УДК 004.056:005.334 DOI: 10.31673/2409-7292.2026.027509

Легомінова Світлана Володимирівна
доктор економічних наук, професор, завідувач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-4433-5123
E-mail: s.legominova@duikt.edu.ua

Примаченко Діана Володимирівна
асистент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0003-2386-7440
E-mail: primachenko.dv@duikt.ua

МЕТОД ОЦІНЮВАННЯ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З УРАХУВАННЯМ ГІБРИДНОГО ВПЛИВУ

У статті розглянуто задачу оцінювання ризику інформаційної безпеки в умовах гібридного впливу, що поєднує технічні, організаційні та інформаційно-психологічні чинники. Обґрунтовано, що використання традиційної оцінки ризику без урахування специфіки гібридного контексту може призводити до недостатньо точного визначення пріоритетності загроз, оскільки різні категорії активів мають неоднакову чутливість до окремих каналів впливу. Запропоновано метод оцінювання ризику інформаційної безпеки, у якому базовий індекс ризику коригується з урахуванням індексу гібридного впливу. Індекс гібридного впливу формується на основі технічної, організаційної та психологічної складових із використанням модифікованого зваженого геометричного агрегування. Для визначення вагових коефіцієнтів складових гібридного впливу запропоновано застосовувати метод аналізу ієрархій з урахуванням категорії активу. Додатково введено коефіцієнт сценарного посилення ризику, що дозволяє оцінювати зміну ризику за консервативним, базовим та критичним сценаріями гібридного тиску. Наведено приклад застосування запропонованого методу для типових категорій активів і сценаріїв загроз. Отримані результати підтверджують, що запропонований підхід дозволяє уникнути спрощеного усереднення різнорідних чинників гібридного впливу, врахувати специфіку активів та виконати сценарне ранжування ризиків інформаційної безпеки. Доведено практичне значення запропонованого методу щодо попереднього кількісного оцінювання ризиків, порівняння сценаріїв гібридного впливу, визначення пріоритетності захисних заходів та обґрунтування управлінських рішень щодо підвищення стійкості організації.

Ключові слова: кібербезпека, інформаційна безпека; кіберризик, гібридний вплив; гібридні загрози; ризик-орієнтований підхід; метод аналізу ієрархій.

Вступ та формулювання проблеми

Функціонування організацій в умовах гібридної війни супроводжується підвищенням інтенсивності інформаційних, кібернетичних, організаційних та психологічних впливів, які можуть безпосередньо або опосередковано змінювати рівень ризику інформаційної безпеки. За таких умов загроза не завжди реалізується лише через технічну вразливість інформаційної системи. Її результативність може залежати від організаційної нестабільності, перевантаження персоналу, порушення процедур управління доступом, зниження уважності працівників, дезінформаційного тиску або використання соціально чутливої тематики в соціоінженерних атаках.

Традиційні підходи до оцінювання ризику інформаційної безпеки переважно ґрунтуються на поєднанні параметрів імовірності реалізації загрози, рівня вразливості, потенційного збитку та результативності заходів захисту. Такі підходи залишаються методично доцільними, однак у контексті гібридної війни вони потребують уточнення, оскільки не завжди відображають багатоканальний характер впливу на активи організації. Один і той самий сценарій загрози може мати різний рівень значущості для різних категорій активів: технічний вплив є більш критичним для серверної інфраструктури, психологічний – для персоналу, організаційний – для управлінських і бізнес-процесів.

Окремою проблемою є спосіб агрегування технічної, організаційної та психологічної складових гібридного впливу. Використання середнього арифметичного для формування узагальненого коефіцієнта є простим, проте методично обмеженим, оскільки передбачає

однакову значущість усіх складових і може занижувати оцінку в тих випадках, коли загроза реалізується переважно через один домінуючий канал. Наприклад, атака з високим технічним компонентом не повинна отримувати знижену оцінку лише через відсутність вираженого психологічного впливу. Водночас повністю індивідуалізоване визначення ваг для кожної загрози ускладнює практичне застосування моделі та підвищує залежність результатів від експертних припущень.

Проблема дослідження полягає у необхідності розроблення методу оцінювання ризику інформаційної безпеки, який дозволяє врахувати гібридний вплив без надмірного ускладнення розрахунків, забезпечити диференціацію технічного, організаційного та психологічного каналів впливу, а також адаптувати оцінку до специфіки різних категорій активів. Вирішення цієї проблеми має значення для підвищення обґрунтованості ранжування ризиків та підтримки прийняття управлінських рішень у сфері інформаційної безпеки.

Аналіз літературних джерел

Проблематика оцінювання ризиків інформаційної безпеки та кібербезпеки розглядається в наукових працях, присвячених ризик-орієнтованому управлінню, математичному моделюванню загроз, кількісному аналізу вразливостей, індикаторним моделям безпеки та забезпеченню кіберстійкості організацій. У дослідженнях Аузіної, Волкової, Норена-Чавеса, Кадлубека та Талассіноса [1] акцентовано увагу на управлінських підходах до реагування на кіберінциденти та підвищення кіберзрілості організацій, що є важливим для формування ризик-орієнтованої моделі прийняття рішень. Робота Берка, Висоцької та Рішняка [2] зосереджена на методах оцінювання ризиків безпеки інформації, зокрема на формалізації взаємозв’язку між загрозами, вразливостями та можливими наслідками.

Індикаторний підхід до оцінювання рівня цифровізації та кібербезпеки розглянуто у праці Барченко, Любчак і Лаврик [3], де запропоновано використання системи показників для аналізу стану безпеки. Такий підхід є важливим для формування вхідних параметрів оцінювання ризику, однак потребує адаптації до ситуацій, у яких ризик формується не лише технічними, а й організаційними та поведінковими чинниками. Дзюба і Чмир [4] обґрунтовують доцільність використання методів математичної статистики для оцінювання ризиків інформаційної безпеки, що підтверджує актуальність кількісного підходу до аналізу ризикових ситуацій.

Для дослідження складних ризикових систем також важливими є роботи, у яких використовуються причинно-наслідкові та ймовірнісні моделі. Зокрема, Хакзад, Хан і Аміотт [5] порівнюють підходи на основі дерев відмов і байєсівських мереж, що демонструє значущість структурного моделювання взаємозв’язків між чинниками ризику. У контексті інформаційної безпеки такі підходи підтверджують необхідність врахування не лише окремих параметрів загрози, а й взаємозалежності умов, у яких вона реалізується. Гловацький [6] розглядає методи оцінювання стану безпеки та загроз інформаційних ресурсів, що є дотичним до задачі визначення базових параметрів ризику.

У документах OECD [7] кібербезпека розглядається як складова економічної безпеки та організаційної стійкості, що особливо важливо для досліджень, пов’язаних із гібридними загрозами. Аналітичні матеріали PwC [8] наголошують на необхідності залучення керівництва до управління кіберризиками та інтеграції кібербезпеки в систему корпоративного управління. Савельєва, Панасько та Пригодюк [9] розглядають особливості впровадження ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства, що формує прикладну основу для подальшого розвитку методів оцінювання ризику.

Узагальнення наукових джерел дозволяє зробити висновок, що існуючі підходи створюють необхідну базу для оцінювання ризиків інформаційної безпеки, однак недостатньо деталізують питання врахування гібридного впливу як багатоканального чинника, що по-різному проявляється для різних категорій активів. Недостатньо розробленим залишається питання агрегування технічної, організаційної та психологічної складових гібридного впливу

© Легомінова С.В., Примаченко Д.В. Метод оцінювання ризику інформаційної безпеки з урахуванням гібридного впливу. Сучасний захист інформації, 2(66), 106–115.
https://doi.org/10.31673/2409-7292.2026.027509

без їх штучного усереднення та без надмірного ускладнення моделі. Це обґрунтовує доцільність розроблення методу, який поєднує базову оцінку ризику, зважене агрегування складових гібридного впливу та сценарне коригування результату.

Мета та постановка задачі

Метою статті є розроблення методу оцінювання ризику інформаційної безпеки організації з урахуванням гібридного впливу шляхом поєднання базового індексу ризику, зваженого агрегування технічної, організаційної та психологічної складових і сценарного коригування результату залежно від рівня гібридного тиску.

Для досягнення поставленої мети необхідно вирішити такі завдання: обґрунтувати доцільність урахування гібридного впливу під час оцінювання ризиків інформаційної безпеки; визначити технічну, організаційну та психологічну складові гібридного впливу; запропонувати спосіб їх агрегування з урахуванням категорії активу; обґрунтувати застосування методу аналізу ієрархій для визначення вагових коефіцієнтів складових гібридного впливу; ввести сценарний коефіцієнт посилення ризику; продемонструвати застосування запропонованого методу на умовному прикладі оцінювання ризиків для типових категорій активів і сценаріїв загроз.

Основна частина

Оцінювання ризику інформаційної безпеки в умовах гібридної війни потребує врахування не лише базових параметрів загрози, вразливості, рівня захищеності та потенційного збитку, а й специфічного контексту, у межах якого реалізується загроза. Такий контекст може посилювати ризик через одночасний або частково пов'язаний вплив технічних, організаційних та психологічних чинників. При цьому використання єдиного узагальненого коефіцієнта гібридної загрози без урахування типу активу може призводити до спрощеного представлення ризику, оскільки різні категорії активів мають неоднакову чутливість до окремих каналів гібридного впливу.

У межах запропонованого підходу базове значення ризику доцільно розглядати як інтегральний індекс, що визначається через потенційний збиток, імовірність реалізації загрози, рівень вразливості та рівень захищеності активу:

$$RI_0 = D \cdot P \cdot V \cdot (1 - Z), \tag{1}$$

де RI_0 – базовий індекс ризику інформаційної безпеки; D – рівень потенційного збитку в разі реалізації загрози; P – імовірність реалізації загрози; V – рівень вразливості активу щодо відповідної загрози; Z – рівень захищеності активу.

Значення параметрів D, P, V та Z доцільно нормувати в межах інтервалу [0;1], де 0 відповідає мінімальному, а 1 – максимальному рівню відповідного параметра. Водночас отримане значення RI_0 у подальших розрахунках інтерпретується не як імовірність інциденту, а як відносний індекс ризику, призначений для порівняння та ранжування ризиків. Такий підхід є важливим, оскільки після врахування гібридного впливу скориговане значення ризику може перевищувати 1, що є неприпустимим для ймовірності, але допустимим для індексної оцінки.

Для врахування умов гібридної війни вводиться індекс гібридного впливу H, який відображає ступінь посилення ризику через технічний, організаційний та психологічний канали. Відповідні складові позначаються як: H_T – рівень технічного впливу, H_O – рівень організаційного впливу, H_P – рівень психологічного або інформаційно-психологічного впливу.

Кожна із зазначених складових оцінюється в межах інтервалу [0;1]. Значення H_T, H_O та H_P визначаються для конкретної загрози або сценарію її реалізації. Наприклад, для DDoS-атаки домінуючим буде технічний канал впливу, для фішингової атаки із використанням воєнної або соціально чутливої тематики – психологічний канал, а для інцидентів, пов'язаних із порушенням процедур доступу в умовах кадрової перевантаженості – організаційний канал.

Пропонується використовувати зважене геометричне агрегування. Застосування середнього арифметичного передбачає однакову значущість усіх складових та може штучно занижувати оцінку гібридного впливу у випадках, коли загроза реалізується переважно через один домінуючий канал. Наприклад, технічно інтенсивна атака не повинна отримувати низьку оцінку лише через відсутність вираженої психологічної складової.

Разом із тим класичне геометричне агрегування у вигляді:

$$H = H_T^{\omega_T} \cdot H_O^{\omega_O} \cdot H_P^{\omega_P}, \quad (2)$$

також має суттєве обмеження, оскільки за нульового значення хоча б однієї складової загальний індекс набуває нульового значення. Це не відповідає логіці оцінювання гібридного впливу, оскільки відсутність одного каналу впливу не означає відсутності ризику або його гібридного посилення через інші канали.

З огляду на це пропонується використовувати модифіковану форму зваженого геометричного агрегування:

$$H = (1 + H_T)^{\omega_T} \cdot (1 + H_O)^{\omega_O} \cdot (1 + H_P)^{\omega_P} - 1, \quad (3)$$

де H – інтегральний індекс гібридного впливу; ω_T, ω_O, ω_P – вагові коефіцієнти технічного, організаційного та психологічного каналів відповідно. Вагові коефіцієнти мають задовольняти умову: $\omega_T + \omega_O + \omega_P = 1$.

Запропонована форма агрегування має кілька методичних переваг. По-перше, нульове значення однієї зі складових не обнуляє загальний індекс гібридного впливу. По-друге, внесок кожного каналу залежить не лише від його поточного рівня для конкретної загрози, а й від значущості цього каналу для відповідної категорії активу. По-третє, індекс H залишається нормованим у межах [0;1], якщо значення H_T, H_O, H_P належать інтервалу [0;1], а сума вагових коефіцієнтів дорівнює 1.

Вагові коефіцієнти ω_T, ω_O, ω_P доцільно визначати не для кожної окремої загрози, а для категорії активів. Це дозволяє уникнути надмірної деталізації моделі та забезпечує її практичну застосовність. Категорія активу визначає чутливість активу до відповідного каналу гібридного впливу, тоді як конкретна загроза визначає поточні значення H_T, H_O, H_P.

Отже, у моделі реалізується така логіка: категорія активу – ω_T, ω_O, ω_P, загроза або сценарій – H_T, H_O, H_P.

Для визначення вагових коефіцієнтів може бути використаний метод аналізу ієрархій, що дозволяє формалізувати експертні судження щодо відносної значущості технічного, організаційного та психологічного каналів гібридного впливу для певної категорії активів. Експертна оцінка в такому разі здійснюється не щодо загального рівня ризику, а щодо порівняльної важливості каналів впливу. Це зменшує суб'єктивність порівняно з прямим призначенням підсумкового коефіцієнта ризику.

У спрощеному вигляді категорії активів можуть бути подані таким чином: серверна та мережева інфраструктура; бази даних та інформаційні ресурси; персонал; управлінські та бізнес-процеси; публічні веб-ресурси й комунікаційні канали. Для кожної з цих категорій визначається власна система ваг. Наприклад, для серверної інфраструктури більшу вагу може мати технічний канал, для персоналу – психологічний, а для управлінських процесів – організаційний.

Скоригований індекс ризику з урахуванням гібридного впливу визначається за формулою:

$$RI_{hyb} = RI_0 \cdot (1 + \lambda H), \quad (4)$$

де RI_{hyb} – індекс ризику з урахуванням гібридного впливу; RI_0 – базовий індекс ризику; H – індекс гібридного впливу; λ – коефіцієнт сценарного посилення ризику.

Коефіцієнт λ не є ваговим коефіцієнтом технічного, організаційного чи психологічного каналу. Його призначення полягає у визначенні загального масштабу впливу гібридного

© Легомінова С.В., Примаченко Д.В. Метод оцінювання ризику інформаційної безпеки з урахуванням гібридного впливу. Сучасний захист інформації, 2(66), 106–115.
https://doi.org/10.31673/2409-7292.2026.027509

контексту на базовий ризик. Іншими словами, вагові коефіцієнти ω_T, ω_O, ω_P, відповідають на питання, який канал впливу є більш значущим для певної категорії активу, тоді як λ визначає, наскільки сильно умови гібридної війни можуть посилити базову оцінку ризику.

Оскільки точне статистичне визначення λ потребує репрезентативних даних щодо інцидентів інформаційної безпеки організації в умовах гібридної війни, які не завжди є доступними, у межах запропонованої методики доцільно використовувати сценарний підхід. Для цього можуть бути задані три рівні сценарного посилення: $\lambda = 0{,}25$ – консервативний сценарій, $\lambda = 0{,}5$ – базовий сценарій, $\lambda = 1{,}0$ – критичний сценарій.

Консервативний сценарій відповідає умовам, за яких організація функціонує відносно стабільно, а гібридний контекст розглядається як додатковий, але не домінуючий чинник посилення ризику. Базовий сценарій відображає ситуацію підвищеного гібридного тиску, коли зростає інтенсивність кібератак, навантаження на персонал, частота соціоінженерних впливів та організаційних порушень. Критичний сценарій застосовується для умов, за яких гібридний вплив має системний характер і може суттєво змінювати рівень ризику для активів організації.

Таким чином, для кожного ризику можуть бути отримані три скориговані оцінки: $RI_{0.25} = RI_0 \cdot (1 + 0.25H)$, $RI_{0.5} = RI_0 \cdot (1 + 0.5H)$, $RI_{1.0} = RI_0 \cdot (1 + H)$.

Використання декількох сценаріїв дозволяє не фіксувати одне універсальне значення коефіцієнта λ, а оцінити чутливість ризику до зміни рівня гібридного тиску. Якщо певний ризик залишається високим навіть за консервативного сценарію, його можна розглядати як стійко значущий. Якщо ж ризик істотно зростає лише за критичного сценарію, це свідчить про його залежність від загального рівня гібридного впливу на організацію.

Загальна послідовність застосування запропонованої методики передбачає такі етапи. Спочатку визначаються категорії активів, для яких здійснюється оцінювання ризику. Далі для кожної категорії активів за допомогою методу аналізу ієрархій визначаються вагові коефіцієнти технічного, організаційного та психологічного каналів гібридного впливу. Після цього формується перелік загроз або сценаріїв, для яких задаються значення H_T, H_O, H_P. На наступному етапі розраховується базовий індекс ризику RI_0, індекс гібридного впливу H та скориговані значення ризику для заданих сценаріїв λ. Завершальним етапом є порівняння отриманих значень і визначення ризиків, найбільш чутливих до умов гібридної війни.

Для демонстрації практичного застосування запропонованої методики розглянемо умовний приклад оцінювання ризиків інформаційної безпеки для декількох категорій активів організації. Приклад має ілюстративний характер і призначений для перевірки логіки розрахунку, порівняння сценаріїв гібридного впливу та визначення ризиків, чутливих до умов гібридної війни. У межах прикладу виділено п’ять категорій активів: серверна інфраструктура, бази даних, персонал, управлінські процеси та публічні веб-ресурси. Для кожної категорії активів визначаються вагові коефіцієнти технічного, організаційного та психологічного каналів гібридного впливу. Ваги відображають не рівень поточної загрози, а чутливість відповідної категорії активів до певного каналу впливу. Умовні значення вагових коефіцієнтів наведено в табл. 1.

Таблиця 1

Вагові коефіцієнти каналів гібридного впливу для категорій активів

Категорія активів	ω_T	ω_O	ω_P
Серверна інфраструктура	0,65	0,25	0,10
Бази даних	0,50	0,35	0,15
Персонал	0,20	0,25	0,55
Управлінські процеси	0,20	0,55	0,25
Публічні веб-ресурси	0,60	0,15	0,25

Наведені значення відповідають логіці диференційованої чутливості активів. Для серверної інфраструктури домінуючим є технічний канал, оскільки основні ризики для такої

категорії активів пов’язані з експлуатацією технічних вразливостей, порушенням доступності, несанкціонованим втручанням у роботу обладнання або сервісів. Для персоналу найвищу вагу має психологічний канал, оскільки працівники є основною ціллю соціоінженерних, фішингових та інформаційно-психологічних впливів. Для управлінських процесів пріоритетним є організаційний канал, оскільки порушення процедур, неузгодженість повноважень, дефіцит відповідальних осіб або робота в аварійному режимі безпосередньо впливають на здатність організації реагувати на інциденти.

На наступному етапі формується перелік загроз або сценаріїв, для яких визначаються рівні технічного, організаційного та психологічного впливу. У прикладі розглянуто п’ять типових сценаріїв, характерних для організацій, що функціонують в умовах підвищеного кібернетичного та інформаційного тиску.

Таблиця 2

Значення складових гібридного впливу для окремих сценаріїв загроз

Сценарій загрози	H_T	H_O	H_P
DDoS-атака на критичний сервіс	0,90	0,20	0,10
Фішингова атака з використанням воєнної тематики	0,40	0,30	0,90
Компрометація облікових записів	0,70	0,50	0,60
Порушення процедур доступу в умовах кадрової перевантаженості	0,30	0,80	0,40
Дезінформаційна атака щодо діяльності організації	0,20	0,30	0,90

Значення, наведені в табл. 2, задаються за шкалою від 0 до 1. Вони характеризують не загальний рівень ризику, а профіль гібридного впливу конкретного сценарію. Наприклад, DDoS-атака має високий технічний компонент, але відносно низький психологічний компонент. Фішингова атака з використанням воєнної тематики має виражений психологічний компонент, оскільки ефективність такого впливу значною мірою пов’язана з емоційним станом, довірою до повідомлення, тривожністю та актуальністю тематики для працівника. Порушення процедур доступу в умовах кадрової перевантаженості має домінуючий організаційний компонент, оскільки основним джерелом підвищення ризику є не окрема технічна вразливість, а нестабільність процесів управління доступом.

Для кожної пари “категорія активів – сценарій загрози” індекс гібридного впливу визначається за формулою 3. Наприклад, для категорії “персонал” та сценарію фішингової атаки з використанням воєнної тематики вагові коефіцієнти становлять: ω_T=0,20; ω_O=0,25; ω_P=0,55.

Значення складових гібридного впливу для відповідного сценарію: H_T=0,40; H_O=0,30; H_P=0,90.

Тоді індекс гібридного впливу становить:

$$H = (1 + 0{,}40)^{0.20}(1 + 0{,}30)^{0.25}(1 + 0{,}90)^{0.55} - 1 \approx 0{,}63.$$

Отримане значення H показує, що для категорії “персонал” фішингова атака з використанням воєнної тематики має високий рівень гібридного впливу, оскільки значення психологічного компонента є високим, а саме цей канал має найбільшу вагу для відповідної категорії активів.

Для подальшого розрахунку задаються базові індекси ризику RI_0, визначені за формулою 1.

У межах ілюстративного прикладу наведемо декілька пар “актив – загроза” з умовними значеннями базового індексу ризику.

Таблиця 3

Базові значення ризику для окремих пар «актив – загроза»

Категорія активів	**Сценарій загрози**	$\boldsymbol{RI_0}$
Серверна інфраструктура	DDoS-атака на критичний сервіс	0,58
Персонал	Фішингова атака з використанням воєнної тематики	0,42
Бази даних	Компрометація облікових записів	0,50
Управлінські процеси	Порушення процедур доступу в умовах кадрової перевантаженості	0,46
Публічні веб-ресурси	Дезінформаційна атака щодо діяльності організації	0,35

Після визначення базового індексу ризику та індексу гібридного впливу виконується сценарне коригування:

$$RI_{hyb}^{(s)} = RI_0 \cdot (1 + \lambda_s H), \quad (6)$$

де λ_s – коефіцієнт сценарного посилення ризику. У межах прикладу використовуються три сценарії: $\lambda_1 = 0{,}25, \lambda_2 = 0{,}5, \lambda_3 = 1{,}00$.

Результати розрахунку наведено в табл. 4.

Таблиця 4

Сценарні значення індексу ризику з урахуванням гібридного впливу

Категорія активів	**Сценарій загрози**	$\boldsymbol{RI_0}$	$\boldsymbol{H}$	$\boldsymbol{RI_{0,25}}$	$\boldsymbol{RI_{0,5}}$	$\boldsymbol{RI_{1,00}}$
Серверна інфраструктура	DDoS-атака на критичний сервіс	0,58	0,70	0,68	0,78	0,99
Персонал	Фішингова атака з використанням воєнної тематики	0,42	0,63	0,49	0,55	0,68
Бази даних	Компрометація облікових записів	0,50	0,59	0,57	0,65	0,80
Управлінські процеси	Порушення процедур доступу в умовах кадрової перевантаженості	0,46	0,65	0,53	0,61	0,76
Публічні веб-ресурси	Дезінформаційна атака щодо діяльності організації	0,35	0,46	0,39	0,43	0,51

Отримані результати демонструють, що врахування гібридного впливу змінює не лише абсолютні значення індексу ризику, а й уявлення про пріоритетність окремих ризиків. Найвищі значення у критичному сценарії отримано для DDoS-атаки на серверну інфраструктуру, компрометації облікових записів баз даних та порушення процедур доступу в управлінських процесах. Це пояснюється поєднанням достатньо високого базового індексу ризику та високого значення індексу гібридного впливу для відповідної категорії активів.

Окрему увагу слід звернути на те, що значення H не є однаковим для однієї й тієї самої загрози у всіх категоріях активів. Це зумовлено використанням різних вагових коефіцієнтів ω_T, ω_O, ω_P, які відображають специфіку активу. Наприклад, сценарій із високим психологічним компонентом матиме більший вплив на персонал, ніж на серверну інфраструктуру. Натомість сценарій із високим технічним компонентом сильніше впливатиме на технічні активи, для яких технічний канал має більшу вагу.

Результати сценарного розрахунку можуть бути використані для ранжування ризиків. Наприклад, за базовим сценарієм $\lambda = 0{,}5$ найвищий індекс ризику має DDoS-атака на серверну інфраструктуру: $RI_{0.5}$=0,78. Другу позицію займає компрометація облікових записів баз даних: $RI_{0.5}$=0,65. Третю позицію займає порушення процедур доступу в управлінських процесах: $RI_{0.5}$=0,61.

Це означає, що за умов помірного гібридного тиску першочергову увагу доцільно приділяти забезпеченню доступності критичних сервісів, захисту облікових записів та стабільності процедур управління доступом. При цьому фішингова атака на персонал також

зберігає значущий рівень ризику, однак у наведеному прикладі її пріоритет нижчий через менший базовий індекс RI_0.

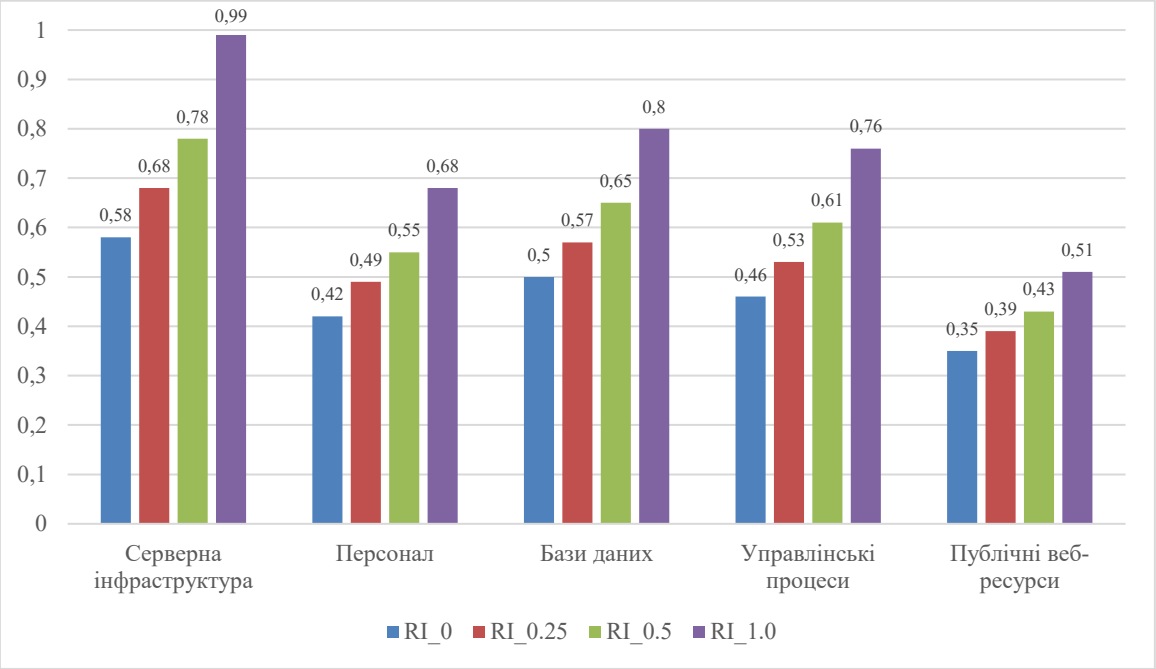

Рис. 1 Порівняльна діаграма індексів ризиків для досліджуваних категорій активів

Сценарний підхід також дозволяє оцінити чутливість ризику до посилення гібридного контексту. Наприклад, для серверної інфраструктури значення ризику зростає з 0,68 у консервативному сценарії до 0,99 у критичному сценарії. Для публічних веб-ресурсів відповідне зростання є менш вираженим – з 0,39 до 0,51. Це свідчить про те, що різні ризики мають неоднакову залежність від рівня гібридного тиску, а отже, повинні аналізуватися не лише за базовим ризиком, а й за сценарною динамікою його зміни.

Наведений приклад демонструє, що запропонована методика дозволяє виконати три практичні завдання. По-перше, вона забезпечує коригування базового індексу ризику з урахуванням гібридного впливу. По-друге, вона дозволяє врахувати різну чутливість категорій активів до технічного, організаційного та психологічного каналів. По-третє, вона надає можливість оцінити зміну ризику за кількома сценаріями гібридного тиску без фіксації одного універсального значення коефіцієнта посилення.

Висновки

У статті запропоновано метод оцінювання ризику інформаційної безпеки оргпнізації з урахуванням гібридного впливу, який дає змогу поєднати базову оцінку ризику з додатковим урахуванням технічного, організаційного та інформаційно-психологічного каналів впливу. Запропонований підхід ґрунтується на розрахунку базового індексу ризику та його подальшому коригуванні за допомогою індексу гібридного впливу, що дозволяє врахувати специфіку функціонування організації в умовах гібридних загроз. Обґрунтовано доцільність використання модифікованого зваженого геометричного агрегування для формування індексу гібридного впливу. Такий підхід забезпечує узгоджене врахування технічної, організаційної та інформаційно-психологічної складових, а також дозволяє адаптувати оцінку до особливостей конкретної категорії активів. Визначення вагових коефіцієнтів для категорій активів, а не для кожної окремої загрози, зберігає практичну застосовність методу та зменшує надмірну деталізацію розрахунків. Для формалізації експертних суджень щодо значущості каналів гібридного впливу запропоновано використовувати метод аналізу ієрархій. Його застосування дозволяє обґрунтовано визначати ваги технічної, організаційної та

© Легомінова С.В., Примаченко Д.В. Метод оцінювання ризику інформаційної безпеки з урахуванням гібридного впливу. Сучасний захист інформації, 2(66), 106–115.
https://doi.org/10.31673/2409-7292.2026.027509

інформаційно-психологічної складових залежно від типу активу, що оцінюється. Це є важливим, оскільки різні активи мають неоднакову чутливість до гібридного впливу: для технічної інфраструктури більш значущими можуть бути технічні чинники, для персоналу – інформаційно-психологічні, для управлінських процесів – організаційні.

Додатково введено коефіцієнт сценарного посилення ризику λ, який відображає загальний рівень впливу гібридного контексту на базову оцінку ризику. Запропоноване використання консервативного, базового та критичного сценаріїв дає змогу не обмежуватися одним фіксованим значенням цього коефіцієнта, а аналізувати чутливість ризику до різного рівня гібридного тиску. Такий сценарний підхід підвищує аналітичну цінність результатів, оскільки дозволяє виявити ризики, які залишаються значущими незалежно від сценарію, а також ризики, що істотно зростають лише за критичних умов. Наведений приклад застосування методу підтвердив можливість його використання для ранжування ризиків інформаційної безпеки за різними категоріями активів і сценаріями загроз. Результати розрахунків показали, що врахування гібридного впливу дозволяє уточнити пріоритетність ризиків, визначити активи, найбільш чутливі до окремих каналів впливу, та оцінити зміну ризику залежно від сценарію гібридного тиску. Практичне значення запропонованого методу полягає в можливості його застосування як інструменту підтримки прийняття рішень у сфері інформаційної безпеки організації. Метод може бути використаний для попереднього кількісного оцінювання ризиків, порівняння сценаріїв гібридного впливу, визначення пріоритетності захисних заходів та обґрунтування управлінських рішень щодо підвищення стійкості організації. Подальші дослідження доцільно спрямувати на уточнення шкал оцінювання вхідних параметрів, верифікацію запропонованої моделі на основі реальних даних про інциденти та розширення переліку категорій активів і сценаріїв загроз.

Перелік посилань

1. Auzina I., Volkova T., Norena-Chavez D., Kadłubek M., Thalassinos E. Cyber Incident Response Managerial Approaches for Enhancing Small–Medium-Size Enterprise's Cyber Maturity. In: Digital Transformation, Strategic Resilience, Cyber Security and Risk Management. Vol. 111A. Bingley: Emerald Publishing Limited, 2023. P. 175–190. DOI: http://dx.doi.org/10.1108/s1569-37592023000111a012.

2. Берко А. Ю., Висоцька В. А., Рішняк І. В. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції. Інформаційні системи та мережі. 2008. № 610(1). С. 20–33. URL: https://lnk.ua/Y7HCO2OWQ.

3. Барченко Н. Л., Любчак В. О., Лаврик Т. В. Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. Кібербезпека: освіта, наука, техніка. 2022. № 2(18). С. 73–85. DOI: https://doi.org/10.28925/2663-4023.2022.18.7385

4. Дзюба Л. Ф., Чмир О. Ю. Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики. Вісник Львівського державного університету безпеки життєдіяльності. 2022. № 26. С. 47–54. URL: https://lnk.ua/6jeUP9iLX

5. Khakzad N., Khan F., Amyotte P. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliability Engineering & System Safety. 2013. Vol. 111. P. 81–92. DOI: http://dx.doi.org/10.1016/j.ress.2011.03.012

6. Гловацький В. В. Методи оцінювання стану безпеки та загроз інформаційних ресурсів. Зв'язок. 2016. № 5. С. 13–16. URL: https://con.dut.edu.ua/index.php/communication/article/view/1324/1257

7. OECD. Economic Security in a Changing World: Building Stronger Defences for a Digital Future – The Role of Cybersecurity. Paris: OECD Publishing, 2025. URL: https://www.oecd.org/en/publications/2025/09/economic-security-in-a-changing-world_78f3b129/full-report/building-stronger-defences-for-a-digital-future-the-role-of-cybersecurity_484bcb90.html

8. PwC. Building Cybersecurity through Top Management Collaboration. Findings from the 2025 Global Digital Trust Insights Survey. 2025. URL: https://www.pwc.com/ua/uk/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey.html

9. Savelieva T., Panasko O., Prigodyuk O. Analysis of Methods and Means to Implement a Risk-Oriented Approach in the Context of Providing Enterprise Information Security. Bulletin of Cherkasy State Technological University. 2018. Vol. 23, No. 1. P. 81–89. DOI: http://dx.doi.org/10.24025/2306-4412.1.2018.153279

10. Memon M., Hameed S. Information Security Risk Plans within Enterprise Architecture Framework. International Journal of Advanced Computer Science and Technology. 2019. Vol. 8, № 10. P. 82-88. https://doi.org/10.30534/ijacst/2019/018102019.

Svitlana Lehominova
Doctor of Economics, Professor, Head of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-4433-5123
E-mail: s.legominova@duikt.edu.ua

Diana Prymachenko
Assistant Professor, Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0003-2386-7440
E-mail: primachenko.dv@duikt.ua

METHOD OF ASSESSING INFORMATION SECURITY RISK TAKING INTO ACCOUNT HYBRID IMPACT

The article considers the problem of assessing information security risk in conditions of hybrid impact, which combines technical, organizational and information-psychological factors. It is substantiated that the use of traditional risk assessment without taking into account the specifics of the hybrid context may lead to insufficiently accurate determination of threat priority, since different categories of assets have different sensitivity to individual channels of influence. A method of assessing information security risk is proposed, in which the basic risk index is adjusted taking into account the hybrid impact index. The hybrid impact index is formed on the basis of technical, organizational and psychological components using modified weighted geometric aggregation. To determine the weight coefficients of the components of hybrid impact, it is proposed to apply the method of hierarchy analysis taking into account the asset category. Additionally, a scenario risk amplification coefficient is introduced, which allows assessing the change in risk under conservative, basic and critical scenarios of hybrid pressure. An example of applying the proposed method for typical asset categories and threat scenarios is given. The results obtained confirm that the proposed approach allows to avoid simplified averaging of heterogeneous factors of hybrid impact, to take into account the specificity of assets and to perform scenario ranking of information security risks. The practical value of the proposed method for preliminary quantitative risk assessment, comparison of hybrid impact scenarios, prioritization of protective measures and justification of management decisions to increase the resilience of the organization is proven.

Keywords: cybersecurity, information security; cyber risk, hybrid impact; hybrid threats; risk-oriented approach; method of analysis of hierarchies.

Надійшла до редакції (Received): 25.04.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

© Легомінова С.В., Примаченко Д.В. Метод оцінювання ризику інформаційної безпеки з урахуванням гібридного впливу. Сучасний захист інформації, 2(66), 106–115.
https://doi.org/10.31673/2409-7292.2026.027509