

2. Ellen MacArthur Foundation. <https://www.ellenmacarthurfoundation.org/>  
(дата звернення 15.11.2024)

## **ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА: ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ**

*Кирчата І.М., к.е.н., доцент  
Горбуненко А.Б., здобувач PhD  
Харківський національний автомобільно-дорожній університет*

Економічна безпека підприємства є однією з найважливіших умов його стабільного функціонування та розвитку в умовах сучасного ринку. Сьогодні бізнес стикається з новими викликами, такими як посилення конкуренції, глобалізація, цифровізація, ризики кіберзагроз і шахрайства. У цьому контексті забезпечення економічної безпеки виходить за межі класичного фінансового аналізу і включає управління ризиками, впровадження інноваційних технологій і побудову прозорої системи контролю.

Економічна безпека підприємства – це стан захищеності його ресурсів, фінансових, матеріальних і людських, від внутрішніх і зовнішніх загроз. Вона охоплює широкий спектр заходів, спрямованих на збереження стабільності, підвищення конкурентоспроможності та забезпечення розвитку підприємства.

Ефективна система економічної безпеки повинна враховувати:

- захист фінансових ресурсів (від шахрайства, корупції та неплатоспроможності контрагентів);
- управління ризиками (включаючи ризики, пов'язані з цифровими технологіями);
- забезпечення конфіденційності інформації;
- побудову стійкої системи управління в кризових умовах;

Сучасна економічна безпека має базуватися на двох принципах: превентивності (упередження загроз) і адаптивності (швидке реагування на виклики).

Цифровізація, будучи процесом інтеграції цифрових технологій у всі аспекти діяльності підприємства, стає ключовим фактором у забезпеченні економічної безпеки, оскільки дозволяє автоматизувати процеси, зменшувати вплив людського фактора та оперативно виявляти загрози.

Сучасні підприємства використовують аналітичні платформи, що дозволяють збирати, обробляти та аналізувати дані в реальному часі. Наприклад, системи Big Data Analytics можуть виявляти аномалії в операційній діяльності, що вказують на можливі ризики або шахрайські дії.

Використання цифрових інструментів для автоматизації бухгалтерського обліку, аудиту та бюджетування зменшує ризик помилок і зловживань. Наприклад, ERP-системи (Enterprise Resource Planning) дозволяють контролювати всі аспекти фінансової діяльності в єдиній інтегрованій платформі.

Захист цифрових даних є критично важливим для економічної безпеки. Підприємства впроваджують системи захисту від кіберзагроз, такі як фаєрволи, антивірусні програми, системи виявлення вторгнень та шифрування даних. Важливим аспектом є навчання персоналу основам кібергігієни.

Алгоритми штучного інтелекту (ШІ) здатні прогнозувати ризики, аналізуючи великі обсяги даних, та автоматично виявляти потенційні загрози. Наприклад, ШІ використовується для аналізу поведінки клієнтів або співробітників, виявляючи незвичні дії, що можуть свідчити про шахрайство.

Хмарні рішення, в свою чергу, забезпечують захист даних через централізоване управління доступом і резервне копіювання. Крім того, хмари дозволяють оперативно масштабувати ресурси для реагування на загрози.

Шахрайство є однією з найпоширеніших загроз для підприємств. Воно може включати фінансові махінації, крадіжку даних, корупцію, маніпуляції з контрактами та фальсифікацію звітності.

До інструментів боротьби із шахрайством відносять:

- внутрішній аудит: регулярна перевірка фінансової діяльності та операцій дозволяє виявляти порушення;
- цифрові системи моніторингу: системи, що автоматично аналізують фінансові операції, можуть ідентифікувати підозрілі транзакції;
- анонімні канали для повідомлень: можливість повідомляти про шахрайство без розкриття особистості сприяє виявленню зловживань;
- впровадження системи комплаєнсу: створення стандартів етичної поведінки та контроль їх дотримання допомагають запобігти корупції.

Управління ризиками є невід'ємною частиною системи економічної безпеки. Це процес ідентифікації, оцінки та мінімізації впливу загроз.

Незважаючи на широке впровадження цифрових технологій, людський фактор залишається важливим у забезпеченні економічної безпеки. Підприємства повинні інвестувати у підвищення кваліфікації працівників. Навчання з кібергігієни, управління ризиками та боротьби з шахрайством є обов'язковими для всіх рівнів персоналу. Формування корпоративної культури, орієнтованої на етичну поведінку та дотримання стандартів безпеки, допомагає мінімізувати внутрішні загрози.

Отже, сталий розвиток економічної безпеки залежить не лише від технологічних рішень, але й від готовності підприємств до адаптації в умовах постійних змін. Інвестиції у сучасні технології, навчання персоналу та формування корпоративної культури є ключовими елементами для побудови ефективної системи економічної безпеки, здатної забезпечити стабільність і розвиток бізнесу у довгостроковій перспективі.