Міністерство освіти і науки України

Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки,
управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали X Міжнародної
науково-практичної конференції

13 травня 2026 р.

Полтава
2026

УДК 005.922.1:004.056

Кудінова Аліна Олександрівна,
кандидат економічних наук, доцент
Костенко Софія Сергіївна, *студентка*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ОСОБЛИВОСТІ УПРАВЛІННЯ ЦИФРОВОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ В СУЧАСНИХ УМОВАХ ГОСПОДАРЮВАННЯ

Сучасні умови господарювання продукують зміни підходів до управління цифровою безпекою організації. Проведені дослідження засвідчують, що системна проблема сучасного менеджменту полягає у критичному розриві між наявністю технічних інструментів захисту та відсутністю цілісної моделі управління. Технологічні рішення (firewalls, антивірусне ПЗ, системи шифрування) часто впроваджуються фрагментарно, без інтеграції в єдину систему захисту, де технології, регламенти, людська поведінка та корпоративні цінності мають функціонувати як синергетична система.

Основними деструктивними факторами, що перешкоджають побудові ефективної системи цифрової безпеки організації можна виділити наступні:

1) методологічна фрагментарність (відсутність єдиної політики безпеки та актуальних моделей ризиків);

2) унеузгодженість (слабка кореляція між IT-департаментами та стратегічним менеджментом);

3) людський фактор (низька цифрова компетентність персоналу та відсутність культури кібергігієни, що створює передумови для ненавмисних витоків конфіденційної інформації);

4) юридичні та комплаєнс-ризики (невідповідність внутрішніх регламентів динамічним змінам у цифровому законодавстві) [1].

Таким чином, підходи до управління цифровою безпекою організації повинні базуватися на переході від реактивного «латання дірок» до проактивного проєктування цифрової стійкості, що вимагає обґрунтування методики, яка б інтегрувала технічні параметри захисту з управлінськими алгоритмами прийняття рішень, створюючи надійний контур безпеки організації в умовах глобальних викликів [2].

Ефективна система цифрової безпеки організації базується на синергетичній взаємодії суб'єктів та об'єктів управління. У цій структурі вище керівництво визначає стратегічний вектор та розробляє політики, персонал виступає безпосереднім виконавцем цих регламентів, а IT-підрозділи забезпечують технологічну реалізацію захисних заходів. Важливу роль відіграє також зовнішня експертиза, яка дозволяє організації інтегрувати передовий досвід та оперативно реагувати на динамічні зміни цифрового ландшафту [3].

У межах практичної реалізації інформаційна безпека організації забезпечується набором конкретних процедур та інструментів, що захищають корпоративні ресурси на фізичному, мережевому та програмному рівнях. Ключові елементи, що формують техніко-технологічний контур цифрової безпеки, представлені у табл. 1.

Критично важливим аспектом управління є безперервність процесу впровадження та оновлення цифрових рішень, що передбачає не лише регулярну модернізацію програмних продуктів та інформаційних систем, а й системне планування навчання персоналу. Формування нових цифрових навичок та компетенцій є необхідною умовою для покращення якості роботи працівників та підвищення загальної результативності організації.

Таблиця 1

Ключові елементи цифрової безпеки організації

Елемент	Сутність
Захист ПЗ	Політики, процедури, інструменти і практичні поради щодо захисту програм і даних, які містяться в них.
Криптографія	Заснований на алгоритмі метод забезпечення захищеного спілкування полягає в тому, що певне повідомлення можуть переглядати та дешифрувати лише конкретні одержувачі.
Аварійне відновлення	Метод відновлення функціональних технологічних систем після стихійних лих, кібератак або інших порушень.
Реагування на інциденти	План організації для реагування на кібератаки, порушення безпеки даних та інші загрози, керування ними й усунення їхніх наслідків.
Убезпечення інфраструктури	Безпека всієї технологічної інфраструктури організації, зокрема систем апаратного й програмного забезпечення.
Керування вразливостями	Процес виявлення, оцінювання й усунення вразливостей у кінцевих точках, програмному забезпеченні та системах організації.

Джерело: побудовано авторами на основі [5, 6]

Критично важливим аспектом управління є безперервність процесу впровадження та оновлення цифрових рішень, що передбачає не лише регулярну модернізацію програмних продуктів та інформаційних систем, а й системне планування навчання персоналу. Формування нових цифрових навичок та компетенцій є необхідною умовою для покращення якості роботи працівників та підвищення загальної результативності організації.

Фактично, мова йде про трансформацію самої культури ведення бізнесу. Зміна форматів діяльності, особливо у сферах, орієнтованих на безпосередню взаємодію зі споживачем, вимагає від підприємства високої швидкості адаптації. Впровадження інноваційних цифрових систем дозволяє гнучко реагувати на ринкові реалії, проте ефективність цих технологій прямо залежить від здатності персоналу та внутрішніх процесів своєчасно підлаштовуватися під динамічні зміни зовнішнього та внутрішнього середовища [4].

Отже, проведений аналіз дозволяє констатувати, що управління цифровою безпекою сучасної організації має трансформуватися з суто технічної функції IT-відділу у стратегічний пріоритет загального менеджменту. Ефективність захисту корпоративного середовища в сучасних умовах господарювання залежить не стільки від потужності інструментів шифрування чи аварійного відновлення, скільки від здатності керівництва подолати методологічну фрагментарність та забезпечити синергію між технологічними рішеннями та культурою кібергігієни персоналу. Впровадження комплексного підходу, що інтегрує захист програм, хмарну безпеку та керування вразливостями, у поєднанні з безперервним навчанням співробітників, створює умови для формування проактивної цифрової стійкості, що дозволяє підприємству не лише мінімізувати ризики витоку інформації, а й гнучко адаптувати бізнес-модель до динамічних викликів цифровізації, забезпечуючи сталий розвиток та конкурентоспроможність у довгостроковій перспективі.

Література

1. Toward effective cybersecurity management: a systematic review of the literature / M. Liu et al. *Journal of Cybersecurity*. 2021. Vol. 7, Iss. 1. DOI: https://doi.org/10.1093/cybsec/tyaf020.

2. Obitade P. Big data analytics and cyber protection in organizations: A theoretical framework. *Journal of Big Data*. 2020. Vol. 7, Iss. 1. 17 p. DOI: https://doi.org/10.1186/s40537-019-0229-9.

3. Latsiou A., Lambrinoudakis C. Cyber supply chain risk management: a systematic literature review and future research directions. *International Journal of Information Security*. 2025. DOI: https://doi.org/10.1007/s10207-025-01207-9.

4. Величко К. Ю., Цибульська Є. І., Овчаренко К. В. Трансформація бізнес-моделей суб'єктів економічних відносин в цифровій економіці. *Вчені записки ХГУ «НУА»*. 2022. Том 29. С. 157–170.

5. Марченко О. В., Краус Н. М., Краус К. М. Інноваційне підприємництво і цифровий бізнес: науково-економічна фіча розвитку та зміни в управлінні. *Ефективна економіка*. 2020. № 4. URL: https://surl.li/kizpwa.

6. Ломачинська І. А., Войцеховська А. П., Чуркіна І. Є. Трансформація бізнес-моделей підприємницької діяльності в умовах цифровізації економіки та фінансового сектору. *Ринкова економіка: сучасна теорія і практика управління*. 2021. Т. 20, № 3(49). С. 97–113.

7. Onyshchenko S., Zhyvylo Ye., Hlushko A., Bilko S. Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. Vol. 5. P. 136–142. DOI: https://doi.org/10.33271/nvngu/2024-5/136.

УДК 658.15

Свистун Людмила Анатоліївна,
кандидат економічних наук, доцент,
Десятерик Софія Станіславівна,
студентка
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

РОЛЬ АНТИКРИЗОВОГО УПРАВЛІННЯ ТА ЙОГО ІНСТРУМЕНТІВ У ЗАБЕЗПЕЧЕННІ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Забезпечення фінансової безпеки підприємств в умовах воєнного стану та тривалої економічної кризи є однією з центральних наукових і прикладних проблем сучасної науки. Алкема В. констатує, що «нестабільне економічне середовище формує принципово нові виклики для управлінських систем підприємств, оскільки традиційні методи фінансового управління виявляються неадаптованими до умов багаторівневої невизначеності» [1, с. 145]. Це і є ключова наукова проблема: існуючий інструментарій антикризового управління сформувався переважно в умовах циклічних економічних криз і не повною мірою враховує специфіку деструктивного впливу збройного конфлікту – руйнування інфраструктури, примусове переміщення персоналу, розрив виробничих і збутових ланцюгів, а також різкі коливання попиту на продукцію.

Близнюк Т., Овсюченко Ю. та Пересада О. визначають фінансову безпеку підприємства як «стан фінансової системи суб'єкта господарювання, за якого забезпечується його здатність протистояти внутрішнім і зовнішнім загрозам, зберігати стійкість і реалізовувати стратегічні цілі розвитку» [2, с. 96]. У такому розумінні антикризове управління виступає не лише реактивним механізмом подолання кризи, а й проактивним інструментом підтримання фінансової безпеки на належному рівні. Науковці також розмежовують два виміри антикризового управління: тактичний (оперативне реагування на кризові явища – управління ліквідністю, реструктуризація