УДК 338

Сисоліна Н. П., к.е.н., доцент
Центральноукраїнський національний технічний університет
м. Кропивницький

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Небезпеки в інформаційній сфері призводять не лише до прямих фінансових витрат (витрати на відновлення систем, штрафи за порушення законодавства тощо), але і до непрямих збитків, які за розміром можуть бути достатньо великими. Непрямі збитки такі як втрата репутації, зниження довіри клієнтів та інвесторів, а також простій бізнес-процесів, призводять до втрати прибутку.

Економічна безпека займає важливу роль в системі стратегічного управління, оскільки допомагає визначити які можливі ризики, їх вплив на кінцевий результат, і які заходи необхідно запровадити [1]. Інформаційна безпека як частина загальної стратегії управління економічними ризиками включає визначення критично важливих інформаційних активів, аналіз ймовірності настання ризику та потенційних збитків, а також впровадження захисних механізмів, які є економічно виправданими (вартість захисту не має перевищувати вартість активу).

На економічну стабільність безпосередньо впливає дотримання національних та міжнародних стандартів (наприклад, ISO 27001, PCI DSS для платіжних систем), це є необхідною умовою для ведення бізнесу та запобігання регуляторним штрафам.

Важливо впроваджувати чітку політику класифікації даних (наприклад, публічна, внутрішня, конфіденційна, комерційна таємниця). За цією класифікацією необхідно визначати рівень доступу, захисту та термін зберігання.

Використання систем Data Loss Prevention може допомогти моніторингу, ідентифікації та блокуванню несанкціонованої передачі конфіденційних даних за межі корпоративної мережі (через електронну пошту, USB-накопичувачі, хмарні сервіси).

Рівень інформатизації на підприємствах дає змогу використовувати визначення рівня ризику, метою якого є ефективне управління інформаційними технологіями та забезпечення економічної безпеки, за рахунок підвищення надійності бізнес-процесів [2].

Застосування надійних алгоритмів шифрування важливо для захисту даних таких як шифрування жорстких дисків, баз даних, використання захищених протоколів (TLS/SSL, VPN).

Підвищення залежності бізнесу від інформаційних технологій супроводжується збільшенням ризиків кібератак, зокрема щодо критичної інфраструктури [3].

Необхідно враховувати можливі кіберзагрози, до яких можна віднести ненавмисні помилки співробітників або навмисні зловживання доступом з метою шантажу чи продажу даних конкурентам, зловмисне програмне забезпечення, яке діє лише у пам’яті системи, уникаючи традиційних антивірусних перевірок, та обладнання сторонніх постачальників, що використовується підприємством тощо.

Для безпеки підприємства можуть застосовувати методи запобігання загроз. Це і систематичний процес сканування мережі, оцінки та пріоритезації виправлення виявлених вразливостей, і розділення корпоративної мережі на менші, ізольовані сегменти, що обмежує розповсюдження атаки у випадку компрометації одного сегмента, і регулярне моделювання кібератак для виявлення та усунення реальних вразливостей до того, як їх використають зловмисники.

Роль інформаційних технологій у забезпеченні безпеки наведено у таблиці 1.

Таблиця 1

Інформаційні технології у забезпеченні безпеки

№	Інформаційні технології	Сутність
1	Архітектура нульової довіри	Сучасна концепція безпеки, за якою жоден користувач, пристрій або програма (як всередині, так і ззовні периметра) автоматично не отримує довіри. Усі повинні постійно проходити перевірку автентичності та авторизації, що мінімізує збитки від внутрішніх та зовнішніх загроз
2	Багатофакторна автентифікація	Обов'язкове використання багатофакторної автентифікації для доступу до критичних систем, що унеможливлює використання викрадених паролів зловмисниками
3	Системи моніторингу поведінки користувачів	Технологія з використанням ШІ для аналізу нормальної поведінки співробітників, при цьому будь-які значні відхилення від норми (так, незвичний час доступу, завантаження великої кількості даних) автоматично позначаються як потенційний інцидент
4	Хмарна безпека	Використання хмарної безпеки – інтеграція безпеки безпосередньо у процес розробки та розгортання програмного забезпечення, що особливо актуально для хмарних інфраструктур

Інформаційна безпека неможлива без чітких планів, які дозволяють підприємству продовжувати критичні операції навіть після значного інциденту (наприклад, масова кібератака або стихійне лихо).

Отже, можливі загрози потребують комплексного підходу щодо управління інформаційними ризиками та розробки достатньо надійних систем, зокрема кібербезпеки, а підприємству необхідно побудувати таку систему безпеки, що включає моніторинг, реагування, методи запобігання загроз, тим самим підвищивши свою безпеку.

Список використаних джерел:

1. Сисоліна Н. П., Савеленко Г. В., Сисоліна І. П. Економічна безпека агропідприємств в умовах війни: можливості та загрози. *Економіка та суспільство*. № 65, 2024 DOI: https://doi.org/10.32782/2524-0072/2024-65-19.

2. Данченко О. Б., Ланських Є. В., Семко О. В. Інформаційні ризики цифрового формату. *Вісник Черкаського державного технологічного університету*. 2020. № 3. С. 58-66. DOI: 10.24025/2306 4412.3.2020.200792.

3. Савеленко Г. В., Сисоліна Н. П., Ніколаєв І. В. Управління ризиками при впровадженні інформаційних систем в електронному бізнесі. *Науковий вісник Льотної академії. Серія: Економіка, менеджмент та право*. Київ: Центр учбової літератури. №9, С.48-59. URL: https://fmnzb.sfa.org.ua/wp-content/uploads/2025/09/5.pdf.