УДК 65.012.8: 004.056

Мараховський Б.О.,
здобувач другого (магістерського) рівня вищої освіти
(Науковий керівник: к.е.н., доцент Дмитришин Б.В.)
Центральноукраїнський національний технічний університет
м. Кропивницький

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ СТІЙКОСТІ ПІДПРИЄМСТВА В УМОВАХ СУЧАСНИХ ВИКЛИКІВ І ЗАГРОЗ

Інформаційна безпека виступає одним із ключових факторів забезпечення економічної стійкості підприємства в умовах зростання технологічних викликів і загроз. У сучасній економіці, де домінують цифрові технології, інформаційні ресурси підприємств є стратегічно важливими активами. Їх втрата або компрометація може призвести до значних фінансових втрат, зупинки бізнес-процесів, зниження конкурентоспроможності та репутаційних ризиків. Ефективна система інформаційної безпеки дозволяє підприємствам не лише зберігати стабільність, а й забезпечувати економічну витривалість у нестабільному середовищі [1].

Зростання кількості кіберзагроз в умовах сучасних глобалізаційних процесів створює серйозні виклики для економічної безпеки підприємств. До найбільш поширених загроз відносяться фішингові атаки, програми-вимагачі, цілеспрямовані атаки на бізнес-структури (APT) та маніпулятивне використання персональних даних. Втрата інформації внаслідок подібних атак може призвести до порушення роботи підприємства, втрати довіри клієнтів і партнерів, а також до значних фінансових витрат, пов’язаних із відновленням роботи систем та виплатами штрафів за невиконання нормативних вимог, таких як GDPR чи ISO 27001 [2].

Особливої уваги заслуговує зв’язок між інформаційною безпекою та економічною стійкістю підприємства. Економічна стійкість передбачає здатність підприємства ефективно функціонувати, мінімізувати втрати та забезпечувати безперервність бізнес-процесів навіть за умов дії несприятливих зовнішніх факторів. Втрата критичних даних, перебої в роботі інформаційних систем або витоки конфіденційної інформації можуть суттєво підірвати здатність підприємства залишатися економічно стабільним і конкурентоспроможним [3].

Реалізація заходів інформаційної безпеки спрямована на забезпечення конфіденційності, цілісності та доступності інформаційних активів. Вона дозволяє мінімізувати економічні ризики шляхом:

1. Запобігання фінансовим втратам. Своєчасне виявлення та нейтралізація кіберзагроз знижує ймовірність зупинки операційної діяльності та витрат на відновлення систем.

2. Захисту репутації. Успішні атаки, які призводять до витоків даних, завдають значної шкоди репутації підприємства, що впливає на довіру клієнтів та партнерів.

3. Дотримання регуляторних вимог. Забезпечення відповідності стандартам інформаційної безпеки дозволяє уникати штрафних санкцій та покращувати інвестиційну привабливість підприємства.

4. Підвищення стійкості бізнесу. Інформаційна безпека сприяє створенню проактивної системи управління ризиками, яка дозволяє швидко реагувати на інциденти, забезпечуючи безперервність операційних процесів.

Крім того, інформаційна безпека сприяє впровадженню інноваційних рішень, які підвищують економічну ефективність підприємства. Наприклад, використання технологій штучного інтелекту для виявлення аномалій у трафіку, впровадження багатофакторної автентифікації або системи моніторингу в режимі реального часу дозволяють значно знизити ризики кібератак. Водночас важливим залишається підвищення обізнаності персоналу, оскільки людський фактор є одним із найвразливіших аспектів системи безпеки [4].

Отже, інформаційна безпека відіграє вирішальну роль у забезпеченні економічної стійкості підприємства, дозволяючи ефективно протистояти викликам сучасного інформаційного середовища. Її інтеграція у загальну стратегію розвитку підприємства забезпечує не лише захист критичних активів, а й створює передумови для зростання конкурентоспроможності, інноваційного розвитку та довгострокової стабільності бізнесу. У світі, де інформація є новою валютою, саме інформаційна безпека стає основою економічної витривалості підприємств.

Список використаних джерел:

1. Моделювання та реінжиніринг бізнес-процесів: підручник / С.В. Козир, В.В. Слєсарєв, С.А. Ус, Т.В. Хом'як ; М-во освіти і науки України ; Нац. техн. ун-т «Дніпровська політехніка». Дніпро : НТУ «ДП», 2022. 163 с.
2. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.
3. Dmytryshyn B., Marakhovskyi B. (2024). Optimization methods for business processes in trade activities // The process and dynamics of the scientific path: collection of scientific papers «SCIENTIA» with Proceedings of the VII International Scientific and Theoretical Conference, November 22, 2024. Athens, Hellenic Republic: International Center of Scientific Research.
4. Архипов О.Є., Архипова Є.О. Положення про інформаційну безпеку в міжнародних стандартах. *Інформаційна безпека людини, суспільства, держави*. 2010. № 2 (4). С. 62-65.

УДК 339.13

Маруся к Д.О.,
здобувач другого (магістерського) рівня вищої освіти
(Науковий керівник: д.е.н., професор Дороніна О.А.)
ДонНУ ім. Василя Стуса

АРХІТЕКТУРА ВИБОРУ: ЯК ДИЗАЙН ОПЦІЙ ВПЛИВАЄ НА ПОВЕДІНКУ СПОЖИВАЧІВ

Постановка проблеми. Сучасний споживач щодня стикається з великим обсягом інформації, що ускладнює процес прийняття рішень. Дизайн опцій,