https://doi.org/10.12958/1817-3772-2025-3(81)-208-213

УДК 658:004.056

Катерина Сергіївна Озарко,
канд. екон. наук, доцент,
ORCID 0000-0002-1452-0686
e-mail: kateruna.ozarko@gmail.com
Державний університет інтелектуальних технологій і зв'язку, м. Одеса
Марія Зіновіївна Піх,
канд. екон. наук,
ORCID 0000-0003-4461-0364
e-mail: pmariyka@gmail.com
ВСП «Львівський фаховий коледж харчової і переробної промисловості НУХТ», м. Львів

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ЗА ДИНАМІЧНИХ УМОВ ГОСПОДАРЮВАННЯ

Постановка проблеми. Сучасні умови господарювання, що характеризуються високим рівнем динамічності та невизначеності, підвищеним рівнем ризиковості, формують стратегічне значення інформаційної безпеки підприємств. Цифровізування бізнес-процесів, глобалізування економічних відносин, посилення кіберзагроз, необхідність безперервного доступу до даних формують все нові виклики для систем менеджменту (управління) підприємств, організацій. Відповідно, зростає актуальність формування, розроблення та застосування ефективних, дієвих методик для оцінювання рівня інформаційної безпеки, які б дозволяли не лишень фіксувати стан захищеності, але й прогнозувати майбутні загрози, їх наслідки.

Традиційні підходи до процесів оцінювання інформаційної безпеки (її рівня) підприємств та організацій, як правило, ґрунтуються на системі перевіряння відповідності технічним стандартам, вимогам. Сучасні ж реалії свідчать про їх суттєву обмеженість (формальне дотримання стандартів не гарантуватиме стійкості до новітніх атак, інсайдерських загроз, витоку комерційної, персональної інформації). Проблеми підсилюються нестачею єдиного методологічного підходу до інтегрального оцінювання рівня інформаційної безпеки (із врахуванням комплексу організаційних, технічних, правових, соціально-поведінкових факторів).

Метою статті є дослідження проблем, потенційних можливостей оцінювання інформаційної безпеки підприємств за динамічних умов господарювання.

Аналіз останніх досліджень та публікацій. Проблематика оцінювання інформаційної безпеки підприємств за динамічних умов господарювання знаходить відображення у працях таких вчених як Ананченко О. [1, с. 297-308], Бакай В. [2, с. 32-35], Білько С. [3, с. 58-77], Безпарточна О. [23, с. 8-19], Бойко О. [4, с. 58-77], Браілко Л. [19, с. 121-127], Васильців В. [5], Ворохоб М. [14, с. 98-112], Дзюба Л. [6, с. 47-54], Дячков Д. [7], Завербний А. [8, с. 13-21; 9, с. 110-113], Зубок М. [10], Кицюк В. [11], Копитко С.Б. [17, с. 45-49], Корчомний Р. [14, с. 98-112], Коршун Н. [14, с. 98-112], Котрелін І. [12, с. 150-155], Леоненко Н. [13], Літвінчук І. [14, с. 98-112], Мазуренко Л. [15], Новаківський І. [16], Обрембальський С. [22, с. 1-11], Панченко О. [18, с. 32-38], Панченко Л. [18, с. 32-38], Поступна О. [13], Пупинін О. [11], Пушак Я. [4, с. 58-77; 9, с. 110-113; 23, с. 8-19], Смотрич Д. [19, с. 121-127], Сусіденко В. [20], Сусіденко О. [20], Топалов В. [21, с. 157-161], Трушкіна Н. [4, с. 58-77; 23, с. 8-19], Чистоклетов Л. [22, с. 1-11], Чмир О. [6, с. 47-54] та ін. Не дивлячись на значні досягнення дискусійним залишається питання адаптивності методів оцінювання рівня інформаційної безпеки до динамічності бізнес-середовища через неврахування швидкого трансформування технологічних процесів, поведінкових характеристик персоналу.

Виклад основного матеріалу дослідження. У науковій літературі останнім часом активно розглядаються питання інформаційної, кібербезпеки підприємств. Науковцями пропонуються різні методи (від застосування багатофакторного аналізування ризиків до побудови і використання економіко-математичних моделей оцінювання кіберстійкості, інформаційної безпеки).

На основі проведеного огляду наукових досліджень за тематикою можна виокремити наступні ключові проблеми оцінювання інформаційної безпеки.

Перш за все ключовою проблемою виступає фрагментарність підходів, оскільки більшість підприємств і організацій зосереджуються виключно на технічних аспектах захисту, частково нехтуючи організаційними, кадровими факторами тощо.

Наступною проблемою є висока динамічність (мінливість, видозмінюваність) кіберзагроз. Пояс-

нення полягає в тому, що нові види атак з'являються швидше, ніж підприємства і організації встигають адаптувати свої системи оцінювання, реагування.

Ще однією проблемою є недостатність кількісних показників (індикаторів) в процесах оцінювання, яке часто володіє якісним характером, не дозволяючи здійснювати порівняльне аналізування, прогнозування тощо.

Вагомою є також обмеженість фінансових, людських ресурсів. Адже середній і, особливо, малий бізнес є вразливими саме через неспроможність інвестувати у комплексні системи моніторингу та здійснення моніторингу, порівняльного аналізування, оцінювання, прогнозування інформаційної безпеки.

Також підприємства і організації стикаються із низькою культурою інформаційної безпеки персоналу. Саме людський фактор продовжує залишатися ключовим джерелом інцидентів. Даний перелік, звісно, не є вичерпним, адже, як вказано вище, саме через високу динамічність він може доповнюватися та видозмінюватися.

Відповідно, підприємствам і організаціям необхідно формувати дієві механізми забезпечення інформаційної безпеки бізнесу, зокрема і за умов воєнного стану. Поетапність формування таких механізмів доцільно здійснювати наступним чином:

1. Проведення детального аналізування зовнішніх і внутрішніх загроз. На даному етапі доцільним є виявлення (ідентифікування) основних ризиків інформаційної безпеки (кібератаки, диверсії, втручання держави-агресора, тощо); оцінювання вразливостей інфраструктури (канали зв'язку, хмара, програмне забезпечення тощо); SWOT-аналізування інформаційного середовища.

2. Формування політики інформаційної безпеки підприємства/організації. На цьому етапі доцільним є розроблення внутрішніх регламентів та протоколів дій при надзвичайних ситуаціях; формування політики доступу до інформації: багаторівнева аутентифікація, контролювання прав і врахування (адаптування до них) вимог міжнародних стандартів (ISO/IEC 27001, NIST, GDPR тощо).

3. Здійснення технічного забезпечення процесів. Формування захисту IT-інфраструктури (брандмауери, антивіруси, IDS/IPS-системи), VPN, шифрування даних. Важливим підетапом повинно стати також віртуалізування/розосередження серверів, перехід на резервні/закордонні хмарні сервіси, здійснення систематичного резервного копіювання (регулярне створення копій, географічне дублювання тощо).

4. Здійснення організаційного забезпечення. Передусім даний етап має бути скерований на персонал, зокрема необхідними є підвищення рівня обізнаності персоналу (проведення навчань, тренінгів, тестувань тощо); забезпечення безперервності бізнес-процесів а також за можливості призначення відповідального за інформаційну безпеку та моніторинг/оцінювання.

5. Проведення юридичного забезпечення. На даному етапі доцільним є актуалізування угод NDA, контрактів із працівниками, партнерами; ведення юридичного аудиту даних (відповідність нормам інформаційної безпеки); формування, застосування міжнародних каналів захисту прав (ЄС, США).

6. Формування та застосування інституційної взаємодії. Здійснення співпраці з державними структурами (CERT-UA, СБУ, Держспецзв'язок та ін.); активна участь у міжгалузевих платформах обмінювання інформацією щодо загроз інформаційній безпеці; оповіщення (за можливості миттєве) щодо інцидентів партнерів, клієнтів.

7. Моніторинг інформаційної безпеки, її рівня та забезпечення ефективного і своєчасного реагування на зміни. На даному етапі доцільними є наступні дії: систематичний моніторинг інформаційних систем; реалізування інцидент-менеджменту (SIEM-системи, автоматичне реагування); здійснення регулярних аудитів безпеки, пентестів, оцінювання вразливостей).

8. Забезпечення адаптивності, гнучкості системи управління інформаційною безпекою. Реалізування цього етапу потребуватиме постійного, систематичного оновлення політик, технологій; розроблення сценаріїв щодо адаптування інформаційної безпеки до нових викликів (воєнні дії, кібершантаж, кібератаки тощо). Етап потребуватиме ефективного використання інновацій (приміром, системи блокчейн для збереження даних).

Що ж стосується безпосередньо процесу оцінювання інформаційної безпеки, то доцільним є застосування агрегованої економіко-математичної моделі. Вказана модель повинна включати розширений набір індикаторів, методику їх нормалізування, агрегування, формули для даних розрахунків, рекомендації щодо валідування і практичного впровадження/використання.

Метою пропонованої моделі є отримання інтегральної кількісної оцінки рівня інформаційної безпеки підприємства (із вказанням шкали даного оцінювання, як загальноприйнятий варіант: від «0» до «100»), яка враховуватиме технічні, організаційні, правові, людські, операційні (стійкість) складові і буде придатною для порівнянь, моніторингу, пріоритизації заходів.

Пропонована структура моделі (за рівнями) оцінювання інформаційної безпеки містить певні складові, передусім категорії (пропонується застосувати наступні: технічну, організаційну, правову, людський фактор, стійкість/реагування. Для кожної із запропонованих категорій доцільно формувати відповідний набір індикаторів (F_i).

Наступною складовою є нормалізування індикаторів до оцінюваної шкали (0–100), здійснення зваженого агрегування в межах кожної категорії та зведення категоріальних балів до інтегрального індексу інформаційної безпеки.

Набір індикаторів рекомендується формувати та погоджувати з вищим керівництвом організації/підприємства. При цьому здійснювати підбір індикаторів (мінімальна кількість 3 позиції) для кожної із запропонованих категорій. Кількість можна розширювати в залежності від потреб системи оцінювання.

Нами пропонується застосування наступних індикаторів для кожної із категорій.

Для технічної категорії (Т) доцільними для оцінювання інформаційної безпеки є наступні індикатори: частка систем із багатофакторним автентифікуванням; частка систем із актуальними оновленнями. Дані індикатори, зрозуміло, вимірюються у відсотках за шкалою 0-100 %. Черговим індикатором може слугувати середній час, необхідний для виявлення інциденту (днів).

Щодо організаційної складової (О), то пропоновані індикатори є такими: документована та затверджена політика безпеки, зокрема й інформаційної; наявність плану реагування на виклики та загрози інформаційній безпеці; регулярність проведення внутрішніх аудитів (кількість за рік); частка бюджету на інформаційну безпеку в загальному ІТ-бюджеті.

У правову (L) складову доцільно включати наступні індикатори: відповідність регуляторним вимогам; наявність угод із підрядниками щодо захисту даних; наявність політики зберігання, видалення персональних даних; кількість інцидентів, пов'язаних з інформаційною безпекою, котрі мали юридичні наслідки.

Вагомим елементом є людський фактор. Інформативними індикаторами можуть бути такі: частка співробітників підприємства, що пройшли тренінг з інформаційної безпеки, захисту інформації тощо (за певний період); результати проведеного фішинг-тесту (частка вразливих); впровадженість політики доступу за ролями, наявність відповідальної особи за інформаційну безпеку (стосується великих підприємств).

Ще однією групою доцільно виділити здатність організації (її інформаційної системи) відновлювати функціональність, забезпечувати безперебійну роботу після інцидентів безпеки (кібератак, збоїв, природніх катастроф), використовуючи механізми адаптування, стійкості (резилієнс (R). Слід наголосити, що резилієнс виходить за межі «простої» стійкості до загроз, акцентуючи увагу на здатності зберігати ключові функції при кризах, швидкості повертатися до нормальної роботи. Індикаторами можуть бути частка критичних систем із бекапами, результати тестів відновлення тощо.

Важливим при побудові економетричної моделі виступає нормалізування індикаторів, адже для «прямих» відсотків чи балів (в діапазоні «0–100») можливе їх безпосереднє використання. Однак, це неможливо застосувати до таких індикаторів як «час», «кількість інцидентів». Тому необхідними є інвертування, нормалізування на шкалу від 0 до 100, доцільним є застосування формули нормалізування, стандартизування індикаторів (перетворення їх значень у порівнянну шкалу).

Важливу роль відіграє зважування індикаторів (міра їх впливу на інформаційну безпеку). Вага індикаторів в межах кожної категорії сумарно становитиме «1». Аналогічно і для всіх категорій (які можуть бути розширені/звужені в залежності від потреб, галузевої приналежності підприємства чи інших важливих чинників).

Інтегральний індекс IFS доцільно розраховувати за наступною формулою:

$$IFS = \sum_{i=1}^{n} q_i * F_i,$$

де *IFS* – інтегральний показник / індикатор рівня інформаційної безпеки, q_i – ваговий коефіцієнт *i*-го фактору (що визначає його важливість), F_i – значення *i*-го фактору (показника, індикатора), *n* – загальна кількість факторів.

Інтерпретування отриманих результатів можливе за різними шкалами. Одним із прикладів шкали може слугувати наступний: від 0 до 40 – низький рівень захищеності (інформаційної безпеки), від 41 до 60 – середній рівень, 61–80, відповідно «добрий» та 81-100 – високий.

Для практичного застосування пропонованої методики потрібне валідування моделі, врахування її чутливості. Доцільним є проведення чутливого аналізування шляхом зміни ваг для категорій (діапазон пропонованих змін становить ±10–20%). Відповідно потрібно здійснити розрахунки та оцінити поведінку інтегрального індикатора, тобто як він змінюватиметься.

Аналізування кореляції між IFS та наявною на підприємстві історією інцидентів дозволятиме підтверджувати, що у випадку нижчих значень IFS та більшої кількості інцидентів запропонована модель є адекватною та відображає реальні закономірності.

Практичне реалізування (запровадження) моделі доцільне покроково. Передусім необхідно узгодити обрані категорії, індикатори, ваги із вищим керівництвом підприємства. Наступним кроком є встановлення джерела отримання даних (HR, фінанси, аудит). Для спрощення процесів розрахунку можлива побудова дашборду (приміром, в Excel, Power BI) для збирання, розрахунків й аналізування. Наступним кроком слугуватиме пілотне оцінювання (протягом 3-6 місяців). Завершальним етапом має

бути корегування ваг, індикаторів. Важливим моментом також буде інтегрування даної моделі до процесу ризик-менеджменту (KPI, бюджетування, план заходів тощо).

Звісно, що модель матиме певні обмеження. Мова йде про рівень якості вихідних даних (критично впливатиме на результати); ваги (суб'єктивізм); важливою буде експертна участь; також модель не враховуватиме зовнішні системні ризики (постачальники хмарних сервісів) без додавання нових індикаторів.

Запропонована економетрична модель може бути ефективним інструментом аналітики у сфері інформаційної безпеки підприємств і організацій, дозволятиме поєднувати кількісні дані із якісними управлінськими висновками, підвищуючи рівень обґрунтованості стратегій розвивання інформаційної безпеки, цифрової стійкості бізнесу, особливо за умов війни.

Пропонована модель може стати основою для ухвалення стратегічних рішень (виправданість інвестування до хмарних сервісів, кіберстрахування, навчання персоналу тощо).

Перспективами подальшого вдосконалення, розвивання системи оцінювання інформаційної безпеки підприємств, організацій за сучасної парадигми є застосування саме інтегрованого підходу, що поєднуватиме кількісні, якісні методи аналізування, враховуватиме динамічність бізнес-середовища.

Загальні висновки. Оцінювання інформаційної безпеки підприємств (її рівня) у динамічних умовах (деколи навіть високо динамічних) господарювання потребує відходу від традиційних формальних підходів та поступової переорієнтації на комплексні, адаптивні, ризик-орієнтовані методики. Важливим завданням є розроблення інтегральних індикаторів, що відображатимуть рівень захищеності не лишень із технічної, але й із організаційної, правової, кадрової та інших точок зору. Перспективним напрямом досліджень виступає створення уніфікованої методики оцінювання, яка забезпечуватиме можливість порівняння різних підприємств, інтегрування оцінки (процесу оцінювання) інформаційної безпеки до загальної системи економічної безпеки. Реалізування зазначених підходів дозволятиме підприємствам не лише своєчасно виявляти, нейтралізувати загрози, але й забезпечувати стійкість, конкурентоспроможність на довгострокову перспективу.

Очікуваними результатами запровадження виступатимуть такі: підвищення стійкості бізнесу до зовнішніх інформаційних загроз, зменшення ризиковості втрат конфіденційної інформації, захист ділової репутації, клієнтських баз, підвищення рівня довіри споживачів, партнерів, інвесторів, інших стейкхолдерів.

ЛІТЕРАТУРА

1. Ананченко О. Методика оцінки ефективності забезпечення інформаційної безпеки освітньої інформаційної системи. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2023. № 1(21). С. 297-308. https://doi.org/10.28925/2663-4023.2023.21.297308

2. Бакай В.Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету*. 2020. № 4. Т. 1. С. 32-35. https://doi.org/10.31891/2307-5740-2020-284-4-5

3. Білько С. Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку. *Науковий вісник Полісся*. 2022. Вип. 1 (24). С. 58-77. https://doi.org/10.25140/2410-9576-2022-1(24)-58-77

4. Бойко О., Пушак Я., Трушкіна Н. Формування сучасної парадигми інформаційної безпеки національної економіки: теоретичні засади. *Вісник післядипломної освіти: зб. наук. пр. Серія «Соціальні та поведінкові науки». Психологія, економіка, державне управління*. 2022. №51. С. 139-160. https://doi.org/10.32405/2522-9931-2022-22(51)-139-160

5. Васильців В.Г. Організаційно-економічний механізм зміцнення економічної безпеки сектору інформаційних технологій. Автореф. дис. ... канд. екон. наук. Київ: Національний інститут стратегічних досліджень, 2018.

6. 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. https://doi.org/10.32447/20784643.26.2022.06

7. Дячков Д.В. Методичні підходи до оцінки інформаційної безпеки підприємства. *Вісник Сумського національного аграрного університету. Серія «Економіка і менеджмент».* 2017. Вип. 12. URL: https://dspace.pdau.edu.ua/items/561a76b9-0e9a-4b94-a0d2-ac211980eb11/full

8. Завербний А.С. Особливості формування системи управління кібербезпекою підприємств у воєнний період: теоретико-прикладний аспект. *Innovation and Sustainability*. 2024. № 1. С. 13-21. https://doi.org/10.31649/ins.2024.1.13.21

9. Завербний А.С., Пушак Я.Я. Проблеми та потенційні можливості розвитку ІТ-сфери в Україні за умов активізування процесів інтегрування до міжнародного ринку: управлінський аспект. *Вісник економічної науки України*. 2022. № 1 (42). С. 110-113. https://doi.org/10.37405/1729-7206.2022.1(42).110-113

10. Зубок М.І. Інформаційна безпека в підприємницькій діяльності. Київ: ГНОЗІС. 2015. 216 с.

11. Кицюк В.М., Пупинін О.С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації*. 2024. № 2. https://doi.org/10.31673/2409-7292.2024.020012

12. Котрелін І.Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 1. С. 150-155. https://doi.org/10.32782/392257

13. Леоненко Н.А., Поступна О.В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2022. Вип. 2(17). URL: http://repositsc.nuczu.edu.ua/handle/123456789/16883

14. Літвінчук І.С., Корчомний Р.О., Коршун Н.В., Ворохоб М.В. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. Вип. 2(10). С. 98-112. https://doi.org/10.28925/2663-4023.2020.10.98112

15. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету ім. В.Н. Каразіна. Серія «Питання політології»*. 2022. Вип. 42. https://doi.org/10.26565/2220-8089-2022-42-08

16. Новаківський І.І. Система управління підприємства в інформаційному суспільстві. Автореф. дис. ... д-ра екон. наук. Львів: Національний університет «Львівська політехніка». 2017.

17. Озарко К.С., Копитко С.Б. Особливості функціонального підходу до управління інформаційною безпекою підприємств за кризових умов. *Вісник економічної науки України*. 2023. № 1 (44). С. 45-49. https://doi.org/10.37405/1729-7206.2023.1(44).45-49

18. Панченко О.А., Панченко Л.В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*. 2015. № 2 (46). С. 32-38. URL: http://nbuv.gov.ua/UJRN/Pinform_2015_2_7

19. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*. 2023. Вип. 77, ч. 2. С. 121-127. https://doi.org/10.24144/2307-3322.2023.77.2.20

20. Сусіденко В., Сусіденко О. Комплексне забезпечення інформаційної безпеки як передумова інноваційного розвитку готельно-ресторанного бізнесу. *Економіка та суспільство*. 2025. Вип. 74. https://doi.org/10.32782/2524-0072/2025-74-96

21. Топалов В.М. Забезпечення інформаційної безпеки бізнесу україни в умовах сучасних загроз. *Цифрова економіка та економічна безпека*. 2024. Вип. 6 (15). С. 157-161. https://doi.org/10.32782/dees.15-24

22. Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії*. 2024. Вип. 31. С. 1-11. https://doi.org/10.5281/zenodo.11381101

23. Bezpartochna O., Pushak Ya., Trushkina N. Current issues of information security management during the state of martial. *Current issues of security management during martial law: scientific monograph*. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach. 2022. P. 8-19.

Надійшла до редакції 11.08.2025 р.
Прийнята до друку 29.08.2025 р.

REFERENCES

1. Ananchenko, O. (2023). Methodology for assessing the effectiveness of information security of the educational information system. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»*, 1 (21), 297–308. https://doi.org/10.28925/2663-4023.2023.21.297308 [in Ukrainian].

2. Bakai, V. Y. (2020). Ensuring the economic security of the enterprise based on the use of digital technologies. *Visnyk Khmelnytskoho natsionalnoho universytetu*, 4 (1), 32–35. https://doi.org/10.31891/2307-5740-2020-284-4-5 [in Ukrainian].

3. Bilko, S. (2022). Information and economic security: level assessment and interconnection. *Naukovyi visnyk Polissia*, 1 (24), 58–77. https://doi.org/10.25140/2410-9576-2022-1(24)-58-77 [in Ukrainian].

4. Boiko, O., Pushak, Ya., & Trushkina, N. (2022). Formation of a modern paradigm of information security of the national economy: theoretical principles. *Visnyk pisliadyplomnoi osvity: zb. nauk. pr. Seriia «Sotsialni ta povedinkovi nauky». Psykholohiia, ekonomika, derzhavne upravlinnia*, (51), 139–160. https://doi.org/10.32405/2522-9931-2022-22(51)-139-160 [in Ukrainian].

5.Vasyltsiv, V. H. (2018). Organizational and economic mechanism for strengthening the economic security of the information technology sector. (Extended abstract of Candidate's thesis). National Institute of Strategic Studies, Kyiv [in Ukrainian].

6. Dziuba, L. F., & Chmyr, O. Yu. (2022). Assessment of information security risks using methods of mathematical statistics. *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti*, (26), 47–54. https://doi.org/10.32447/20784643.26.2022.06 [in Ukrainian].

7. Diachkov, D. V. (2017). Methodological approaches to assessing the information security of an enterprise. *Visnyk Sumskoho natsionalnoho ahrarnoho universytetu. Seriia «Ekonomika i menedzhment»*, (12). https://dspace.pdau.edu.ua/items/561a76b9-0e9a-4b94-a0d2-ac211980eb11/full [in Ukrainian].

8. Zaverbnyi, A. S. (2024). Features of forming a cyber security management system for enterprises during the war period: theoretical and applied aspect. *Innovation and Sustainability*, 1, 13–21. https://doi.org/10.31649/ins.2024.1.13.21

9. Zaverbnyi, A. S., & Pushak, Ya. Ya. (2022). Problems and potential opportunities for the development of the IT sphere in Ukraine under the conditions of intensifying integration processes into the international market: management aspect. *Visnyk ekonomichnoi nauky Ukrainy*, 1 (42), 110–113. https://doi.org/10.37405/1729-7206.2022.1(42).110-113 [in Ukrainian].

10. Zubok, M. I. (2015). Information security in entrepreneurial activity. HNOZIS [in Ukrainian].

11. Kytsiuk, V. M., & Pupynin, O. S. (2024). Enterprise information security: theoretical aspect. *Suchasnyi zakhyst informatsii*, (2). https://doi.org/10.31673/2409-7292.2024.020012 [in Ukrainian].

12. Kotrelin, I. B. (2022). Information security in the conditions of martial law in the aspect of ensuring information rights and freedoms. *Aktualni problemy vitchyznianoi yurysprudentsii*, (1), 150–155. https://doi.org/10.32782/392257 [in Ukrainian].

13. Leonenko, N. A., & Postupna, O. V. (2022). Information security of Ukraine: mechanisms, modern challenges and threats in the conditions of information globalism. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriia: Derzhavne upravlinnia*, 2 (17). http://repositsc.nuczu.edu.ua/handle/123456789/16883 [in Ukrainian].

14. Litvinchuk, I. S., Korchomnyi, R. O., Korshun, N. V., & Vorokhob, M. V. (2020). Approach to assessing information security risks for an automated system of class "1". *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»*, 2 (10), 98–112. https://doi.org/10.28925/2663-4023.2020.10.98112 [in Ukrainian].

15. Mazurenko, L. I. (2022). Information security in the conditions of the Russian-Ukrainian war: challenges and threats. *Visnyk Kharkivskoho natsionalnoho universytetu im. V.N. Karazina. Seriia «Pytannia politolohii»*, (42). https://doi.org/10.26565/2220-8089-2022-42-08 [in Ukrainian].

16. Novakivskyi, I. I. (2017). Enterprise management system in the information society (Extended abstract of Doctor's thesis). National University "Lviv Polytechnic", Lviv [in Ukrainian].

17. Ozarko, K. S., & Kopytko, S. B. (2023). Features of the functional approach to managing information security of enterprises in crisis conditions. *Visnyk ekonomichnoi nauky Ukrainy*, 1 (44), 45–49. https://doi.org/10.37405/1729-7206.2023.1(44).45-49 [in Ukrainian].

18. Panchenko, O. A., & Panchenko, L. V. (2015). Information security and information culture in the modern information society. *Pravova informatyka*, 2 (46), 32–38. http://nbuv.gov.ua/UJRN/Pinform_2015_2_7 [in Ukrainian].

19. Smotrych, D. V., & Brailko, L. (2023). Information security in the conditions of martial law. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu*, 77 (2) , 121–127. https://doi.org/10.24144/2307-3322.2023.77.2.20 [in Ukrainian].

20. Susidenko, V., & Susidenko, O. (2025). Comprehensive provision of information security as a prerequisite for the innovative development of the hotel and restaurant business. *Ekonomika ta suspilstvo*, (74). https://doi.org/10.32782/2524-0072/2025-74-96 [in Ukrainian].

21. Topalov, V. (2024). Ensuring the information security of Ukrainian business in the face of modern threats. *Tsyfrova ekonomika ta ekonomichna bezpeka*, 6 (15) , 157–161. https://doi.org/10.32782/dees.15-24 [in Ukrainian].

22. Chystokletov, L., & Obrembal skyi, S. (2024). Features of ensuring information security in the conditions of the Russian-Ukrainian war. *Akademichni vizii*, (31), 1–11. https://doi.org/10.5281/zenodo.11381101 [in Ukrainian].

23. Bezpartochna, O., Pushak, Ya., & Trushkina, N. (2022). Current issues of information security management during the state of martial. In *Current issues of security management during martial law: scientific monograph* (pp. 8–19). Vysoká škola bezpečnostného manažérstva v Košiciach.

Received: 11.08.2025
Accepted: 29.08.2025

Озарко К. С., Піх М. З. Проблеми та перспективи оцінювання інформаційної безпеки підприємств за динамічних умов господарювання

Стаття присвячена дослідженню проблем, потенційних можливостей оцінювання інформаційної безпеки підприємств за динамічних умов господарювання. На основі проведеного огляду наукових досліджень за тематикою можна виокремлено ключові проблеми оцінювання інформаційної безпеки. Запропоновано агреговану економіко-математичної моделі, яка включає розширений набір індикаторів, методику їх нормалізування, агрегування, формули для даних розрахунків, рекомендації щодо валідування і практичного впровадження/використання.

Ключові слова: інформація, дані, інформаційна безпека, кіберзагроза, воєнний стан, ризик, безпекова політика.

Ozarko K. S., Pikh M. Z. Problems and prospects of assessing the information security of enterprises under dynamic economic conditions

The article is devoted to the study of problems and potential opportunities for assessing the information security of enterprises in dynamic economic conditions. The research uses methods of analysis and synthesis. Based on a review of scientific research on the subject, key problems in assessing information security can be identified. An aggregated economic-mathematical model is proposed, which includes an extended set of indicators, methods for their normalisation and aggregation, formulas for these calculations, recommendations for validation and practical implementation/use.

The purpose of the proposed model is to obtain an integrated quantitative assessment of the level of information security of an enterprise (with an indication of the scale of this assessment, as a generally accepted option: from «0» to «100»), which will take into account technical, organisational, legal, human, operational (resilience) components and will be suitable for comparisons, monitoring and prioritisation of measures.

Assessing the information security of enterprises (at the enterprise level) in dynamic (and sometimes even highly dynamic) economic conditions requires a departure from traditional formal approaches and a gradual transition to comprehensive, adaptive, risk-oriented methodologies. An important task is to develop integrated indicators that reflect the level of security not only from a technical point of view, but also from an organisational, legal, personnel and other points of view. A promising area of research is the creation of a unified assessment methodology that will enable the comparison of different enterprises and the integration of information security assessment (the assessment process) into the overall economic security system. The implementation of these approaches will enable enterprises not only to identify and neutralise threats in a timely manner, but also to ensure long-term stability and competitiveness.

The expected results of implementation will be as follows: increased business resilience to external information threats, reduced risk of confidential information loss, protection of business reputation and customer bases, and increased trust among consumers, partners, investors and other stakeholders.

Keywords: information, data, information security, cyber threat, martial law, risk, security policy.