартів [1–3].

На нашу думку, концептуальні методи ризик-менеджменту повинні враховувати ймовірнісну природу і небезпек, і заходів, проводити їх оцінювання та подальше взаємовідносне оброблення (рис. 3).

На нашу думку, процеси ризик-менеджменту (рис. 3) необхідно доповнити операцією декомпозиції небезпек, з дво- або більше рівневою структурою оцінки (рис. 4). Декомпозиція потрібна і для спрощення системи рівнянь моделювання ризик-подій і для розробки адекватних заходів безпеки.

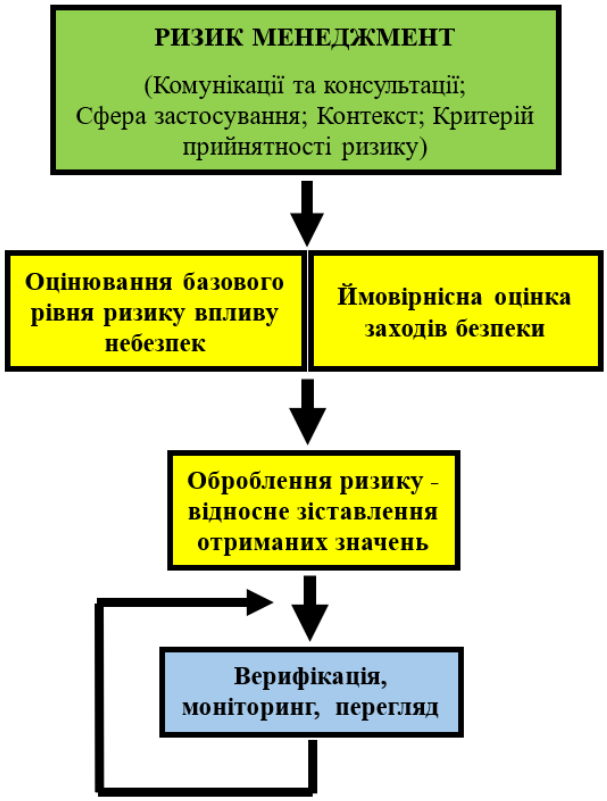

Рис. 3. Концептуальний контур процесів ризик-менеджменту КІ

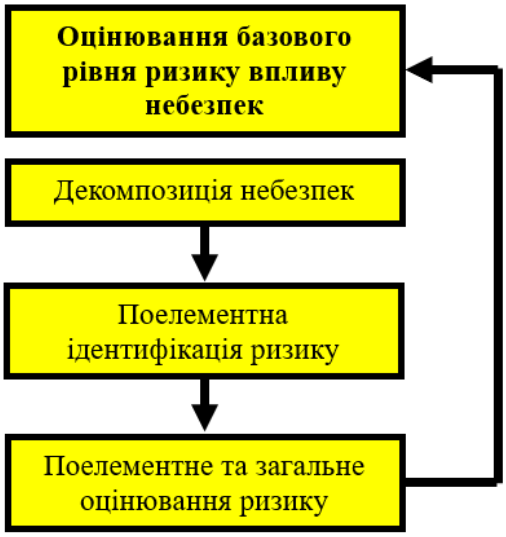

Рис. 4. Оцінювання базового рівня ризику вливу небезпек КІ

Щодо побудови ймовірнісної моделі оцінки заходів безпеки, то це сфера математичного моделювання.

Мета такої моделі – забезпечення формалізованої відповідності між «небезпека → ризик → захід безпеки → залишковий ризик → безпека», до впровадження заходу. Дієвість заходу тут не є детермінованою константою, а має:

a) ймовірність «успіху»/«відмови»;

b) умовний розподіл величини ефекту;

с) деградацію в часі та залежність від режимів/контексту.

При цьому, точність прогнозування це функція, а саме:

$$PA = f(PS, DQ, SA), \quad (1)$$

де PA – точність прогнозування; PS – структура процесу; DQ – якість даних; SA – задоволення припущень.

Тоді, ефективність прогнозування – це ступінь досягнення цілей управління або прийняття рішень завдяки прогнозу. Не плутати із ступінем статистичної близькості прогнозу до факту.

Отже, розробку заходів безпеки доцільно розпочинати після ідентифікації небезпек та визначення цілей систем, які взаємодіють, декомпозованих до рівня, що забезпечує можливість математичної формалізації механізмів реалізації їх мети.

Достатнім рівнем декомпозиції слід вважати такий рівень, на якому процеси реалізації небезпек можуть бути математично або фізично змодельовані.

Припущення дослідження наступні:

– небезпека це джерело потенційної шкоди;

– захід безпеки це джерело потенційної користі/засіб зменшення потенційної шкоди та/або тяжкості цієї шкоди;

– алгоритм прогнозування «успіху» в антагоністичній парі симетричний для обох об'єктів прогнозування;

– теорія ймовірностей не розрізняє небезпеку і заходи як такі – вона прогнозує ймовірності реалізації подій (включно з подіями відмови бар’єрів, подіями ескалації, подіями реалізації сценарію тощо).

Гіпотеза дослідження наступна: «У спрощеній антагоністичній постановці небезпеки та заходи можуть бути формалізовані як стохастично еквівалентні фактори протилежного знаку, тоді як їх інтерпретація як «шкоди» або «захисту» визначається виключно цілями та позицією спостерігача».

Гіпотеза ілюструється на спрощеній антагоністичній постановці: «Коли йде двобій об'єктів і обидва об'єкти мають на меті знищення один одного, то напад стає і небезпекою, і заходом безпеки одночасно в даний момент часу».

У даному дослідженні під симетричністю методів і методологій ймовірнісного аналізу розуміється те, що оцінювання ймовірності реалізації загроз та оцінювання ймовірності досягнення запланованого ефекту заходів безпеки є однотипними задачами стохастичного моделювання, які відрізняються виключно умовами та знаком впливу на цілі системи.

У цій постановці розглядаються не «дії» як такі, а випадкові події їх результатів, що дозволяє відокремити математичну структуру ймовірнісного опису від семантичної інтерпретації впливу як «загрози» або «контрзаходу».

Математичну формалізацію та перевірку (доведення) гіпотези можливо представити у наступному вигляді.

Розглянемо стохастичну систему, що описує взаємодію двох агентів A та B.

Антагоністична стохастична постановка вводиться як формальний інструмент для обґрунтування методологічної симетрії ймовірнісного аналізу небезпек і заходів безпеки.

У такій постановці одні й ті самі випадкові події (результати дій, відмови бар’єрів, ескалації) мають інваріантну ймовірнісну структуру, тоді як їх інтерпретація як загроз або заходів безпеки визначається виключно знаком впливу на цільовий функціонал суб’єкта.

Звідси випливає, що техніки [2; 3] є застосовними симетрично як до оцінювання ймовірності реалізації загроз, так і до ймовірнісного оцінювання заходів безпеки за фіксованого контексту, а центральним обмеженням практики є не відсутність математичного апарату, а відсутність нормативної вимоги та процедурної необхідності оцінювати ймовірність ефекту попередні оцінки заходів.

Наприклад, FTA/ETA формалізують структуру причинно-наслідкових комбінацій подій для сценарію ініціювання небезпеки і можуть працювати для сценарію відмови/успіху бар’єра/заходу; байєсівські мережі – залежності між подіями загроз і заходів безпеки; марковські моделі – деградацію станів загроз і заходів у часі.

1. Математична модель.

1.1. Простір станів.

Стан системи в момент часу $t \geq 0$ задається вектором:

$$S(t) = (s_A(t), s_B(t)) \in \mathrm{R}_+^2, \quad (2)$$

де $S(t)$ – вектор стану системи в момент часу t; $s_A(t)$ – величина що характеризує стан агенту A; $s_B(t)$ – величина що характеризує стан агенту B; R^2_+ – простір станів.

Вираз (2) означає, що в кожний момент часу система описується двовимірним вектором невід'ємних випадкових величин, які кількісно характеризують стан кожного з двох антагоністично взаємодіючих агентів.

1.2. Простір дій.

Кожен агент $i \in \{\mathrm{A},\mathrm{B}\}$ у кожний момент часу $t \geq 0$ обирає керування (вплив).

$$a_i(t) \in K \subset \mathrm{R}_+, \quad (3)$$

де $a_i(t)$ – адаптована керуюча зміна; K – компактна множина допустимих значень інтенсивності дій; $K \subset \mathrm{R}_+$ – множина всіх допустимих значень інтенсивності дій.

1.3. Стохастична динаміка.

Еволюція системи описується системою диференціальних рівнянь (4, 5):

$$ds_A(t) = -\xi(a_B(t))dt + \sigma dW_A(t), \quad (4)$$

$$ds_B(t) = -\xi(a_A(t))dt + \sigma dW_B(t), \quad (5)$$

де $s_A(t)$, $s_B(t)$ – це поточний стан агентів A і B у момент часу t; $a_A(t)$, $a_B(t)$ – це дії агентів A і B у момент часу t; $\xi(\cdot)$ – функція, яка перетворює силу дії на реальну шкоду. Мінус, тому що дія знижує показники стану опонентів A, B; dt – елементарний проміжок часу; $W_A(t)$,$W_B(t)$ – величина, яка описує випадкові процеси (вінерівські процеси); $dW_A(t)$,$dW_B(t)$ – величина, яка характеризує випадкові зміни (незначні); σ – коефіцієнт, який показує наскільки сильний випадковий вплив.

Рівняння описують як з часом змінюється рівень «життєздатність» агентів під взаємним впливом дій кожного окремо опонента та впливом випадкових зовнішніх факторів.

Ключова ідея моделі. Кожен агент шкодить лише опоненту, а не самому собі. A впливає на B, B впливає на A. Власні дії напряму не «виснажують» власний стан (це свідоме спрощення), що робить модель абсолютно антагоністичною.

Зазначене спрощення введено навмисно з метою елімінування другорядних ефектів та фокусування виключно на інваріантності ймовірнісної структури подій, що є принциповим для обґрунтування методологічної симетрії аналізу небезпек і заходів безпеки.

2. Цільові функціонали та коректна нульова сума.

2.1. Базовий функціонал.

Вводиться єдиний функціонал «позитивного результату» для агента A.

$$J_A(a_A, a_B) = \mathrm{E}\left[\int_0^T (s_A(t) - s_B(t))dt\right], \quad (6)$$

де J_A – критерій позитивного результату для агента A; a_A,a_B – дії (стратегії) агентів A, B; $J_A(a_A,a_B)$ – вираз означає, що результат дій агента A залежить від дій обох сторін, а не лише від нього самого; $\int_0^T$ – інтеграл, означає підсумовування по часу (накопичення в часі). Враховується увесь інтервал часу, від 0 до T, де $T > 0$ це фіксований горизонт аналізу, до якого оцінюється результат; $\mathrm{E}[\cdot]$ – математичне сподівання за траєкторіями стохастичного процесу; $s_A(t)$, $s_B(t)$ – стани агентів A, B; dt – елементарний проміжок часу, це означає, що ми враховуємо не лише величину «позитивного результату), а й те, як довго він зберігається.

У кожен момент часу дивимось хто з опонентів сильніший: A чи B; підсумовуємо цю перевагу за весь час; усереднюємо з урахуванням випадкових факторів; отримуємо результат для агента A.

Вираз (6) показує, що агент A максимізує інтегральну різницю між власною «життєздатністю» та «життєздатністю» опонента B, що відповідає максимізації прагнення «виживання» обох опонентів.

2.2. Антагоністичність безпеки.

Функціонал агента B визначається як показано у (7):

$$J_B(a_A, a_B) := -J_A(a_A, a_B), \quad (7)$$

де J_A, J_B – критерії позитивного результату для агентів A та B; Вираз (7) означає, що все що вигідно для агента A, на стільки ж невигідно для агента B.

Доведення тут, це пряма підстановка:

$$J_B(a_A, a_B) - J_A(a_A, a_B) = 0, \quad (8)$$

Рівності (6, 7) визначають гру з нульовою сумою; отже, у жодних додаткових припущеннях щодо часових моментів реалізації мети опонентів A, B чи позитивності очікувань немає необхідності. Мінімально необхідну і достатню умову антагоністичності моделі можна вважати описаною.

3. Маржинальний ефект дії агентів.

Нехай стратегія агента B зафіксована. Це означає, що агент B поводиться однаково в обох випадках, аналізуємо лише наслідок рішення агента A. Формально: a_B в обох формулах однакове (тримаємо це сталим).

Розглянемо дві альтернативні стратегії агента А: базову a^0_A та альтернативну a_A.

Визначимо маржинальний ефект для двох стратегій агента A, a_A та a^0_B. Маржинальний ефект зміни стратегії агента A визначається як різниця значень цільових функціоналів при незмінній стратегії агента B, а саме:

$$\Delta_A\left[a_A; a^0_A | a_B\right]: = J_A(a_A, a_B) - J_A(a^0_A, a_B), \quad (9)$$

$$\Delta_B\left[a_A; a^0_A | a_B\right]: = J_B(a_A, a_B) - J_B(a^0_A, a_B), \quad (10)$$

де a_A *і* a^0_A – повні стратегії агента A (керування на всьому часовому інтервалі); $J_A(\cdot,\cdot)$, $J_B(\cdot,\cdot)$ – цільові функціонали агентів A та B; Δ_A – маржинальний позитив для агента A, тобто зміна його цільового функціонала при переході від a^0_A до a_A; Δ_B – маржинальний ефект для агента B від тієї самої зміни дій (стратегії) агента A.

Таким чином, Δ_A та Δ_B кількісно описують вплив однієї й тієї самої дії a^0_A на цілі різних агентів.

У випадку антагоністичної гри з нульовою сумою, де $J_B = -J_A$, безпосередньо випливає: $\Delta_B = -\Delta_A$, тобто будь-яке покращення позиції агента A є симетричним погіршенням позиції агента B.

Інтерпретація.

Якщо $\Delta_A>0$, перехід від a^0_A до a_A є вигідним для агента A (інтерпретується як захід безпеки з його точки зору).

Одночасно $\Delta_B<0$, тобто та сама дія є шкідливою для агента B (інтерпретується як загроза з його точки зору).

Це формалізує дуальність інтерпретації дій у симетричних антагоністичних системах. Графічну інтерпретацію маржинального ефекту від дії агенту A (дуальність вигід і втрат) наведено на рисунку 5.

Рисунок наочно демонструє, що одна й та сама зміна стратегії породжує протилежні за знаком маржинальні ефекти для різних агентів, тобто реляційний характер інтерпретації дій як «загрози» або «заходу безпеки». Тобто дія сама по собі не є ні «хорошою», ні «поганою» – її значення залежить від того, з чиєї точки зору її оцінюють.

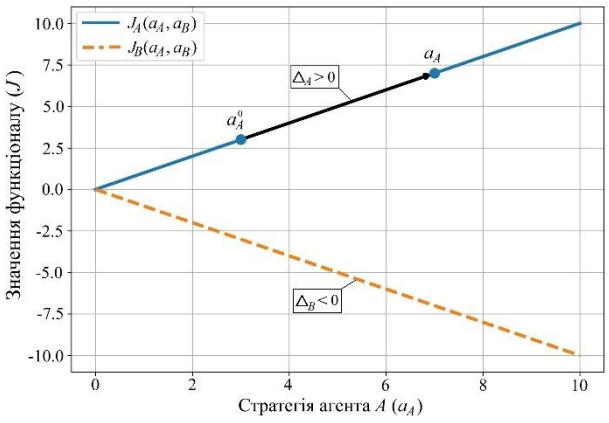

Рис. 5. Маржинальний ефект від дії агента А (дуальність вигід і втрат) за фіксованої стратегії агента В

4. Теорема дослідження.

Нехай система (4, 5) керується відповідно до функціоналів (6, 7). Тоді для будь-яких стратегій a_A, a^0_A та будь-якої фіксованої стратегії a_B виконується тотожність:

$$\Delta_B\left[a_A; a_A^0 | a_B\right] = -\Delta_A\left[a_A; a_A^0 | a_B\right], \quad (11)$$

Доведення.

Із означення нульової суми (7) маємо:

$$\begin{aligned} & J_B(a_A, a_B) \\ & = -J_A(a_A, a_B) \; \forall a_A, a_B \in \mathrm{K}, \end{aligned} \quad (12)$$

Тоді, застосовуючи це до обох доданків у визначенні (10) маємо:

$$\begin{aligned} \Delta_B &= J_B(a_A, a_B) - J_B(a_A^0, a_B) \\ &= (-J_A(a_A, a_B)) - (-J_A(a_A^0, a_B)) \\ &= -(J_A(a_A, a_B)) - J_A(a_A^0, a_B)) \\ &= -\Delta_A \end{aligned} \quad (13)$$

Доведення є елементарним і не вимагає:

– симетрії функції шкоди чи початкових умов;

– існування єдності/рівноваги;

– регулярності функції цінності;

– інших додаткових припущень.

Отримана симетрія маржинальних ефектів означає, що з позицій ймовірнісного аналізу відсутні підстави застосовувати різні класи методів до оцінювання загроз і заходів безпеки; відмінність між ними визначається не математичною природою подій, а знаком впливу на цільовий функціонал системи.

Отримана ілюстративна тотожність $\Delta_B = -\Delta_A$ у грі з нульовою сумою демонструє, що знак ефекту дії визначається цільовою функцією спостерігача, тоді як модуль ефекту є інваріантним.

5. Твердження, які випливають з доведеної теореми:

Твердження 1. Для будь-якої зміни (дії) від від a^0_A до a_A виконується:

$$sing(\Delta_B) = -sing(\Delta_A), \quad (14)$$

Доведено застосуванням знакової функції до обох частин (11).

Інтерпретація: Одна і та сама дія a_A є:

– заходом безпеки для A (якщо $\Delta_A>0$);

– небезпекою для B ($\Delta_B= -\Delta_A <0$), одночасно, в одному і тому ж самому часовому зрізі, що підтверджує гіпотезу.

Твердження 2. Для будь-якої зміни (дії) виконується:

$$\left|\Delta_A\right| = \left|\Delta_B\right|, \quad (15)$$

Це означає, що дія має єдину кількісну природу впливу, а відмінність полягає виключно в знаку, що визначається цілями спостерігача.

Твердження 3. У грі з нульовою сумою виконується інваріант нульової суми:

$$\begin{aligned} & \Delta_A\left[a_A; a_A^0 | a_B\right] + \\ & +\Delta_B\left[a_A; a_A^0 | a_B\right] = 0, \end{aligned} \quad (16)$$

Доводиться переформулюванням (11).

Інтерпретація: Сума впливів на цілі обох агентів дорівнює нулю. Будь-який позитивний наслідок для одого агента є тотожнім негативним наслідком для іншого.

Отже, гіпотеза знайшла математичне підтвердження.

Доведено:

– дуальність інтерпретацій «небезпека-захід безпеки» є математичною необхідністю;

– небезпеки та заходи не є онтологічно різними сутностями, вони є реляційними інтерпретаціями одного й того ж самого стохастичного впливу;

– критерієм класифікації тут є знак впливу на цільовий функціонал спостерігача;

– кількісна величина впливу є інваріантною відносно спостерігача.

Практичне застосування доказу.

Результати доказу мають значення для:

– загальної теорії безпеки та при оновленні стандартів ризик-менеджменту. Формалізаця (аналіз) відносності категорій «небезпека»/«загроза» та «захід». Розуміння атак і захисту як дуальних явищ. Аналіз взаємодії «атакувальних» і «захисних» контурів у кіберфізичних системах КІ; для обґрунтування вимог до прогнозного оцінювання результативності бар'єрів (заходів) безпеки та їх деградації;

– аналізу конфліктів. Математичне обґрунтування симетрії сприйняття;

– оптимізації процесів прийняття рішень. Врахування множинних перспектив при оцінці дії.

З огляду на вище викладене, повертаючись до обговорення моделей ймовірнісної оцінки заходів безпеки, можливо стверджувати, що у їх якості слід застосовувати існуючі і нові методи ймовірнісної оцінки небезпек, лише коригуючи мету розрахунку.

З метою якісного оброблення ризику згідно вимог цільової рамки (рис. 3), встановлення рівня безпеки, через відносне зіставлення отриманих значень оцінки ризику і оцінки ефективності заходів безпеки, пропонуємо використовувати принцип адекватності ймовірностей [15].

Застосування цього принципу забезпечує усунення методологічної асиметрії між оцінюванням загроз і оцінюванням заходів безпеки, оскільки вимагає узгодженого ймовірнісного опису обох типів подій у межах єдиного контуру ризик-менеджменту.

Практичне значення дослідження.

Отримані у ході дослідження результати можуть бути використані для вдосконалення практики ризик-орієнтованого управління безпекою критичної інфраструктури шляхом включення прогнозного ймовірнісного оцінювання ефективності заходів безпеки.

Запропонований принцип адекватності ймовірностей може застосовуватися як метакритерій перевірки валідності рішень щодо вибору та пріоритезації контрзаходів, а також при розробленні галузевих і об’єктово-орієнтованих методик оцінювання безпеки КІ.

Обмеження дослідження. Дослідження має концептуально-методологічний характер і не включає емпіричної валідації запропонованих положень на основі статистичних даних експлуатації конкретних об’єктів КІ. Формалізація ймовірнісної моделі результативності заходів безпеки здійснювалася у спрощеній постановці та потребує подальшого уточнення для складних багатокомпонентних і міжсекторальних систем.

Перспективи подальшого дослідження полягають:

– у розробленні прикладних ймовірнісних моделей оцінювання ефективності заходів безпеки;

– у розробленні об’єктно-орієнтованих методик ймовірнісного аналізу і прогнозного оцінювання ефективності заходів безпеки.

Висновки

1. У роботі на основі нормативно-структурного та логіко-структурного аналізу міжнародних стандартів і національних регуляторних вимог показано, що чинний ризик-орієнтований підхід до виробничої безпеки і безпеки критичної інфраструктури має системні методологічні обмеження.

2. Встановлено, що ключовим обмеженням чинного підходу є асиметрія ймовірностей: ймовірність реалізації загроз оцінюється, тоді як ймовірність досягнення запланованого ефекту заходів безпеки не є обов’язковим елементом ризик-оцінювання.

3. Показано, що зазначена асиметрія призводить до систематичного заниження оцінки залишкового ризику та формування ілюзії керованості безпеки, особливо в умовах деградації бар’єрів (заходів), призводить до каскадності і динаміки загроз.

4. Запропоновано принцип адекватності ймовірностей як метакритерій валідності ризик-орієнтованого підходу, відповідно до якого оцінювання ризику є методологічно коректним лише за умови узгодженого врахування ймовірностей сценаріїв загроз та результативності заходів безпеки.

5. За допомогою антагоністичної стохастичної постановки (моделі) обґрунтовано, що ймовірнісна природа загроз і заходів безпеки є ізоморфною, а відмінність між ними визначається виключно знаком впливу на цільовий функціонал системи та позицією спостерігача.

6. Синтезовано цільовий контур ризик-менеджменту КІ, який включає прогнозне оцінювання ефективності заходів, урахування їх деградації та багаторівневий моніторинг, що підвищує керованість питань виробничої безпеки та безпеки критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO 31073:2022. Risk management. Vocabulary. Geneva : International Organization for Standardization, 2022. 15 p.

2. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). Київ : ДП «УкрНДНЦ», 2018. 23 с.

3. ДСТУ EN IEC 31010:2022. Керування ризиками. Методи оцінки ризиків (EN IEC 31010:2019, IDT ; IEC 31010:2019, IDT). Київ : ДП «УкрНДНЦ», 2022. 94 с.

4. ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT). Київ : ДП «УкрНДНЦ», 2021. 26 с.

5. ДСТУ EN ISO 14090:2022. Адаптація до змін клімату. Принципи, вимоги та настанови (EN ISO 14090:2019, IDT; ISO 14090:2019, IDT). Київ : ДП «УкрНДНЦ», 2022. 48 с.

6. ДСТУ ISO 55001:2019. Управління активами. Системи управління. Вимоги (ISO 55001:2014, IDT). Київ : ДП «УкрНДНЦ», 2019. 58 с.

7. ДСТУ 2293:2014. Охорона праці. Терміни та визначення основних понять. Київ : ДП «УкрНДНЦ», 2015. 17 с.

8. PwC. Global Digital Trust Insights 2026. 2025. URL: https://www.pwc.es/es/publicaciones/digital/global-digital-trust-insights-2026.pdf (дата звернення: 17.01.2026).

9. The Hacker News. Security Theater: Vanity Metrics Keep You Busy – and Exposed [Електронний ресурс]. 2025. URL: https://thehackernews.com/2025/04/security-theater-vanity-metrics-keep.html (дата звернення: 17.01.2026).

10. SAFE Security. Measuring Cybersecurity ROI: A Framework for 2026 Decision-Makers [Електронний ресурс]. 2025. URL: https://safe.security/resources/blog/measuring-cybersecurity-roi-a-framework-for-2026-decision-makers/ (дата звернення: 17.01.2026).

11. Gartner. Gartner Identifies the Top Cybersecurity Trends for 2025 [Електронний ресурс]. 2025. URL: https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025 (дата звернення: 17.01.2026).

12. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX (зі змінами, внесеними Законом України від 22.08.2024 № 3931-IX). *Відомості Верховної Ради України*. 2023. № 5. Ст. 13 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 19.01.2026).

13. Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності : постанова Кабінету Міністрів України від 01.04.2025 № 367 : станом на 19.01.2026 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text (дата звернення: 19.01.2026).

14. ДСТУ EN IEC 31010:2013. Керування ризиками. Методи оцінки ризиків (EN IEC 31010:2013, IDT ; IEC 31010:2013, IDT). Київ : ДП «УкрНДНЦ», 2015. 94 с.

15. Matsuk Z., Belikov A., Slashchova O., Digtyar K., Ikonnikov M. Safety theory. The principle of probability adequacy in the methodology of risk management of infrastructure systems stability : plenary presentation. *Proceedings of the VII International Conference "Essays on Mining Science and Practice"*. November 5–7, 2024. Dnipro, Ukraine [Електронний ресурс]. URL: https://www.rmget.com/index.php/keynote-lectures.html (дата звернення: 25.01.2026).

REFERENCES

1. ISO 31073:2022. Risk management. Vocabulary. Geneva : International Organization for Standardization, 2022. 15 p.

2. *DSTU ISO 31000:2018. Menedzhment ryzykiv. Pryntsypy ta nastanovy (ISO 31000:2018, IDT)* [DSTU ISO 31000:2018. Risk management. Principles and guidelines (ISO 31000:2018, IDT)]. Kyiv : SE "UkrNDNTS", 2018, 23 p. (in Ukrainian).

3. *DSTU EN IEC 31010:2022. Keruvannya ryzykamy. Metody otsinky ryzykiv (EN IEC 31010:2019, IDT; IEC 31010:2019, IDT)* [DSTU EN IEC 31010:2022. Risk management. Risk assessment methods (EN IEC 31010:2019, IDT; IEC 31010:2019, IDT)]. Kyiv : SE "UkrNDNTS", 2022, 94 p. (in Ukrainian).

4. *DSTU EN ISO 22301:2021. Bezpeka ta stabil'nist'. Systemy upravlinnya neperervnistyu biznesu. Vymohy (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT)* [DSTU EN ISO 22301:2021. Security and stability. Business continuity management systems. Requirements (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT)]. Kyiv : SE "UkrNDNTS", 2021, 26 p. (in Ukrainian).

5. *DSTU EN ISO 14090:2022. Adaptatsiya do zmin klimatu. Pryntsypy, vymohy ta nastanovy (EN ISO 14090:2019, IDT; ISO 14090:2019, IDT)* [DSTU EN ISO 14090:2022. Adaptation to climate change. Principles, requirements and guidelines (EN ISO 14090:2019, IDT; ISO 14090:2019, IDT)]. Kyiv : SE "UkrNDNTS", 2022, 48 p. (in Ukrainian).

6. *DSTU ISO 55001:2019. Upravlinnya aktyvamy. Systemy upravlinnya. Vymohy (ISO 55001:2014, IDT)* [DSTU ISO 55001:2019. Asset management. Management systems. Requirements (ISO 55001:2014, IDT)]. Kyiv : SE "UkrNDNTS", 2019, 58 p. (in Ukrainian).

7. *DSTU 2293:2014. Okhorona pratsi. Terminy ta vyznachennya osnovnykh ponyat'* [DSTU 2293:2014. Occupational health and safety. Terms and definitions of basic concepts]. Kyyiv : SE “UkrNDNTS”, 2015, 17 p. (in Ukrainian).

8. PwC. (2025). Global digital trust insights 2026. URL: https://www.pwc.es/es/publicaciones/digital/global-digital-trust-insights-2026.pdf

9. The Hacker News. (2025). Security theater : Vanity metrics keep you busy – and exposed. URL: https://thehackernews.com/2025/04/security-theater-vanity-metrics-keep.html

10. SAFE Security. (2025). Measuring cybersecurity ROI : A framework for 2026 decision-makers. URL: https://safe.security/resources/blog/measuring-cybersecurity-roi-a-framework-for-2026-decision-makers/

11. Gartner. (2025, March 3). Gartner identifies the top cybersecurity trends for 2025. URL: https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025

12. *Zakon Ukrayiny “Pro krytychnu infrastrukturu” vid 16.11.2021 № 1882-IX (zi zminamy, vnesenymy Zakonom Ukrayiny vid 22.08.2024 № 3931-IX)* [Law of Ukraine “On Critical Infrastructure” dated 16.11.2021 No. 1882-IX (as amended by the Law of Ukraine dated 22.08.2024 No. 3931-IX)]. *Vidomosti Verkhovnoyi Rady Ukrayiny* [Bulletin of the Verkhovna Rada of Ukraine]. 2023, no. 5. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (date of access : 19.01.2026). (in Ukrainian).

13 *Pro zatverdzhennya vymoh shchodo upravlinnya ryzykamy bezpeky na ob"yektakh krytychnoyi infrastruktury I katehoriyi krytychnosti : postanova Kabinetu Ministriv Ukrayiny vid 01.04.2025 № 367 : stanom na 19.01.2026* [On approval of requirements for security risk management at critical infrastructure facilities of category I criticality: resolution of the Cabinet of Ministers of Ukraine dated 01.04.2025 No. 367: as of 19.01.2026]. URL: https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text (in Ukrainian).

14. *DSTU EN IEC 31010:2013. Keruvannya ryzykamy. Metody otsinky ryzykiv (EN IEC 31010:2013, IDT ; IEC 31010:2013, IDT)* [DSTU EN IEC 31010:2013. Risk management. Risk assessment methods (EN IEC 31010:2013, IDT; IEC 31010:2013, IDT)]. Kyiv : State Enterprise “UkrNDNTs”, 2015, 94 p. (in Ukrainian).

15. Matsuk Z., Belikov A., Slashchova O., Digtyar K. and Ikonnikov M. Safety theory. The principle of probability adequacy in the methodology of risk management of infrastructure systems stability [Plenary presentation]. In Proceedings of the VII International Conference “Essays on Mining Science and Practice”. November 5–7, 2024, Dnipro, Ukraine. URL: https://www.rmget.com/index.php/keynote-lectures.html

Надійшла до редакції: 01.03.2026.
Прийнято після рецензування: 01.05.2026.
Дата публікації: 29.05.2026.