УДК 005.934:658.5:005.334:351.863

Р. Б. Лизун
ORCID 0009-0005-7848-1160

ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ МЕХАНІЗМІВ МЕНЕДЖМЕНТУ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

У статті обґрунтовано теоретичні засади формування механізмів менеджменту безпеки підприємств в умовах гібридних загроз. Доведено, що сучасне безпекове середовище характеризується високим рівнем невизначеності, турбулентності, нелінійністю ризиків, посиленням кіберзагроз, інформаційних впливів, логістичних дестабілізацій, кадрових і психологічних викликів. Обґрунтовано необхідність переходу від традиційного розуміння безпеки як захисту ресурсів до її трактування як інтегрованої системи управління адаптивною стійкістю підприємства. На основі аналізу сучасних зарубіжних і українських досліджень систематизовано наукові підходи до розуміння економічної безпеки, кіберстійкості, управління ризиками, антикризового управління, управління безперервністю бізнесу, організаційної резильєнтності та гібридних загроз. Запропоновано авторське трактування поняття «гібридні загрози підприємства» як комплексу взаємопов'язаних внутрішніх і зовнішніх дестабілізаційних впливів економічного, цифрового, інформаційного, психологічного, кадрового, організаційного та репутаційного характеру, які формують нелінійні ризики функціонування підприємства в умовах високої невизначеності. Сформульовано авторський підхід до визначення менеджменту безпеки підприємства як інтегрованої системи стратегічного, організаційного, кадрового, цифрового та адаптивного управління, спрямованої на забезпечення стійкості, здатності до швидкого реагування, відновлення та розвитку підприємства в умовах гібридних загроз. Визначено ключові механізми менеджменту безпеки підприємства: стратегічний, організаційний, ризик-орієнтований, кадровий, психологічний, цифровий, інформаційний, комунікаційний, антикризовий та адаптивно-резильєнтний. Запропоновано авторську архітектуру механізмів менеджменту безпеки підприємства в умовах гібридних загроз.

Ключові слова: *менеджмент безпеки, гібридні загрози, безпекоорієнтований менеджмент, підприємство, адаптивна стійкість, резильєнтність, ризик-менеджмент, кіберстійкість, антикризове управління, механізми менеджменту безпеки.*

DOI 10.34079/2518-1394-2026-16-31-31-44

Постановка проблеми. Сучасні умови функціонування підприємств характеризуються безпрецедентним рівнем турбулентності, нестабільності та невизначеності. Щодо підприємств в Україні, то повномасштабна війна, глобальні економічні кризи, цифровізація бізнес-середовища, кіберзагрози, руйнування логістичних ланцюгів, інформаційні атаки та психологічний тиск формують нову архітектуру ризиків, яка суттєво трансформує підходи до управління підприємствами. Тому, традиційні системи забезпечення безпеки, орієнтовані переважно на фізичний захист активів або мінімізацію фінансових ризиків, виявляються вже недостатньо ефективними. Особливої актуальності нині набуває проблема формування механізмів менеджменту безпеки підприємств в умовах гібридних загроз, адже гібридний характер сучасних викликів проявляється у поєднанні економічних, інформаційних, цифрових,

© Лизун Р. Б., 2026

психологічних, соціальних, кадрових та репутаційних впливів, які взаємодіють між собою та формують складну нелінійну систему ризиків. Отже, нині доцільно переходити від фрагментарного реагування на окремі загрози до формування інтегрованої системи безпекоорієнтованого менеджменту.

Метою статті є обґрунтування теоретичних засад та розроблення науково-методичного підходу до формування механізмів менеджменту безпеки підприємств в умовах гібридних загроз, спрямованих на забезпечення їх адаптивної стійкості, резильєнтності та ефективного функціонування в середовищі високої невизначеності.

Аналіз останніх досліджень і публікацій. Якщо подивитись на це питання у контексті сучасного наукового дискурсу, то значна увага приділяється питанням економічної безпеки підприємств, ризик-менеджменту, кризового управління, цифрової безпеки та резильєнтності організацій, проте, більшість досліджень зосереджується переважно на окремих аспектах безпеки, а це не дозволяє сформувати цілісне бачення механізмів менеджменту безпеки підприємств у контексті гібридних загроз. Крім того, недостатньо дослідженими, на нашу думку, залишаються питання інтеграції адаптивних, цифрових, психологічних та організаційних механізмів у єдину систему управління безпекою підприємства. Отже, актуальність зазначеної проблематики зумовлює необхідність розвитку теоретичних засад формування механізмів менеджменту безпеки підприємств в умовах гібридних загроз та обґрунтування сучасних управлінських підходів до забезпечення адаптивної стійкості підприємств.

Проведений нами аналіз низки літературних джерел дозволив зробити висновок, що проблематика менеджменту безпеки підприємств в умовах гібридних загроз формується на перетині кількох наукових напрямів: економічної безпеки підприємства, ризик-менеджменту, організаційної резильєнтності, кіберстійкості, антикризового управління, управління ланцюгами постачання та досліджень гібридних впливів.

Щодо зарубіжного наукового дискурсу останніх років, то помітним є зміщення акценту від традиційного розуміння безпеки як захисту активів до розуміння безпеки як здатності організації виявляти, поглинати, локалізувати та долати комплексні ризики. Зокрема, у дослідженні А. Бахманової, присвяченому систематичному аналізу кіберризиків, підкреслено, що сучасний кіберризик-менеджмент стикається з проблемою нестачі релевантних даних, складністю ідентифікації ризик-факторів, а також недостатньою залученістю вищого менеджменту до управління кіберстійкістю організації (Bahmanova, 2024). А це дає нам підстави говорити про те, що кіберзагрози в умовах гібридних впливів не можуть розглядатися лише як технічна проблема ІТ-відділу, а мають бути інтегровані в систему стратегічного менеджменту безпеки підприємства.

Дотичним до цього є дослідження Т. Д. Ле та співавторів, у якому здійснено систематичний огляд 65 рецензованих праць з проблематики аналітики кібербезпеки для корпоративного середовища (cybersecurity analytics for the enterprise environment), і в якому автори доводять, що зростання масштабу та складності кіберзагроз зумовлює потребу підприємств у аналітиці безпеки, заснованій на даних (data-driven security analytics) (Le, Nguyen and Tran, 2025). А це дає нам підстави зробити висновок, що для формування механізмів менеджменту безпеки необхідно переходити від інтуїтивного реагування на загрози до аналітично обґрунтованого, цифрово підтриманого управління ризиками.

Важливим є розгляд окремого напряму зарубіжних досліджень, який пов’язаний із управлінням ризиками кібербезпеки ланцюгів постачання (cyber supply chain risk management). Так, А. Латсіоу та співавтори фокусують увагу на тому, що сучасні організації дедалі більше залежать від зовнішніх постачальників технологій, сервісів і цифрових рішень, що формує нові вразливості у ланцюгах постачання (Latsiou et al., 2025). У контексті гібридних загроз це отримує особливого значення, оскільки

дестабілізація підприємства може відбуватися не лише через прямий вплив на нього, а й через ураження його партнерів, постачальників, логістичних операторів, цифрових платформ або фінансових посередників.

Практико-орієнтований вимір досліджуваної нами проблематики досить повно розкрито у звітах Європейського агентства з кібербезпеки (ENISA) щодо управління кіберкризами (cyber crisis management), де наголошено на необхідності підготовки організацій до кіберкриз, розвитку процедур координації, сценарного реагування, обміну інформацією та післякризового навчання (European Union Agency for Cybersecurity (ENISA), 2024). На нашу думку, для підприємств це означає, що менеджмент безпеки має включати не лише превентивні заходи, а й механізми кризової готовності, швидкого відновлення та організаційного навчання після інцидентів.

Проблематика гібридних загроз активно розглядається і в безпекових дослідженнях. Так, у праці Т. Хідашелі «Гібридні загрози та резильєнтність» («Hybrid Threats and Resilience») гібридні загрози визначаються як поєднання традиційних і сучасних методів впливу, зокрема інформаційної війни, кібератак і психологічних операцій, спрямованих на дестабілізацію об’єкта впливу (Khidasheli T., 2024). І хоча це дослідження має переважно макрорівневу та безпеково-політичну спрямованість, але його положення, на нашу думку, можуть бути адаптовані до рівня підприємства, оскільки сучасні компанії також стають об’єктами інформаційного, цифрового, економічного та психологічного тиску.

У цьому ж контексті важливою є робота О. Карпенко, присвячена європейському досвіду протидії гібридним загрозам для економічного відновлення України, в якій авторка систематизує категоріальний апарат дослідження гібридних загроз, акторів та інструментів протидії, а також окреслює напрями використання досвіду ЄС у процесі економічного відновлення України (Karpenko, 2024). На нашу думку, ця праця дозволяє пов’язати проблематику гібридних загроз не лише з національною безпекою, а й з економічною стійкістю, відновленням та управлінськими практиками.

Що стосується українських науковців, то їх дослідження останніх років дедалі ширше розкривають проблеми економічної безпеки підприємств в умовах війни, воєнного стану та системної нестабільності. Так, С. Лаптєв, досліджуючи вплив державної політики на економічну безпеку підприємств України в умовах воєнної дестабілізації, підкреслює, що державні рішення можуть як посилювати, так і послаблювати резильєнтність бізнесу (Laptiev & Zakharov, 2025), а це, у свою чергу, дозволяє розглядати менеджмент безпеки підприємства не ізольовано, а як систему, що взаємодіє з інституційним, регуляторним і політико-економічним середовищем.

У статті А. Загородньої «Економічна безпека підприємства: сучасні виклики та загрози» («Economic Security of the Enterprise: Modern Challenges and Threats») проаналізовано сучасні підходи до розуміння економічної безпеки підприємства та класифіковано загрози за джерелами, природою, ймовірністю реалізації та можливими наслідками (Zahorodnia and Fedorenko, 2024.). Цінність цієї праці, на нашу думку, полягає у систематизації загроз економічній безпеці, хоча вона потребує подальшого розширення через інтеграцію гібридних, цифрових, інформаційних і психологічних впливів.

Більш наближеним до логіки нашого дослідження ми вважаємо підхід І. П. Потапюк, який поглиблює теоретико-методичні засади окреслення загроз економічній безпеці підприємства, акцентує увагу на необхідності уточнення характеристик загроз, що є важливим для побудови класифікації гібридних загроз у діяльності підприємств (Потапюк, 2024). Разом з тим вважаємо, що подальшого розвитку потребує саме управлінський аспект — тобто не лише ідентифікація загроз, а й формування механізмів менеджменту безпеки.

Важливо зазначити, що у сучасних українських публікаціях воєнний стан розглядається як чинник, що суттєво посилює традиційні та гібридні загрози економічній безпеці підприємств. Зокрема, у дослідженнях останніх років зазначено, що воєнний стан загострює інформаційні маніпуляції, правові та регуляторні ризики, ринкові загрози, порушення бізнес-процесів і репутаційні втрати, що зумовлює потребу в адаптації інструментарію управління ризиками та підвищенні організаційної стійкості (Марценюк та Файфер, 2025; Любиченко, 2026), а це, на нашу думку, зайвий раз підтверджує актуальність переходу від вузького розуміння економічної безпеки до ширшої концепції менеджменту безпеки підприємства.

Привертає увагу той факт, що значне місце в українських дослідженнях приділено стратегічному управлінню економічною безпекою підприємств в умовах воєнного стану. Так, С. Співак розглядає удосконалення стратегії управління економічною безпекою підприємств крізь призму антикризового управління, ризиків, фінансової стійкості та стратегічного управління (Співак, Шерстюк та Юрик, 2025), що є важливим для обґрунтування стратегічного контуру механізмів менеджменту безпеки, однак його варто доповнити організаційними, цифровими, кадровими та комунікаційними складовими.

Перспективним є також екосистемний підхід до управління економічною безпекою підприємства. Зокрема, у статті (Марценюк та Файфер, 2025) удосконалено модель екосистеми управління економічною безпекою підприємства в умовах воєнної економіки та післявоєнного відновлення, де враховано фінансові, операційні, ризикові та зовнішні чинники, а також взаємодію підприємств, банків, уряду, міжнародних організацій, органів безпеки та військових структур. Вважаємо, що ця ідея важлива тим, що безпека підприємства не може розглядатися лише як внутрішня функція; вона формується у взаємодії з ширшою інституційною та партнерською екосистемою.

Дослідження з фінансової безпеки суб'єктів підприємництва в Україні в умовах гібридних війн також демонструють необхідність урахування взаємодії підприємства з контрагентами, ринками та зовнішнім середовищем. Так, Л. Яструбецька підкреслює, що фінансова безпека є важливою складовою економічної безпеки підприємства і має розглядатися з урахуванням спроможності суб'єкта реалізовувати власні інтереси у взаємодії з контрагентами (Яструбецька, 2022), а це означає, що такий підхід може бути використаний для розширення фінансового компонента механізму менеджменту безпеки в умовах гібридних загроз.

Таким чином, проведений нами аналіз сучасних зарубіжних і українських досліджень дозволяє виокремити кілька наукових тенденцій: по-перше, безпека підприємства дедалі частіше розглядається не як статичний стан захищеності, а як динамічна здатність до адаптації, відновлення та трансформації; по-друге, гібридні загрози вимагають переходу від фрагментарного управління окремими ризиками до інтегрованого менеджменту безпеки; по-третє, цифровізація, кіберризики, інформаційний вплив, логістичні розриви, кадрове виснаження та репутаційні атаки мають розглядатися як взаємопов'язані елементи єдиної системи загроз; по-четверте, сучасні дослідження ще недостатньо розкривають саме механізми менеджменту безпеки підприємств, тобто сукупність стратегічних, організаційних, цифрових, кадрових, психологічних, комунікаційних та адаптивно-резильєнтних інструментів управління.

Саме це і зумовлює необхідність подальшого обґрунтування теоретичних засад формування механізмів менеджменту безпеки підприємств в умовах гібридних загроз. Тому, метою статті є обґрунтування теоретичних засад формування механізмів менеджменту безпеки підприємств в умовах гібридних загроз та визначення ключових управлінських компонентів забезпечення адаптивної стійкості підприємства.

Виклад основного матеріалу дослідження. Сучасне середовище функціонування підприємств характеризується високим рівнем динамічності,

невизначеності та багатовекторності ризиків, а умови воєнного стану, цифровізація економіки, глобальна взаємозалежність бізнес-процесів, інформаційні війни, кіберзагрози та нестабільність міжнародних ринків формують нову архітектуру небезпек, яка суттєво відрізняється від традиційних уявлень про загрози економічній безпеці підприємства.

На нашу думку, однією з ключових особливостей сучасного безпекового середовища є гібридизація загроз і якщо раніше ризики здебільшого розглядалися як окремі локалізовані явища (фінансові, виробничі, кадрові чи інформаційні), то нині вони дедалі частіше поєднуються між собою, формуючи складні нелінійні системи впливу. Це дає підстави говорити про те, що саме така взаємодія різних видів ризиків і визначає сутність гібридних загроз.

У міжнародному безпековому дискурсі поняття Hybrid Warfare та hybrid threats тривалий час використовувалося переважно у сфері національної безпеки та геополітики, але сучасні умови демонструють, що об'єктами гібридного впливу дедалі частіше стають не лише держави, а й підприємства, організації, логістичні системи, фінансові установи, освітні заклади та цифрові платформи. На нашу думку, особливість гібридних загроз полягає у тому, що вони: мають багатокомпонентний характер; поєднують різні інструменти впливу; реалізуються одночасно у кількох середовищах; створюють каскадний ефект дестабілізації; посилюють одна одну; ускладнюють процес прогнозування та реагування. Крім того, варто зазначити, що на відміну від традиційних ризиків, гібридні загрози не мають чітких меж між зовнішнім і внутрішнім середовищем підприємства. Наприклад, кібератака може спричинити: фінансові втрати; інформаційну паніку; репутаційну кризу; психологічне виснаження персоналу; порушення логістики; втрату довіри партнерів і клієнтів тощо. Тобто, один дестабілізаційний вплив здатний активізувати цілий ланцюг взаємопов'язаних кризових процесів. Тому, вважаємо, що у сучасних умовах до основних проявів гібридних загроз у діяльності підприємств доцільно віднести: кіберзагрози; інформаційні маніпуляції; психологічний вплив на персонал; логістичні дестабілізації; фінансову нестабільність; репутаційні атаки; кадрові ризики; енергетичну нестабільність; регуляторні та правові ризики; кризові комунікаційні впливи.

Особливої актуальності проблема гібридних загроз набуває для українських підприємств в умовах війни, що зумовлено тим, що повномасштабна агресія спричинила не лише фізичні руйнування виробничої та логістичної інфраструктури, але й суттєво посилила інформаційний тиск, кіберризики, психологічне виснаження персоналу, нестабільність ринків, міграцію трудових ресурсів та невизначеність стратегічного планування. І як результат - підприємства змушені функціонувати в умовах постійної турбулентності та багаторівневої нестабільності. З огляду на це, важливого значення набуває розуміння гібридних загроз не лише як зовнішніх дестабілізаційних впливів, а як системного фактору трансформації управлінського середовища підприємства, адже гібридність проявляється не лише у множинності загроз, а й у зміні самої логіки управління, коли традиційні інструменти контролю та стабілізації стають недостатньо ефективними.

На основі вищевикладеного пропонуємо авторське трактування поняття «гібридні загрози підприємства» – це комплекс взаємопов'язаних внутрішніх і зовнішніх дестабілізаційних впливів економічного, цифрового, інформаційного, психологічного, кадрового, організаційного та репутаційного характеру, які формують нелінійні ризики функціонування підприємства в умовах високої невизначеності та потребують інтегрованих адаптивних механізмів менеджменту безпеки. Таке трактування, на нашу думку, дозволяє розширити традиційне розуміння безпеки підприємства та перейти від вузького підходу, орієнтованого переважно на захист ресурсів, до системного бачення

безпеки як здатності підприємства адаптуватися, зберігати функціональність, швидко реагувати на дестабілізаційні впливи та відновлювати свою діяльність.

Крім того, подальше узагальнення сучасних наукових підходів і практики функціонування підприємств в умовах війни дозволяє систематизувати основні види гібридних загроз (табл. 1).

Таблиця 1

Основні види гібридних загроз у діяльності підприємств

Вид загрози	Прояви	Потенційні наслідки
Кіберзагрози	кібератаки, злам систем, витік даних	порушення роботи систем, фінансові втрати
Інформаційні загрози	дезінформація, фейки, інформаційний тиск	репутаційні втрати, паніка
Психологічні загрози	стрес, тривожність, вигорання персоналу	зниження продуктивності, кадрові втрати
Логістичні загрози	руйнування ланцюгів постачання	зрив поставок, зупинка виробництва
Фінансові загрози	інфляція, валютна нестабільність	зниження платоспроможності
Кадрові загрози	дефіцит персоналу, міграція кадрів	зниження кадрового потенціалу
Репутаційні загрози	інформаційні атаки, скандали	втрата довіри клієнтів і партнерів
Енергетичні загрози	перебої електропостачання	порушення операційної діяльності
Правові та регуляторні загрози	зміна законодавства, санкційні ризики	додаткові витрати, управлінська нестабільність

Джерело: сформовано автором на основі (Latsiou et al., 2025; European Union Agency for Cybersecurity (ENISA), 2024; Khidasheli, 2024; Genini, 2025; Kott, Dubynskyi, Paziuk, Galaitsi, Trump and Linkov, 2024; Hasan, 2024)

Отже, гібридні загрози створюють принципово нові умови функціонування підприємств, у яких безпека вже не може розглядатися як окрема функція контролю чи захисту і при яких вона трансформується у складну інтегровану систему управління адаптивною стійкістю підприємства, що, у свою чергу, вимагає формування нових механізмів менеджменту безпеки. Саме це зумовлює необхідність переходу до безпекоорієнтованої моделі управління, заснованої на принципах адаптивності, резильєнтності, системності та інтегрованого управління ризиками.

Трансформація сучасного безпекового середовища зумовлює необхідність переосмислення традиційних підходів до управління безпекою підприємства, адже в умовах гібридних загроз безпека перестає бути виключно функцією захисту ресурсів або контролю ризиків і поступово перетворюється на інтегровану управлінську систему забезпечення адаптивної стійкості підприємства.

На нашу думку, традиційні концепції економічної безпеки підприємства здебільшого ґрунтувалися на ідеї підтримання стабільності, мінімізації загроз та захисту фінансово-економічних інтересів підприємства. Водночас сучасні умови функціонування бізнесу демонструють, що абсолютна стабільність стає практично недосяжною, а головною умовою виживання підприємства виступає його здатність швидко адаптуватися до змін, реагувати на кризові впливи та відновлювати функціонування після дестабілізаційних подій.

У цьому контексті важливого значення набуває розвиток Resilience Engineering, відповідно до якого організація розглядається як динамічна адаптивна система, здатна функціонувати в умовах невизначеності та турбулентності, а резильєнтність підприємства визначається не лише здатністю протистояти загрозам, але й умінням

навчатися, трансформувати внутрішні процеси та формувати нові механізми реагування. Тому, сучасний менеджмент безпеки дедалі більше інтегрує: ризик-менеджмент, управління безперервністю бізнесу; адаптивне управління; кібербезпеку; психологічну безпеку; антикризове управління; цифрову аналітику; комунікаційне управління; управління людським капіталом. А це, в свою чергу, свідчить про поступовий перехід від вузького трактування безпеки до безпекоорієнтованого менеджменту як системи стратегічного управління стійкістю підприємства. У межах традиційного підходу основна увага приділялася переважно: контролю загроз; збереженню ресурсів; забезпеченню стабільності; захисту інформації; фінансовій безпеці.

Однак у сучасних умовах підприємство змушене працювати не лише з відомими ризиками, а й із високим рівнем невизначеності, швидкими змінами зовнішнього середовища та нелінійними кризовими процесами, а це зумовлює необхідність формування адаптивної моделі менеджменту безпеки. Тому наступним кроком, для систематизації змін у підходах до управління безпекою підприємства, доцільно порівняти традиційну та сучасну управлінські моделі (табл. 2).

Таблиця 2

Трансформація підходів до менеджменту безпеки підприємства

Традиційний підхід	Сучасний безпекоорієнтований підхід
Реагування на загрози	Адаптація до невизначеності
Захист ресурсів	Забезпечення стійкості системи
Контроль	Резильєнтність
Ієрархічне управління	Гнучке адаптивне управління
Локальне управління ризиками	Інтегрований ризик-менеджмент
Фокус на фізичній безпеці	Комплексна безпека
Закритість інформації	Інформаційна адаптивність
Стабільність як мета	Динамічна стійкість як мета
Мінімізація втрат	Здатність до швидкого відновлення

Джерело: сформовано автором

Дані табл. 2 свідчать про те, що сучасний менеджмент безпеки підприємства набуває системного, інтегрованого та адаптивного характеру. У центрі уваги опиняється не лише протидія загрозам, а й формування організаційної здатності функціонувати в умовах нестабільності.

Особливу роль у цьому процесі відіграє людський фактор, що зумовлено тим, що у сучасних умовах персонал стає не лише об’єктом захисту, але й одним із ключових елементів системи безпеки підприємства. Психологічне виснаження, професійне вигорання, стрес, кадрова нестабільність та інформаційний тиск безпосередньо впливають на ефективність діяльності підприємства та його здатність реагувати на кризові ситуації. Відповідно, важливого значення набувають питання психологічної безпеки, яка передбачає формування середовища довіри, комунікаційної відкритості, підтримки та адаптивної взаємодії між працівниками, а у контексті гібридних загроз психологічна безпека персоналу стає складовою загальної системи менеджменту безпеки підприємства.

Крім того, сучасний менеджмент безпеки неможливо розглядати поза процесами цифровізації, адже використання цифрових платформ, хмарних сервісів, аналітики даних, автоматизованих систем управління та штучного інтелекту створює як нові можливості для підвищення ефективності безпеки, так і нові ризики, пов’язані з кіберзагрозами, витоком інформації та цифровою вразливістю підприємства.

У таких умовах менеджмент безпеки підприємства доцільно розглядати як багаторівневу систему управління, що охоплює: стратегічний рівень; організаційний рівень; кадровий рівень; цифровий рівень; інформаційно-комунікаційний рівень; антикризовий рівень; адаптивно-резильєнтний рівень.

Таким чином, на основі проведеного дослідження пропонуємо авторське трактування поняття «менеджмент безпеки підприємства» - це інтегрована система стратегічного, організаційного, кадрового, цифрового та адаптивного управління, спрямована на забезпечення стійкості, здатності до швидкого реагування, відновлення та розвитку підприємства в умовах гібридних загроз і високої невизначеності. Це, на нашу думку, дозволяє перейти від фрагментарного сприйняття безпеки до її розуміння як системоутворюючого елементу сучасного управління підприємством, а безпека у цьому випадку виступає не лише інструментом захисту, а й механізмом підтримання життєздатності, конкурентоспроможності та стратегічної адаптивності підприємства.

У свою чергу, варто зазначити, що складність і багатовекторність сучасних гібридних загроз зумовлюють необхідність формування комплексних механізмів менеджменту безпеки підприємств, здатних забезпечувати не лише захист ресурсів, а й підтримання адаптивної стійкості організації в умовах високої невизначеності. Особливість сучасних механізмів менеджменту безпеки полягає у тому, що вони повинні функціонувати в умовах постійної зміни середовища та непередбачуваності загроз, а це потребує переходу від жорстких ієрархічних систем контролю до гнучких моделей управління, заснованих на швидкому обміні інформацією, аналітичному прогнозуванні, кризовій готовності та здатності організації до швидкої адаптації. Тому, на нашу думку, у сучасних умовах доцільно виділити кілька ключових механізмів менеджменту безпеки підприємства, які і формуватимуть єдину інтегровану систему забезпечення стійкості організації (табл. 3).

Таблиця 3

Ключові механізми менеджменту безпеки підприємства в умовах гібридних загроз

Механізм	Основний зміст	Очікуваний ефект
Стратегічний	формування безпекової стратегії та сценарного планування	підвищення стратегічної стійкості
Організаційний	адаптація структури управління та бізнес-процесів	підвищення гнучкості управління
Ризик-орієнтований	ідентифікація, оцінка та моніторинг ризиків	зниження рівня невизначеності
Кадровий	розвиток компетентностей персоналу та кадрової стійкості	збереження людського капіталу
Психологічний	підтримка психологічної безпеки персоналу	зниження стресу та вигорання
Цифровий	забезпечення кіберстійкості та цифрового захисту	підвищення цифрової безпеки
Інформаційний	управління інформаційними потоками та протидія дезінформації	мінімізація інформаційних ризиків
Комунікаційний	кризові комунікації та взаємодія зі стейкхолдерами	підтримка довіри та репутації
Антикризовий	сценарне реагування та плани безперервності діяльності	швидке відновлення діяльності
Адаптивно-резильєнтний	розвиток здатності до трансформації та навчання	забезпечення довгострокової стійкості

Джерело: сформовано автором

Представлені механізми не існують ізольовано, а формують взаємопов’язану систему управління безпекою підприємства, а узагальнення проведеного дослідження дозволяє стверджувати, що ефективність менеджменту безпеки підприємства залежить не від окремих інструментів захисту, а від рівня інтеграції різних механізмів у єдину систему управління адаптивною стійкістю. Тому, доцільно представити авторське

бачення архітектури механізмів менеджменту безпеки підприємства в умовах гібридних загроз (рис. 1).

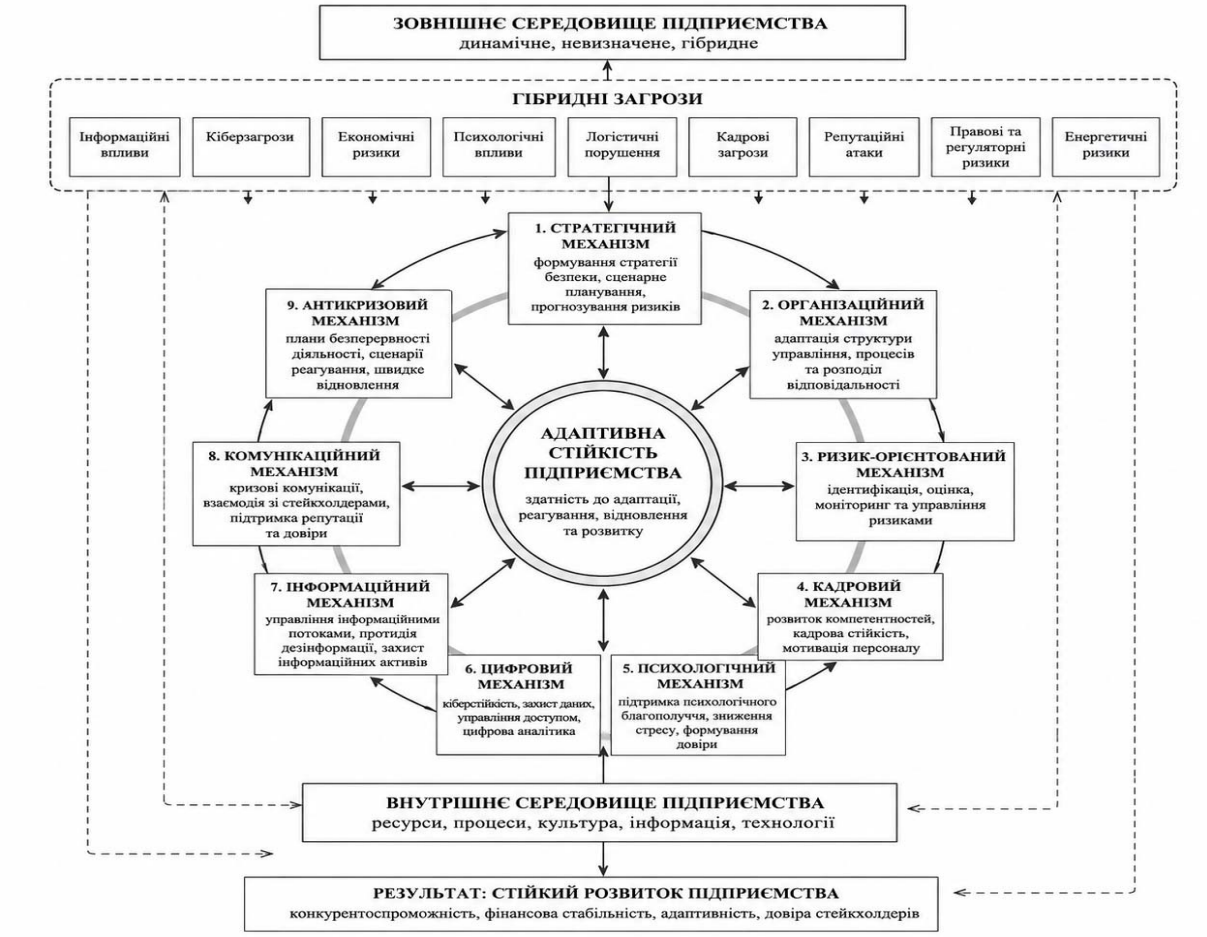

Рисунок 1. *Архітектура механізмів менеджменту безпеки підприємства в умовах гібридних загроз*

Джерело: сформовано автором

Представлена на рис. 1 архітектура механізмів менеджменту безпеки підприємства демонструє інтегрований характер сучасної системи управління безпекою в умовах гібридних загроз, яка на відміну від традиційних підходів, орієнтованих переважно на локалізацію окремих ризиків, ґрунтується на взаємодії стратегічних, організаційних, кадрових, цифрових, інформаційних та антикризових механізмів у межах єдиної системи забезпечення адаптивної стійкості підприємства. Центральним елементом моделі виступає адаптивна стійкість підприємства, яка визначає його здатність до реагування на дестабілізаційні впливи, швидкого відновлення функціонування та подальшого розвитку в умовах невизначеності.

При цьому кожен із представлених механізмів виконує окрему функцію в системі менеджменту безпеки, однак їх ефективність досягається саме через інтегровану взаємодію. Запропонована архітектура також відображає взаємозалежність внутрішнього та зовнішнього середовища підприємства: з одного боку, гібридні загрози формуються під впливом зовнішніх факторів (воєнних ризиків, цифрового середовища, інформаційного тиску, економічної нестабільності та регуляторних змін), з іншого боку, рівень стійкості підприємства визначається його внутрішніми характеристиками (організаційною структурою, кадровим потенціалом, рівнем цифровізації, корпоративною культурою та здатністю до кризового реагування). Крім того, важливою

особливістю запропонованої моделі є її адаптивний характер, що передбачає можливість трансформації механізмів менеджменту безпеки відповідно до змін безпекового середовища, що дозволяє розглядати менеджмент безпеки не як статичну систему захисту, а як динамічний управлінський процес, спрямований на підтримання довгострокової стійкості та конкурентоспроможності підприємства.

Висновки. Отже, за результатами проведеного дослідження, можна зробити такі висновки:

сучасне середовище функціонування підприємств характеризується високим рівнем невизначеності, нестабільності та багатовекторності ризиків, що зумовлює необхідність трансформації традиційних підходів до управління безпекою, а проведене дослідження дозволило обґрунтувати теоретичні засади формування механізмів менеджменту безпеки підприємств в умовах гібридних загроз та сформувати низку наукових висновків;

встановлено, що сучасні гібридні загрози мають комплексний характер і поєднують економічні, цифрові, інформаційні, психологічні, кадрові, логістичні та репутаційні впливи, які взаємодіють між собою та формують нелінійну систему ризиків для підприємства і на відміну від традиційних загроз, гібридні ризики характеризуються високою динамічністю, взаємозалежністю та складністю прогнозування, що суттєво ускладнює процес управління безпекою підприємства;

у результаті аналізу сучасних зарубіжних і українських наукових підходів встановлено, що більшість досліджень у сфері економічної безпеки, ризик-менеджменту, кіберстійкості та антикризового управління мають фрагментарний характер і переважно зосереджуються на окремих аспектах безпеки. Водночас сучасні умови функціонування підприємств потребують формування інтегрованого підходу до менеджменту безпеки, який би поєднував стратегічні, організаційні, кадрові, цифрові, інформаційні та адаптивно-резильєнтні механізми управління;

обґрунтовано, що сучасний менеджмент безпеки підприємства доцільно розглядати не лише як систему захисту ресурсів чи мінімізації загроз, а як інтегровану систему управління адаптивною стійкістю підприємства в умовах високої невизначеності при якій безпека виступає системоутворюючим елементом управління підприємством, що забезпечує його здатність до реагування, адаптації, відновлення та розвитку;

запропоновано авторське трактування поняття «гібридні загрози підприємства», під якими запропоновано розуміти комплекс взаємопов’язаних внутрішніх і зовнішніх дестабілізаційних впливів економічного, цифрового, інформаційного, психологічного, кадрового, організаційного та репутаційного характеру, які формують нелінійні ризики функціонування підприємства в умовах високої невизначеності та потребують інтегрованих адаптивних механізмів менеджменту безпеки;

сформульовано авторський підхід до трактування менеджменту безпеки підприємства як інтегрованої системи стратегічного, організаційного, кадрового, цифрового та адаптивного управління, спрямованої на забезпечення стійкості, здатності до швидкого реагування, відновлення та розвитку підприємства в умовах гібридних загроз;

визначено ключові механізми менеджменту безпеки підприємства в умовах гібридних загроз, серед яких: стратегічний; організаційний; ризик-орієнтований; кадровий; психологічний; цифровий; інформаційний; комунікаційний; антикризовий; адаптивно-резильєнтний механізми;

доведено, що ефективність менеджменту безпеки залежить не від окремих інструментів захисту, а від рівня інтеграції зазначених механізмів у єдину систему управління адаптивною стійкістю підприємства.

Практична цінність дослідження полягає у можливості використання запропонованих теоретичних положень для формування сучасних систем менеджменту

безпеки підприємств, розроблення стратегій забезпечення стійкості, удосконалення антикризового управління та адаптації підприємств до умов гібридних загроз, а перспективи подальших досліджень пов'язані з розробленням методичних підходів до оцінювання ефективності механізмів менеджменту безпеки підприємств, формуванням системи індикаторів адаптивної стійкості, побудовою моделей безпекоорієнтованого управління та дослідженням цифрових інструментів забезпечення резильєнтності підприємств в умовах воєнної та посткризової трансформації економіки.

Бібліографічний список

Любиченко, О.О., 2026. Інформаційна стійкість України в умовах гібридних загроз: теоретичні інтерпретації та український досвід. Державне управління: удосконалення та розвиток, 2, с. 77–89. DOI: http://doi.org/10.32702/2307-2156.2026.2.23 (Дата звернення 28.01.2026).

Марценюк, Л. В. та Файфер, С. М., 2025. Комплексний підхід до створення бізнес-екосистеми економічної безпеки підприємств України в умовах воєнної економіки та післявоєнного відновлення. *Агросвіт*, 4, с. 56-63. DOI: https://doi.org/10.32702/2306-6792.2025.4.56 (дата звернення: 28.01.2026).

Потапюк, І. П., 2024. Теоретико-методичні засади визначення загроз економічній безпеці підприємства. *Проблеми менеджменту та інформаційних технологій*, 13, с. 54–63. DOI: https://doi.org/10.54929/2786-5738-2024-13-04-07 (дата звернення: 28.01.2026).

Співак, С., Шерстюк, Р., та Юрик, Н., 2025. Удосконалення стратегії управління економічною безпекою підприємства в умовах воєнного стану. *Галицький економічний вісник*, 97(6), с. 211-217. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2025.06.211 (Дата звернення 28.01.2026).

Яструбецька, Л. С., 2022. *Фінансова безпека суб'єктів підприємництва в Україні в умовах гібридних загроз: монографія.* Львів : ЛНУ ім. Івана Франка. Доступно: <https://econom.lnu.edu.ua/wp-content/uploads/2016/09/Financial-SecurityHybrid-Wars_Yastrubetska.pdf (Дата звернення: 28.01.2026).

Bahmanova, A., 2024. Cyber Risk Management: A Systematic Literature Review. *Proceedings of the International MultiConference of Engineers and Computer Scientists*, p. 115–122. DOI: https://doi.org/10.54808/JSCI.22.02.37 (Accessed 28.01.2026).

Beska, S., 2025. *Cyber Resilience in Ukraine.* Budapest : Central European University, 94 p. Available at: <Cyber Resilience in Ukraine> (Accessed 28.01.2026).

European Union Agency for Cybersecurity (ENISA), 2024. *Best Practices in Cyber Crisis Management*. Athens : ENISA, 87 p. DOI: https://doi.org/10.2824/767828 (Accessed 28.01.2026).

Genini, D., 2025. Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives*, 33(2), p. 122–149. DOI: https://doi.org/10.1177/2336825X251322719 (Accessed 28.01.2026).

Hasan, M., 2024. Enhancing Enterprise Security with Zero Trust Architecture. ArXiv:2410.18291. DOI: https://doi.org/10.48550/arXiv.2410.18291 (Accessed 28.01.2026).

Karpenko, O., 2024. European Experience in Countering Hybrid Threats for Ukraine's Economic Recovery. *International Economic Policy*, 41, p. 188–207. DOI: https://www.doi.org/10 .33111/iep.eng.2024.41.12 (Accessed 28.01.2026).

Khidasheli, T., 2024. Hybrid Threats and Resilience. Tbilisi : Friedrich Naumann Foundation, 54 p. Available at: <https://www.freiheit.org/sites/default/files/2024-12/hybrid-threats-and-resilience-final.pdf> (Accessed 28.01.2026).

Kott, A., Dubynskyi, G. Y., Paziuk, A., Galaitsi, S. E., Trump, B. D. and Linkov, I., 2024. Russian Cyber Onslaught was Blunted by Ukrainian Cyber Resilience. *Computer*, 57(8), p. 82–89 DOI: 10.1109/MC.2024.3404568 (Accessed 28.01.2026).

Laptiev, S., & Zakharov, O., 2025. The impact of state policy on the economic security of enterprises in Ukraine: current challenges and strategic responses. *Economics, Finance and Management Review*, 1(21), 29–42. DOI: https://doi.org/10.36690/2674-5208-2025-1-29-42 (Accessed 28.01.2026).

Latsiou, A. et al, 2025. Cyber Supply Chain Risk Management: Emerging Threats and Enterprise Security Challenges. *International Journal of Information Security*, 24, p. 1–18. DOI: https://doi.org/10.1007/s10207-025-01207-9 (Accessed 28.01.2026).

Le, T. D., Nguyen, H. and Tran, P., 2025. Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. Electronics, 14(11), Article 2252. DOI: https://doi.org/10.3390/electronics14112252 (Accessed 28.01.2026).

Zahorodnia, A. B. and Fedorenko, T., 2024. Economic Security of the Enterprise: Modern Challenges and Threats. *SMART SCM: Supply Chain Management Solutions*, 26, P. 45–53. DOI: https://doi.org/10.46783/smart-scm/2024-26-6 (Accessed 28.01.2026).

References

Liubychenko O. O. Informatsiina stiikist Ukrainy v umovakh hibrydnykh zahroz: teoretychni interpretatsii ta ukrainskyi dosvid [Information resilience of Ukraine under hybrid threats: Theoretical interpretations and Ukrainian experience]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok,* 2, c. 77–89. DOI: http://doi.org/10.32702/2307-2156.2026.2.23 (Accessed 28.01.2026) (in Ukrainian).

Martsenyuk L. V. and Faifer S. M., 2025. Kompleksnyi pidkhid do stvorennia biznes-ekosystemy ekonomichnoi bezpeky pidpryiemstv Ukrainy v umovakh voiennoi ekonomiky ta pisliavoiennoho vidnovlennia [A comprehensive approach to creating a business ecosystem of economic security of Ukrainian enterprises in wartime and post-war recovery]. *Ahrosvit,* 4, p. 56-63. DOI: https://doi.org/10.32702/2306-6792.2025.4.56 (Accessed 28.01.2026) (in Ukrainian).

Potapiuk, I. P., 2024. Teoretyko-metodychni zasady vyznachennia zahroz ekonomichnii bezpetsi pidpryiemstva [Theoretical and methodological principles of identifying threats to economic security of enterprises]. *Problemy menedzhmentu ta informatsiinykh tekhnolohii*, 13, c. 54–63. DOI: https://doi.org/10.54929/2786-5738-2024-13-04-07 (Accessed 28.01.2026) (in Ukrainian).

Spivak, S., Sherstiuk, R. and Yuryk, N., 2025. Udoskonalennia stratehii upravlinnia ekonomichnoiu bezpekoiu pidpryiemstva v umovakh voiennoho stanu [Improvement of enterprise economic security management strategy under martial law]. *Halytskyi ekonomichnyi visnyk*, 97(6), c. 211-217. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2025.06.211 (Accessed 28.01.2026) (in Ukrainian).

Yastrubetska, L. S., 2022. Finansova bezpeka subiektiv pidpryiemnytstva v Ukraini v umovakh hibrydnykh zahroz [Financial security of business entities in Ukraine under hybrid threats]. Lviv: Ivan Franko National University. Available at: <https://econom.lnu.edu.ua/wp-content/uploads/2016/09/Financial-SecurityHybrid-Wars_Yastrubetska.pdf (Accessed 28.01.2026) (in Ukrainian).

Bahmanova, A., 2024. Cyber Risk Management: A Systematic Literature Review. *Proceedings of the International MultiConference of Engineers and Computer Scientists*, p. 115–122. DOI: https://doi.org/10.54808/JSCI.22.02.37 (Accessed 28.01.2026).

Beska, S., 2025. *Cyber Resilience in Ukraine.* Budapest : Central European University, 94 p. Available at: <Cyber Resilience in Ukraine> (Accessed 28.01.2026).

European Union Agency for Cybersecurity (ENISA), 2024. *Best Practices in Cyber Crisis Management*. Athens : ENISA, 87 p. DOI: https://doi.org/10.2824/767828 (Accessed 28.01.2026).

Genini, D., 2025. Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives*, 33(2), p. 122–149. DOI: https://doi.org/10.1177/2336825X251322719 (Accessed 28.01.2026).

Hasan, M., 2024. Enhancing Enterprise Security with Zero Trust Architecture. ArXiv:2410.18291. DOI: https://doi.org/10.48550/arXiv.2410.18291 (Accessed 28.01.2026).

Karpenko, O., 2024. European Experience in Countering Hybrid Threats for Ukraine's Economic Recovery. *International Economic Policy*, 41, p. 188–207. DOI: https://www.doi.org/10 .33111/iep.eng.2024.41.12 (Accessed 28.01.2026).

Khidasheli, T., 2024. Hybrid Threats and Resilience. Tbilisi : Friedrich Naumann Foundation, 54 p. Available at: <https://www.freiheit.org/sites/default/files/2024-12/hybrid-threats-and-resilience-final.pdf> (Accessed 28.01.2026).

Kott, A., Dubynskyi, G. Y., Paziuk, A., Galaitsi, S. E., Trump, B. D. and Linkov, I., 2024. Russian Cyber Onslaught was Blunted by Ukrainian Cyber Resilience. *Computer*, 57(8), p. 82–89 DOI: 10.1109/MC.2024.3404568 (Accessed 28.01.2026).

Laptiev, S., & Zakharov, O., 2025. The impact of state policy on the economic security of enterprises in Ukraine: current challenges and strategic responses. *Economics, Finance and Management Review*, 1(21), 29–42. DOI: https://doi.org/10.36690/2674-5208-2025-1-29-42 (Accessed 28.01.2026).

Latsiou, A. et al, 2025. Cyber Supply Chain Risk Management: Emerging Threats and Enterprise Security Challenges. *International Journal of Information Security*, 24, p. 1–18. DOI: https://doi.org/10.1007/s10207-025-01207-9 (Accessed 28.01.2026).

Le, T. D., Nguyen, H. and Tran, P., 2025. Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. Electronics, 14(11), Article 2252. DOI: https://doi.org/10.3390/electronics14112252 (Accessed 28.01.2026).

Zahorodnia, A. B. and Fedorenko, T., 2024. Economic Security of the Enterprise: Modern Challenges and Threats. *SMART SCM: Supply Chain Management Solutions*, 26, P. 45–53. DOI: https://doi.org/10.46783/smart-scm/2024-26-6 (Accessed 28.01.2026).

Lyzun R. B.

THEORETICAL FOUNDATIONS OF FORMING SECURITY MANAGEMENT MECHANISMS OF ENTERPRISES UNDER HYBRID THREATS CONDITIONS

The article substantiates the theoretical foundations for the formation of enterprise security management mechanisms under conditions of hybrid threats. The relevance of the study is determined by the transformation of the modern business environment, which is characterized by a high level of uncertainty, turbulence, nonlinearity of risks, digitalization of business processes, the intensification of cyber threats, information influence, logistics disruptions, personnel instability, psychological pressure and reputational risks. It is argued that traditional approaches to enterprise security, focused mainly on resource protection, financial stability or response to individual threats, are no longer sufficient in the context of multidimensional and interconnected risks. The purpose of the article is to substantiate the theoretical foundations for the formation of enterprise security management mechanisms under conditions of hybrid threats and to identify the key managerial components of ensuring the adaptive resilience of an enterprise. Based on the analysis of contemporary foreign and

Ukrainian scientific literature, the article systematizes approaches to economic security, risk management, cyber resilience, crisis management, business continuity management, organizational resilience and hybrid threats. The study shows that hybrid threats should be considered not only as external destabilizing influences, but also as a systemic factor transforming the logic of enterprise management. The author proposes an interpretation of "hybrid threats to an enterprise" as a complex of interrelated internal and external destabilizing influences of economic, digital, informational, psychological, personnel-related, organizational and reputational nature, which generate nonlinear risks to enterprise functioning under conditions of high uncertainty and require integrated adaptive security management mechanisms. The article also formulates the author's approach to defining enterprise security management as an integrated system of strategic, organizational, personnel-related, digital and adaptive management aimed at ensuring resilience, rapid response capability, recovery and development of an enterprise under conditions of hybrid threats. The key mechanisms of enterprise security management are identified and substantiated, including strategic, organizational, risk-oriented, personnel-related, psychological, digital, informational, communication, crisis-management and adaptive-resilient mechanisms. The article emphasizes that the effectiveness of enterprise security management depends not on the isolated application of individual protection tools, but on the level of integration of these mechanisms into a single system for managing adaptive resilience. The author's architecture of enterprise security management mechanisms under conditions of hybrid threats is proposed. The practical value of the study lies in the possibility of using the proposed theoretical provisions for developing security-oriented management systems, improving crisis management and increasing the resilience of enterprises in wartime and post-crisis economic transformation.

Keywords: *security management, hybrid threats, security-oriented management, enterprise, adaptive resilience, organizational resilience, risk management, cyber resilience, crisis management, business continuity management, enterprise security management mechanisms.*

Стаття надійшла до редакції: 02.03.2026.
Прийнято до публікації: 23.03.2026 р.