середовища та створення передумов для сталого розвитку роздрібного бізнесу в цифровій економіці.

Список використаних джерел:

1. Котлер Ф., Картаджая Х., Сетіаван І. Маркетинг 5.0: технології для людства. Київ: Наш формат, 2022.
2. Laudon K. C., Traver C. G. E-Commerce: Business, Technology, Society. Pearson, 2022.
3. OECD. Digital Transformation of Retail Trade. Paris: OECD Publishing, 2021.
4. Porter M. E. Competitive Advantage: Creating and Sustaining Superior Performance. – New York: Free Press, 2008.

УДК 65.012.8: 004.056

Компанієць А. О.,
здобувач другого (магістерського) рівня вищої освіти
(Науковий керівник: д.е.н., професор Зайченко В. В.)
Центральноукраїнський національний технічний університет
м. Кропивницький

ВПЛИВ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ЕКОНОМІЧНУ СТІЙКІСТЬ ПІДПРИЄМСТВА В УМОВАХ СУЧАСНИХ ЗАГРОЗ

У сучасних умовах інформаційна безпека посідає ключове місце серед чинників, що визначають економічну стійкість підприємства, особливо з огляду на стрімке зростання кіберризиків та технологічних загроз. У цифровій економіці інформація та дані стали стратегічно важливими активами, від стану захищеності яких залежить безперебійність діяльності підприємства, його фінансові результати та конкурентні позиції на ринку. Будь-яка втрата, блокування або викривлення інформації здатні спричинити значні економічні збитки, порушення бізнес-процесів, погіршення репутації та зниження довіри партнерів. Наявність комплексної системи управління інформаційною безпекою забезпечує підприємству здатність протистояти зовнішнім загрозам, зберігати стабільність та підтримувати економічну витривалість у мінливому середовищі [1; 2].

Актуальність проблеми значно посилилася в умовах повномасштабної агресії Російської Федерації проти України, коли кіберпростір став одним із ключових фронтів гібридної війни [3]. Кількість кібератак на українські підприємства, органи влади та критичну інфраструктуру зросла в рази. Поширеними є фішингові кампанії, вірусні програми-вимагачі, атаки на серверні потужності, спроби викрадення конфіденційних даних або їх шифрування для подальшого вимагання викупу. Особливо небезпечними є цілеспрямовані довготривалі атаки (APT), що здійснюються із застосуванням складних інструментів та спрямовані на підрив діяльності підприємства. Подібні інциденти здатні спричиняти суттєві фінансові втрати, зупинку операційної діяльності, розрив господарських зв’язків та юридичну відповідальність у разі порушення міжнародних стандартів, таких як GDPR [4], ISO/IEC 27001 [5].

Ефективно вибудувана система інформаційної безпеки відіграє ключову роль у забезпеченні економічної стійкості підприємства, оскільки дозволяє мінімізувати негативні наслідки кібератак і запобігати їхньому впливу на основні показники діяльності. Надійний захист інформаційних активів забезпечує безперервність бізнес-процесів, стабільність фінансових потоків та збереження майнових і немайнових ресурсів підприємства. У воєнних умовах, коли ризик втручання у роботу цифрових систем з боку ворожих суб'єктів залишається високим, інформаційна безпека виступає одним із фундаментальних елементів загальної системи економічної безпеки підприємства.

Крім того, наявність сучасної комплексної системи захисту інформації (КСЗІ) підвищує здатність підприємства адаптуватися до турбулентних умов зовнішнього середовища, що безпосередньо впливає на його конкурентоспроможність і довгострокову стабільність. Високий рівень інформаційної безпеки завдяки використанню КСЗІ (рис. 1) сприяє зміцненню довіри з боку інвесторів, партнерів та споживачів, що є особливо важливим у період економічної нестабільності та загроз, спричинених війною.

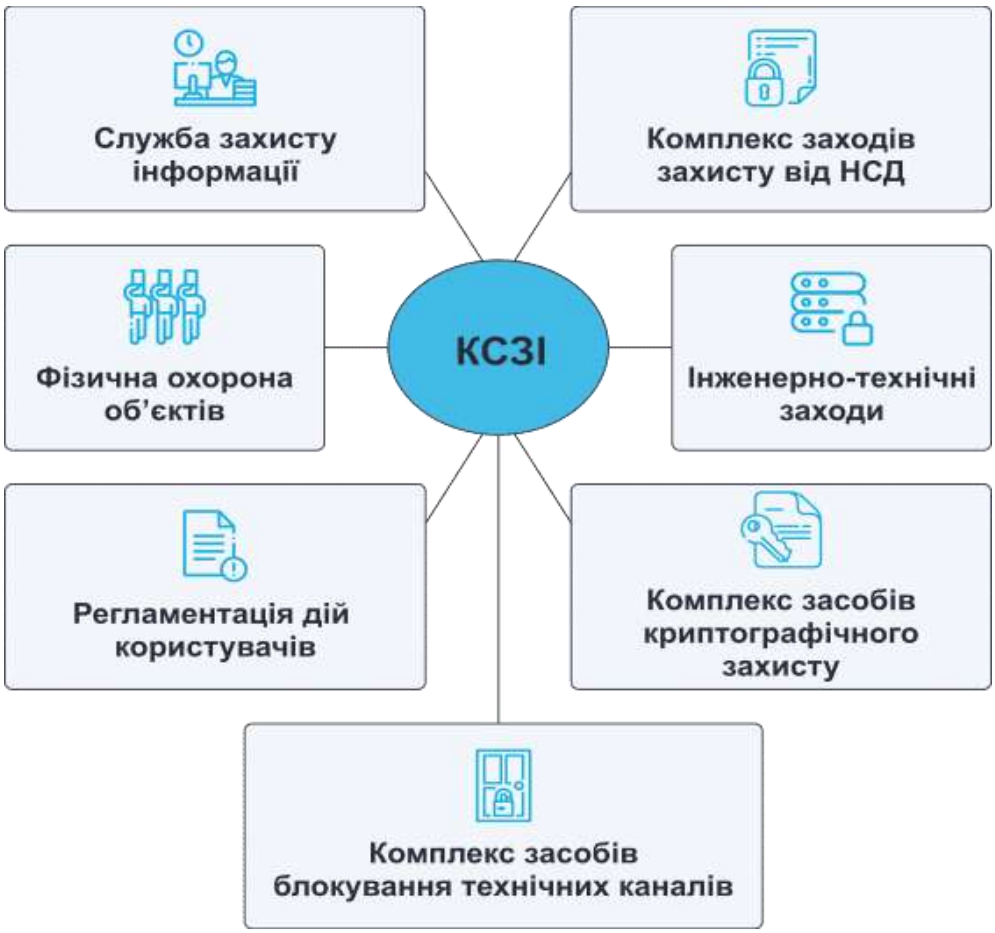

Рис. 1. Архітектура КСЗІ сучасного підприємства

Джерело: [6]

Забезпечення інформаційної безпеки передбачає підтримання конфіденційності, цілісності та доступності інформаційних активів. Реалізація відповідних заходів мінімізує ключові економічні ризики підприємства, зокрема [7; 8]:

1. Запобігання фінансовим втратам. Вчасне виявлення та блокування кібератак дає змогу уникнути витрат на відновлення даних, простою виробництва або сервісів, а також недоотримання доходів.

2. Захист ділової репутації. Витоки даних чи компрометація інформації суттєво шкодять іміджу підприємства, знижують довіру клієнтів і партнерів, що прямо впливає на його ринкову позицію.

3. Дотримання нормативних вимог. Виконання міжнародних та національних стандартів інформаційної безпеки дозволяє підприємству уникати штрафів і підвищує його інвестиційну привабливість.

4. Формування стійкості до кризових ситуацій. Наявність проактивної системи управління інформаційними ризиками забезпечує можливість швидкого реагування на інциденти, що підтримує безперервність бізнес-процесів навіть у надзвичайних умовах.

Отже, інформаційна безпека є критично важливим елементом забезпечення економічної стійкості підприємства в умовах сучасних викликів, включаючи воєнні загрози, зростання кіберризиків та загальну турбулентність зовнішнього середовища. Її інтеграція в систему стратегічного управління дозволяє не лише ефективно захищати інформаційні активи, а й створює основу для довгострокової стабільності, інноваційного розвитку та зміцнення конкурентоспроможності підприємства. У час, коли інформація є одним із найцінніших ресурсів, а війна триває і впливає на всі сфери економіки, інформаційна безпека стає фундаментом економічної витривалості та здатності підприємства протистояти зовнішнім загрозам.

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. Мельник А. Ф., Карлін М. І. Цифрова економіка: теоретичні засади та тенденції розвитку. Львів: ЛНУ ім. І. Франка, 2020. 284 с.
3. CERT-UA. Огляд кіберінцидентів в Україні та рекомендації щодо їх запобігання. Державна служба спецзв'язку та захисту інформації України, 2023. 54 с.
4. Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer, 2017. 383 p.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022. 33 p.
6. Комплексна система захисту інформації – URL: https://www.h-x.technology/ua/services/kszi-implementation-ua.
7. Ліпкан В. А., Ліпкан О. С. Інформаційна безпека підприємства: теорія і практика. Київ: КНТ, 2019. 372 с.
8. Лапін Є. Б. Економічні ризики в інформаційному суспільстві: аналіз та мінімізація. Харків: ХНЕУ ім. С. Кузнеця, 2021. 248 с.