УДК 004.056:338.1 DOI: http://dx.doi.org/10.30970/meu.2025.53.0.5309
JEL M15, E21

ОЦІНЮВАННЯ РИЗИКІВ В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ У КОНТЕКСТІ ЗОВНІШНІХ ЗАГРОЗ

Андрій Денисенко[1] , Ірина Нетреба[2], Володимир Овсієнко[3]

[1,3]Приватний вищий навчальний заклад «Європейський університет»
03115, м. Київ, бульвар академіка Вернадського, 16 В
[1]e-mail: andriy.denysenko@e-u.edu.ua, ORCID: 0009-0007-8057-9444
[2]Київський національний університет імені Тараса Шевченка
01033, м. Київ, вул. Володимирська, 60
e-mail: netrebai@knu.ua, ORCID: 0000-0001-5586-5405
[3]e-mail: volodumur.ovsienko@e-u.edu.ua, ORCID: 0009-0001-4763-2537

Анотація. *У статті розглянуто особливості оцінювання ризиків в системі управління інформаційною безпекою підприємств в умовах зростання впливу зовнішніх загроз. Здійснено аналіз сучасних підходів до ідентифікації ризиків та оцінювання їх впливу на функціонування підприємств у цифровому середовищі. Надано характеристику процесу створення зведеного реєстру активів і ризиків, що включає ідентифікацію активів, визначення ймовірності реалізації загроз, оцінювання потенційних збитків підприємства та обчислення рівня ризику з використанням матриці ризиків. В основу методики покладено систему експертних оцінок, що доповнюється кількісною шкалою для визначення критичності ризиків. Пріоритезацію ризиків здійснено з урахуванням рівня збитків і доступності ресурсів на їх обробку. Наведено критерії для ухвалення рішень щодо подальшого управління ризиками – прийняття, обробка, уникнення або передача. Обґрунтовано необхідність розробки плану обробки ризиків з деталізацією необхідних заходів, відповідальних осіб, термінів, витрат і контрольних показників. Особливу увагу приділено процедурі документування кожного етапу, включаючи прийняття остаточних ризиків, узгодження з власниками та періодичний перегляд реєстрів.*

Ключові слова*: інформаційна безпека, інформаційні активи, ризик-менеджмент, оцінювання ризику, обробка ризиків, підприємство, цифровізація.*

Постановка проблеми. У сучасних умовах цифровізації бізнесу підприємства стикаються з дедалі більшою кількістю зовнішніх загроз інформаційній безпеці, що можуть призвести до значних фінансових втрат, порушення неперервності бізнес-процесів, втрати конфіденційної інформації та репутаційних ризиків. Традиційні підходи до забезпечення інформаційної безпеки виявляються недостатніми без

системного управління ризиками, що передбачає їх ідентифікацію, кількісну оцінку та обґрунтовану обробку. Відсутність чітких методичних засад оцінювання рівня ризиків, особливо у контексті зовнішніх кіберзагроз, ускладнює процедуру прийняття рішень щодо доцільності розробки і реалізації низки заходів, спрямованих на захист інформації та розподіл наявних ресурсів.

Найбільш ефективним у цій сфері є використання рекомендацій, викладених у міжнародному стандарті ISO/IEC 27001:2022, який забезпечує структуровану модель впровадження, функціонування, моніторингу та удосконалення системи управління інформаційною безпекою (СУІБ). Проте, незважаючи на наявні загальні вимоги, на практиці доволі складно адаптувати ці положення до реалій та потреб конкретного підприємства, особливо щодо оцінювання та пріоритезації ризиків з урахуванням специфіки зовнішніх загроз. Таким чином, актуальним питанням є створення прозорого, адаптивного алгоритму оцінювання ризиків, що уможливить формалізацію процесів прийняття рішень, планування заходів з обробки ризиків, а також забезпечить відповідність підприємства положенням ISO/IEC 27001:2022 та його додатків.

Аналіз основних досліджень і публікацій. Проблематика управління ризиками інформаційної безпеки в умовах активізації зовнішніх загроз нині широко досліджується науковцями, а також є одним із важливих аспектів, що викладені у практичних рекомендаціях міжнародних стандартів. Ключовим нормативним документом у цій сфері є ISO/IEC 27001:2022 [12], що визначає вимоги до створення, впровадження, підтримки та постійного удосконалення СУІБ. У новій редакції стандарту значну увагу приділено оцінюванню ризиків, узгодженості заходів безпеки, а також циклічності процесу прийняття рішень у контексті ризик-орієнтованого підходу.

У працях науковців акцентовано увагу на різноманітних підходах до кількісної та якісної оцінки ризиків. Так, у дослідженні M. Whitman та H. Mattord [9] обґрунтована необхідність застосування багаторівневої моделі управління ризиками, що включає ідентифікацію активів, загроз та визначення ймовірностей їх реалізації. У наукових роботах R. Baskerville та M. Siponen [10], вивчаються питання економічної доцільності впровадження заходів безпеки з позиції оптимізації витрат і зниження потенційних збитків. У вітчизняній науковій літературі значний внесок у вивчення проблематики оцінювання ризиків на підприємствах зробили дослідники Василюк В. Я., Климчик С. О., Олешко Т.І., Бойко Ю.П., Панченко В. А. [5; 7; 8]. Слід зазначити, що у сучасних умовах вагомого значення також набуває пошук можливостей інтегрування різних методик оцінки ризику, враховуючи особливості побудови бізнес-процесів підприємств та сферу діяльності. Наукова праця Карпович І., Гладкої О., Бухало Ю. [6] вміщує обґрунтування доцільності застосування положень теорії графів, що поєднані з експертними методами для оцінювання і аналізу можливих ризиків інформаційної безпеки підприємств.

Водночас, більшість досліджень зосереджені переважно на загальних підходах до управління ризиками або окремих напрямах, таких як аудит, політика безпеки чи інцидент-менеджмент. Недостатньо висвітленими залишаються питання практичної реалізації оцінювання ризиків відповідно до ISO/IEC 27001:2022 у контексті зовнішніх загроз. Сьогодні актуальними є питання формалізації експертних оцінок, впровадження критеріїв пріоритезації та організації процедури узгодження і обробки ризиків на рівні підприємств. Отже, існує потреба у створенні практико-орієнтованої методики, що уможливить інтегрування вимог ISO/IEC 27001:2022 у внутрішні бізнес-процеси підприємства та забезпечить відповідність міжнародним стандартам і реальну ефективність у протидії зовнішнім загрозам.

Постановка завдання. Зважаючи на актуальність проблеми управління ризиками інформаційної безпеки, а також необхідність адаптації міжнародного стандарту ISO/IEC 27001:2022 [12] до практичної діяльності підприємств, метою даного дослідження є удосконалення процедури оцінювання, зокрема, встановлення пріоритетів та обробка ризиків у СУІБ.

Для досягнення мети необхідно вирішити низку завдань: визначити основні типи зовнішніх загроз, які є найбільш вагомими для підприємств та оцінити їх вплив на активи інформаційної системи; удосконалити методику кількісного оцінювання ризиків на основі експертного визначення ймовірності загроз і можливих збитків; обґрунтувати доцільність використання матриці ризиків та критеріїв для прийняття рішень щодо їх обробки; розкрити сутність пріоритезації ризиків з урахуванням доступності ресурсів і критичності впливу; визначити процедуру документування результатів оцінювання та обробки ризиків для подальшого аудиту, перегляду та ухвалення рішень керівниками підприємств. Реалізація поставлених завдань спрямована на забезпечення практичного впровадження вимог міжнародного стандарту у діяльність підприємств, підвищення рівня інформаційної безпеки та оптимізацію процесу управління ризиками в умовах постійних зовнішніх загроз.

Методи дослідження. У процесі дослідження використано комплекс методів, спрямованих на системний аналіз та практичну реалізацію процесів управління ризиками інформаційної безпеки відповідно до вимог міжнародного стандарту ISO/IEC 27001:2022. Зокрема, аналіз нормативно-правової та методичної бази, включаючи положення стандартів ISO/IEC 27001:2022 та ISO/IEC 27005 - для визначення вимог до оцінювання ризиків, контролю безпеки та удосконалення процедури прийняття рішень щодо ризиків; метод системного аналізу – для виокремлення ключових етапів процесу управління ризиками в СУІБ, встановлення взаємозв'язків між активами, загрозами і потенційними наслідками інцидентів; метод експертних оцінок — для визначення ймовірності реалізації зовнішніх загроз та можливих фінансових збитків. Залучення експертів забезпечує оцінювання суб'єктивних характеристик, якщо відсутні достовірні статистичні дані; використання матриці ризиків — для формалізації результатів експертного аналізу за допомогою шкал імовірності та шкоди, що дає змогу розрахувати рівень ризику; кластеризація та ранжування ризиків – для здійснення пріоритезації ризиків на основі їх критичності, доступності ресурсів на обробку та відповідності критеріям прийнятності ризику.

Виклад основного матеріалу дослідження. Визначення та аналіз ризиків у СУІБ підприємства, особливо у контексті зовнішніх загроз, є критично важливою процедурою для забезпечення захисту конфіденційності інформації, дотримання принципів цілісності і доступності даних. Успішність ризик-менеджменту у сфері інформаційного забезпечення управління значним чином залежить від таких складових:

- своєчасна ідентифікація потенційних загроз;
- оцінювання впливу загроз на окремі бізнес-процеси та функціонування підприємства загалом;
- визначення ймовірності настання ситуації, що може призвести до фінансових втрат;
- розробка заходів, спрямованих на зменшення ризиків.

Оцінювання ризиків, як правило, виконують учасники Робочої групи СУІБ. Результати роботи документуються у вигляді окремого реєстру ризиків (зведений реєстр ризиків з оцінками і пріоритетами). Для підготовки зведеного реєстру ризиків

необхідно скласти зведену форму, що вміщує активи і ризики інформаційної безпеки (Таблиця 1):

Таблиця 1

Зведена форма реєстру активів і ризиків інформаційної безпеки*

Реєстр активів					Реєстр ризиків				Оцінка ризиків				Інформація для розробки заходів з обробки ризиків			
№	Найменування активу	Власник активу	Клас активу	Місце розташування	№	Опис ризику	Хто визначив ризик?	Поточні ключові заходи, спрямовані на зниження ризику	Оцінка імовірності ризику	Оцінка впливу ризику - збитки	Загальна оцінка ризику	Критерій прийнятності ризиків	Опис заходів з обробки ризику та посилання на контролі безпеки	Власник ризику (відповідальний за заходи щодо зниження ризику)	Трудовитрати, л / д	Вартість

**Джерело: систематизовано авторами*

Для проведення відповідних розрахунків необхідно знати дві змінні величини: імовірність і збитки. Визначення цих складових проводиться методом експертних оцінок. Для зниження похибки, що може виникнути у зв'язку з використанням методу експертних оцінок, доцільно використовувати методику вибору варіантів, наведену нижче (Таблиці 2, 3):

Таблиця 2

Визначення імовірності настання ризикової події*

Імовірність виникнення	Опис	Числове значення
Дуже низька	Якщо малоімовірно, що ця ризикова подія може відбутися (<5%)	1
Низька	Якщо ризикова подія, швидше за все, не настане (5-20%)	2
Середня	Якщо імовірність настання ризикової події досить вагома (21-40%)	3
Висока	Якщо ризик найімовірніше реалізується (41-60%)	4
Дуже висока	Якщо ризик напевно реалізується (> 60%)	5

**Джерело: систематизовано авторами*

Оцінювання ризику здійснюють за формулою:

*Ризик = Імовірність * Збиток* (1)

Як вже зазначалося, важливим етапом в оцінюванні ризиків інформаційної безпеки є їх пріоритезація, що відбувається на підставі критичності ризиків та залежить,

в першу чергу, від величини збитків. Якщо одночасно виникають ризики, що мають однакове числове значення, першим обробляють той, значення збитку якого вище.

Таблиця 3

Визначення впливу ризикової події на фінансові результати (потенційні збитки) підприємства

Потенційний збиток	Опис впливу на фінансові результати підприємства	Числове значення
Дуже низький	Вплив на фінансові результати підприємства незначний	1
Низький	Вплив на фінансові результати підприємства не надто суттєвий	2
Середній	Суттєвий вплив на фінансові результати підприємства	3
Високий	Вплив на фінансові результати підприємства значний, можливе виникнення фінансової кризи	4
Дуже високий	Руйнівний вплив на фінансові результати підприємства, значні фінансові збитки, порушення фінансової рівноваги, що може згодом призвести до банкрутства	5

**Джерело: систематизовано авторами*

Також вагомим аспектом є доступність ресурсів на їх обробку, зокрема, встановлення меншого пріоритету обробці ризику з більшим значенням збитків, якщо на даний момент ресурси для його обробки відсутні. На основі цих факторів визначаються критерії для оцінювання і прийняття ризиків.

Таблиця 4

Критерії для оцінювання та прийняття ризиків*

Значення ризику	Дії з ризиком
1-9	Ризики приймаються, обробка не потрібна
10-16	Ризики обробляються за наявності ресурсів і за рішенням Робочої групи СУІБ
20-25	Ризики обробляються в обов'язковому порядку

**Джерело: систематизовано авторами*

Для спрощення процесу розрахунку ризиків необхідно використовувати матрицю для визначення ризику, наведену у Таблиці 5: достатньо визначити імовірність і збиток, після чого значення ризику буде отримано на перетині відповідного стовпця і рядка.

Таблиця 5

Визначення ризику *

Дуже висока	**5**	**10**	**15**	**20**	**25**
Висока	**4**	**8**	**12**	**16**	**20**
Середня	**3**	**6**	**9**	**12**	**15**
Низька	**2**	**4**	**6**	**8**	**10**
Дуже низька	**1**	**2**	**3**	**4**	**5**
Імовірність / **Збитки**	Дуже низькі	Незначні	Середні	Високі	Дуже високі

**Джерело: систематизовано авторами*

Таким чином, за результатами пріоритезації ризиків в обов'язковому порядку здійснюється узгодження зведеного реєстру активів і ризиків відповідальними особами і оформлюється окремим документом.

Ризики, за якими прийнято рішення про неприйняття заходів, заносяться у «Положення про прийняття остаточних ризиків». Цей документ формують учасники Робочої групи СУІБ та узгоджують з власниками ризиків. При оформленні результатів прийняття остаточних ризиків може бути обрана форма, наведена у Таблиці 6:

Таблиця 6

Форма звіту про прийняття остаточних ризиків та плану дій щодо реагування на них*

Характеристика ризику		Ризик до прийняття заходів, значення			План робіт					Ризик після ухвалення заходів, значення			Аналіз результативності заходів
№	Опис	Імовірність	Збиток	Значення ризику	Опис заходів з обробки ризику та посилання на контролі безпеки	Відповідальний за реалізацію заходів для зниження ризику (власник ризику)	Термін	Трудозатрати, л / д	Вартість	Імовірність	Збиток	Значення ризику	

**Джерело: систематизовано авторами*

Зазначимо, що форма «Звіту про прийняття остаточних ризиків» може бути довільною, однак має обов'язково вміщувати наступні атрибути:

- Пріоритет;
- Характеристика ризику;
- Причина прийняття ризику.

Прийняття остаточних ризиків здійснюється на основі «Звіту про виконання плану обробки ризиків» за результатами аналізу ситуації керівниками підприємства.

Висновки та перспективи подальших досліджень. У результаті проведеного дослідження удосконалено процедуру визначення та оцінювання ризиків у системі управління інформаційною безпекою підприємства з урахуванням вимог міжнародного стандарту ISO/IEC 27001:2022. Використання на практиці матриці ризиків, побудованої на основі експертних оцінок, дає змогу керівникам підприємства формалізувати процес прийняття рішень, ефективніше розподіляти ресурси та адаптувати політики безпеки до конкретних умов, у яких працює підприємство, що викликані зовнішніми загрозами.

Перспективи подальших досліджень полягають в удосконаленні технічного інструментарію для автоматизації процедури оцінювання ризиків відповідно до обраної моделі; розширенні методики з урахуванням нефінансових наслідків, зокрема за наявності репутаційних, правових, операційних ризиків; адаптації моделі до галузевої специфіки, а також інтеграції підходу до ризик-менеджменту з іншими підсистемами управління підприємством: IT-аудитом, безперервністю бізнесу (BCM) та інцидент-менеджментом.

Оцінювання та управління ризиками інформаційної безпеки є невід'ємною частиною стратегії будь-якого підприємства. Реалізація цих процедур на належному рівні дає змогу мінімізувати негативні наслідки зовнішніх та внутрішніх загроз, забезпечуючи стабільну роботу компанії та захист її критично важливих активів. Отримані результати можуть бути використані як основа для впровадження або удосконалення СУІБ на підприємствах для забезпечення відповідності міжнародним вимогам до захисту інформації в умовах динамічного зовнішнього оточення.

---

1. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України від 9 січня 2007 року. № 537-V. Відомості Верховної Ради України. 2007. № 12. Ст.102.
2. Про інформацію. Закон України від 2 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text 9. (дата звернення: 21.06.2025).
3. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 5 липня 1994 року. № 80/94. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 22.06.2025).
4. Архипов О.Є, Архипова Є.О. Положення про інформаційну безпеку в міжнародних стандартах. *Інформаційна безпека людини, суспільства, держави.* 2010. №2 (4). С. 62-65.
5. Василюк В. Я., Климчик С. О. Інформаційна безпека держави. Київ: ВД «Скіф», 2008. 136 с.
6. Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології*. 2021. №1(23). С. 62–68.
7. Олешко Т.І. Бойко Ю.П., Нінічук С.В. Характеристика та аналіз ризик-менеджменту для підприємств комерційної діяльності. *Регіональна економіка та управління.* 3 (29). 2020. С. 72-76.
8. Панченко В. А. Менеджмент інформаційної безпеки комерційного підприємства. *Центральноукраїнський науковий вісник. Економічні науки*. 2019. Вип. 3(36). С. 219-228. DOI: https://doi.org/10.32515/2663-1636.2019.3(36).219-228.
9. Whitman, M. E., & Mattord, H. J. (2019). Principles of Information Security (6th ed.). Cengage Learning.
10. Siponen, M., Wilson, R. and Baskerville, R. Power and practice in information systems security research. International Conference on Information Systems (ICIS), 2018, Paris.
11. Abbas, S., Naser, W., & Kadhim, A. Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Global Journal of Engineering and Technology Advances. 2023. DOI: https://doi.org/10.30574/gjeta.2023.14.2.0031
12. ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems. URL: https://www.iso.org/standard/27001 (дата звернення: 14.06.2025).

References

1. Pro Osnovni zasady rozvytku informatsiinoho suspil′stva v Ukraini na 2007-2015 roky. Zakon Ukrainy vid 9 sichnia 2007 roku № 537-V.
2. Pro Informatsiiu. Zakon Ukrainy vid 2 zhovtnia 1992 roku № 2657-XII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2657-12#Text 9. (accessed 21 June 2025).
3. Pro zakhyst informatsii v informatsiyno-telekomunikatsiynykh systemakh. Zakon Ukrainy vid 5 lypnya 1994 roku № 80/94. Retrieved from: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (accessed 22 June 2025).
4. Arkhipov, O. Ye., Arkhipova, Ye. O. (2010). Polozhennia pro informatsiinu bezpeku v mizhnarodnykh standartakh. *Informatsiina bezpeka lyudyny, suspil'stva, derzhavy. [Information security of the person, society and state]*. 2(4). P. 62-65.

5. Vasiliuk, V. Ya., Klymchyk, S. O. (2008). Informatsiina bezpeka derzhavy. Kyiv. 136 p.
6. Karpovich, I., Hladka, O. & Bukhalo, Yu. (2021). Tekhnolohiyi modelyuvannya ta otsinky ryzykiv informatsiynoyi bezpeky *[Information security risk modeling and assessment technologies]*. Tekhnichni nauky ta tekhnolohiyi – Technical sciences and technologies, 1(23), 62–68.
7. Oleshko, T.I., Bojko, Yu.P. and Ninichuk S.V. (2020). Kharakterystyka ta analiz ryzyk-menedzhmentu dlia pidpryiemstv komertsijnoi diial'nosti. *Rehional'na ekonomika ta upravlinnia. [Regional economics and management]*. №3(29). pp. 72-76.
8. Panchenko, V.A. (2019). Information security management of a commercial enterprise. Tsentral'noukrayins'kyy naukovyy visnyk. Ekonomichni nauky *[Central Ukrainian Scientific Bulletin. Economic sciences]*, №3 (36), pp. 219-228. DOI: https://doi.org/10.32515/2663-1636.2019.3(36).219-228.
9. Whitman, M. E., & Mattord, H. J. (2019). Principles of Information Security (6th ed.). Cengage Learning.
10. Siponen, M. , Wilson, R. and Baskerville, R. (2018), Power and practice in information systems security research. International Conference on Information Systems (ICIS), Paris.
11. Abbas, S., Naser, W., & Kadhim, A. (2023). Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). *Global Journal of Engineering and Technology Advances.* DOI: https://doi.org/10.30574/gjeta.2023.14.2.0031
12. ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems. URL: https://www.iso.org/standard/27001 (accessed 14 June 2025).

RISK ASSESSMENT IN THE INFORMATION SECURITY MANAGEMENT SYSTEM OF ENTERPRISES IN THE CONTEXT OF EXTERNAL THREATS

Andriy Denysenko[1], Iryna Netreba [2], Volodymyr Ovsiienko[3]

[1,3] «Private higher educational institution "European University»
03115, Kyiv, Academician Vernadskyi Boulevard, 16 V
[1]e-mail: andriy.denysenko@e-u.edu.ua, ORCID: 0009-0007-8057-9444
[2] Taras Shevchenko National University of Kyiv
01033, Kyiv, Volodymyrska Street, 60
e-mail: netrebai@knu.ua, ORCID: 0000-0001-5586-5405
[3]e-mail: volodumur.ovsienko@e-u.edu.ua, ORCID: 0009-0001-4763-2537

Abstract. The article examines the features of risk assessment in the information security management system of enterprises in the context of the growing impact of external threats. An analysis of modern approaches to identifying risks and assessing their impact on the functioning of enterprises in the digital environment is carried out. A description of the process of creating a consolidated register of assets and risks at the enterprise is provided, which includes identifying assets, determining the probability of threat realization, assessing potential losses, and calculating the risk level using a risk matrix. The methodology is based on a system of expert assessments, supplemented by a quantitative scale to determine the criticality of risks. Risks are prioritized taking into account the level of potential losses and the availability of resources for their processing. Criteria for making decisions on further risk management are given - acceptance, processing, avoidance or transfer. The need to develop a risk processing plan with a detailing of the necessary measures, responsible persons, deadlines, and control indicators is substantiated. Particular attention is paid to the procedure

for documenting each stage, including the acceptance of final risks, coordination with owners and periodic review of registers. It was determined that after a detailed risk analysis, it is necessary to develop and implement an action plan to reduce them and compare the obtained risk values after the implementation of measures. It is important to describe the risk treatment actions, identify employees responsible for the implementation of risk reduction measures, establish deadlines for the plan implementation and calculate the cost of work. Based on the analysis of the report on the implementation of the risk treatment plan, enterprise managers consider possible scenarios and make decisions. Thus, this approach is aimed at systematizing the information security management process and maintaining transparency in decision-making regarding cyber risks at the enterprise level for the further formation of a strategy for protecting information resources, taking into account external cyber threats.

Keywords: information security, information assets, risk management, risk assessment, risk processing, enterprise, digitalization.

Стаття надійшла до редколегії 24.05.2025
Прийнята до друку 25.06.2025
Опублікована (оприлюднена) 09.07.2025