

УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВІЗАЦІЇ

Сучасний етап розвитку світової економіки характеризується стрімкою цифровою трансформацією, яка докорінно змінює підходи до ведення бізнесу та створює принципово нові виклики для економічної безпеки підприємств. Цифровізація, охоплюючи всі сфери господарської діяльності, не лише відкриває нові можливості для оптимізації бізнес-процесів та підвищення конкурентоспроможності, але й формує складний комплекс загроз, що потребують переосмислення традиційних механізмів забезпечення економічної безпеки.

Ефективне управління економічною безпекою в умовах цифровізації потребує комплексного та системного підходу, що інтегрує технологічні, організаційні та стратегічні аспекти. Стратегічний рівень управління передбачає інтеграцію питань економічної безпеки в загальну цифрову стратегію підприємства. Це означає, що рішення щодо впровадження нових технологій, вибору цифрових партнерів або трансформації бізнес-моделі мають прийматися з обов'язковим урахуванням їхнього впливу на економічну безпеку. Цифрова стратегія має формуватися не як автономний напрям розвитку, а як органічна частина загальної стратегії підприємства, де цілі цифровізації узгоджуються з цілями забезпечення довгострокової стійкості та безпеки бізнесу [1].

Технології аналітики великих даних та штучного інтелекту відкривають нові можливості для превентивного виявлення загроз економічній безпеці. Системи моніторингу в реальному часі здатні аналізувати величезні обсяги даних, виявляти зміни у фінансових операціях, ідентифікувати підозрілу активність користувачів та прогнозувати потенційні ризики. Блокчейн-технології створюють нові можливості для забезпечення прозорості та незмінності критичних даних, що є особливо важливим для управління ланцюгами постачання, верифікації контрагентів та запобігання шахрайству [2].

Організаційний вимір управління економічною безпекою передбачає формування адекватної організаційної структури та системи управління ризиками. Традиційна модель, коли питання безпеки є виключною відповідальністю профільного підрозділу, не відповідає вимогам цифрової епохи. Натомість необхідна інтеграція функцій забезпечення економічної безпеки у всі бізнес-процеси та формування культури безпеки, де кожен співробітник усвідомлює свою роль у захисті економічних інтересів підприємства. Це вимагає створення системи розподілених повноважень та відповідальності, коли власники бізнес-процесів несуть безпосередню відповідальність за безпеку у своїх функціональних зонах, а централізовані служби безпеки виконують координуючі, методологічні та контрольні функції.

Система управління ризиками в умовах цифровізації має бути побудована на принципах безперервності та динамічності. Традиційні підходи, що передбачають періодичну оцінку ризиків та статичне планування заходів реагування, не встигають за темпами змін у цифровому середовищі. Натомість необхідна система постійного моніторингу ризиків, що використовує автоматизовані інструменти збору та аналізу інформації про потенційні загрози, оперативно актуалізує оцінку ризиків та забезпечує гнучке коригування захисних заходів відповідно до змін у зовнішньому та внутрішньому середовищі.

Управління людським капіталом набуває особливого значення в контексті економічної безпеки цифрового підприємства. Недостатній рівень цифрової грамотності персоналу є однією з головних вразливостей, адже навіть найдосконаліші технічні засоби захисту можуть бути скомпрометовані через помилки або недбалість користувачів. Це актуалізує необхідність систематичних програм підвищення цифрової та кіберграмотності, що охоплюють не лише технічні аспекти безпечної роботи з цифровими інструментами, але й формують відповідальне ставлення до корпоративних даних та розуміння економічних наслідків інцидентів безпеки [4].

Стратегія управління талантами має враховувати критичну важливість залучення та утримання фахівців у сфері інформаційної безпеки, аналітики даних та цифрових технологій. Дефіцит кваліфікованих спеціалістів у цих сферах створює серйозні виклики для підприємств, особливо малого та середнього бізнесу, що не можуть конкурувати з великими корпораціями за рівнем винагороди. Це вимагає інноваційних підходів до розвитку внутрішніх талантів, партнерства з освітніми закладами, залучення зовнішніх експертів на проєктній основі та створення привабливої корпоративної культури, що компенсує можливі обмеження у рівні матеріальної мотивації.

Фінансовий аспект забезпечення економічної безпеки в умовах цифровізації потребує збалансованого підходу до інвестицій у захисні механізми. Підприємства стикаються з дилемою між необхідністю значних інвестицій у цифрову безпеку та обмеженістю ресурсів. Вирішення цього протиріччя лежить у площині ризик-орієнтованого підходу, що передбачає концентрацію ресурсів на захисті найбільш критичних активів та процесів, використання економічно ефективних рішень на основі хмарних технологій та аутсорсингу окремих функцій безпеки, а також розгляд інвестицій у безпеку не як витрат, а як необхідного елементу створення довгострокової вартості бізнесу.

Взаємодія із зовнішніми стейкхолдерами є важливим елементом системи управління економічною безпекою в цифрову епоху. Цифровізація робить підприємства все більш взаємозалежними, коли безпека окремої організації значною мірою визначається безпекою її партнерів, постачальників та інших учасників цифрової екосистеми. Це актуалізує необхідність формування вимог до рівня цифрової безпеки контрагентів, включення відповідних застережень у договірні відносини, проведення аудитів безпеки партнерів та участі у галузевих ініціативах з обміну інформацією про загрози та кращі практики захисту.

Виміри ефективності системи управління економічною безпекою в умовах цифровізації потребують комплексного підходу, що поєднує фінансові та нефінансові показники. Традиційні метрики, такі як кількість

інцидентів безпеки або час реагування на інциденти, мають доповнюватися показниками, що відображають стратегічний вплив заходів безпеки на бізнес. Це може включати оцінку впливу інцидентів на репутацію підприємства, аналіз втрат від простоїв систем через кібератаки, вимірювання рівня довіри клієнтів до захисту їхніх даних або оцінку конкурентних переваг, отриманих завдяки вищому рівню цифрової зрілості та безпеки порівняно з конкурентами.

Перспективи розвитку систем управління економічною безпекою визначаються еволюцією самих цифрових технологій. Поширення штучного інтелекту та машинного навчання відкриває можливості для створення автономних систем захисту, здатних самостійно виявляти, класифікувати та нейтралізувати загрози без втручання людини. Водночас це породжує нові виклики, пов'язані з потенційною вразливістю самих систем штучного інтелекту до маніпуляцій та необхідністю збереження людського контролю над критичними рішеннями у сфері безпеки.

Розвиток квантових обчислень несе в собі як загрози, так і можливості для економічної безпеки. З одного боку, поява потужних квантових комп'ютерів може зробити вразливими існуючі криптографічні системи, що становить фундаментальну загрозу для конфіденційності та цілісності даних. З іншого боку, квантові технології відкривають можливості для створення принципово нових, більш надійних систем захисту інформації. Підприємствам необхідно вже зараз готуватися до постквантової епохи, відстежуючи розвиток квантово-стійких криптографічних алгоритмів та плануючи поступову міграцію своїх систем безпеки.

Інтернет речей та гіперконективність створюють нову конфігурацію загроз, коли потенційна поверхня атаки розширюється за рахунок множини підключених пристроїв, багато з яких мають обмежені можливості захисту. Управління безпекою у світі, де фізичні та цифрові процеси тісно інтегровані, вимагає нових підходів, що враховують специфіку промислових систем, критичної інфраструктури та розподілених мереж пристроїв.

Соціальні та етичні аспекти цифровізації також мають враховуватися в системі управління економічною безпекою. Збір та використання великих обсягів даних про клієнтів, працівників та інших стейкхолдерів ставить питання про межі допустимого моніторингу та використання інформації. Підприємства мають знаходити баланс між необхідністю захисту своїх економічних інтересів та повагою до приватності індивідів, формуючи етичні принципи роботи з даними, що відповідають не лише формальним юридичним вимогам, але й соціальним очікуванням та цінностям [3].

Таким чином, управління економічною безпекою підприємства в умовах цифровізації являє собою складний, багатовимірний процес, що вимагає інтеграції технологічних, організаційних, фінансових та стратегічних аспектів. Успішність цього процесу визначається здатністю підприємства не лише реагувати на поточні загрози, але й передбачати майбутні виклики, адаптувати свої стратегії та операційні моделі до динамічного цифрового середовища та перетворювати потенційні ризики цифровізації на джерела конкурентних переваг. Це вимагає формування нової організаційної культури, де питання економічної безпеки інтегровані у всі бізнес-процеси, а цифрова трансформація розглядається не як окремий проект, а як безперервний процес еволюції підприємства відповідно до вимог цифрової епохи.

Список використаних джерел:

1. Бугріменко Р., Смірнова П. Вплив розвитку цифрової трансформації на діяльність підприємства. Економіка та суспільство. 2024. № 59. DOI: <https://doi.org/10.32782/2524-0072/2024-59-29>
2. Глушко А.Д., Янко А.С., Білько С.С. Цифрова трансформація бізнес-процесів: безпековий аспект. Цифрова економіка та економічна безпека. 2025. № 2 (17). С. 160-166. DOI: <https://doi.org/10.32782/dees.17-22>
3. Кульчицький І.І. Цифрова економіка та економічна безпека підприємства: стратегії управління. Актуальні питання економічних наук. 2024. DOI: <https://doi.org/10.32782/a-economics.2024.123>
4. Шостак Л.В., Федонюк А.А., Помазун О.О. Особливості кібербезпеки бізнесу в умовах воєнного часу. Цифрова економіка та економічна безпека. 2024. № 3 (12). С. 121-125. DOI: <https://doi.org/10.32782/dees.12-22>