

ЄМЕЦЬ АНАТОЛІЙ, здобувач вищої освіти

Науковий керівник – **БУРКОВСЬКА АННА**, доктор філософії (економіка),
доцент кафедри менеджменту, бізнесу та адміністрування,
Миколаївський національний аграрний університет, м. Миколаїв

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ УПРАВЛІННЯ ЦИФРОВИМИ БІЗНЕС-СИСТЕМАМИ

У сучасному цифровому середовищі бізнес усе більше залежить від інформаційних технологій та автоматизованих систем управління. Цифрові бізнес-системи дозволяють оптимізувати операційні процеси, підвищувати ефективність та зменшувати витрати, однак їхня функціональність неможлива без належного рівня кібербезпеки. Відсутність надійного захисту інформації може призвести до серйозних фінансових втрат, порушення репутації компанії та навіть до зупинки критично важливих процесів [1].

Кібербезпека виступає не лише технічним, а й стратегічним елементом управління цифровими бізнес-системами. Вона включає комплекс заходів, спрямованих на захист даних, систем і мереж від несанкціонованого доступу, атак та шкідливого програмного забезпечення. Для менеджменту це означає необхідність формування політик безпеки, інвестування у технології захисту та підвищення компетентності персоналу щодо цифрових загроз [2].

Цифрові бізнес-системи стикаються з багатьма видами загроз, що можуть серйозно вплинути на їхню ефективність і безпеку. Серед них ключовими є кібератаки типу фішинг, зловмисне програмне забезпечення, ransomware-атаки, несанкціонований доступ до даних та внутрішні загрози від некваліфікованого або недобросовісного персоналу. Також загрозу становлять вразливості в програмному забезпеченні, відсутність регулярного оновлення систем та недостатній контроль над мережевою інфраструктурою [3]. Всі ці фактори можуть призводити до витоку конфіденційної інформації, фінансових збитків, порушення законодавчих норм та шкоди репутації компанії.

Впровадження ефективних стратегій кібербезпеки дозволяє підприємствам не лише захищати активи, а й підвищувати довіру клієнтів і партнерів. Цифрові системи обробляють велику кількість конфіденційної інформації, включно з фінансовими даними, персональними даними співробітників та інформацією про клієнтів. Їхній захист є необхідною умовою для забезпечення безперервності бізнес-процесів і конкурентоспроможності компанії [3].

Кібербезпека забезпечує стабільність роботи цифрових платформ, що дозволяє уникати простоїв та фінансових втрат, пов'язаних із кібератаками. Вона підвищує рівень довіри клієнтів та партнерів, адже надійний захист даних демонструє відповідальність компанії та її готовність захищати інтереси стейкхолдерів. Крім того, системи кібербезпеки дозволяють швидко виявляти та локалізувати загрози, що підвищує оперативність реагування на інциденти та знижує ризики серйозних порушень. Інтеграція кібербезпеки у стратегічне управління також сприяє дотриманню законодавчих і нормативних вимог щодо захисту інформації, що забезпечує легальність і прозорість бізнес-операцій [2].



Аналіз практики показує, що найбільш ефективне управління кібербезпекою досягається через інтеграцію технологічних рішень з організаційними та кадровими заходами. Сучасні системи моніторингу загроз, шифрування даних, багаторівневої аутентифікації та автоматизованого реагування на атаки доповнюються навчанням персоналу та регулярними аудитами безпеки. Лише такий комплексний підхід дозволяє мінімізувати ризики та забезпечити надійність цифрових бізнес-систем [4].

Прогноз розвитку кібербезпеки у найближчі роки вказує на зростання її стратегічного значення для управління цифровими бізнес-системами. Очікується, що кількість кіберзагроз буде зростати пропорційно розвитку цифровізації та впровадженню нових технологій, таких як хмарні сервіси, Інтернет речей та штучний інтелект. Менеджменту необхідно буде інтегрувати проактивні системи захисту, інструменти аналітики кіберризиків та моделі прогнозування атак. Підприємства, які вчасно адаптують стратегії кібербезпеки до нових викликів, отримають значну конкурентну перевагу та зможуть гарантувати стабільність і безпеку бізнес-процесів [5].

Таким чином, кібербезпека є ключовим елементом управління цифровими бізнес-системами. Вона забезпечує захист критично важливої інформації, підтримує безперервність операцій та сприяє розвитку довіри з боку клієнтів і партнерів. Успішна інтеграція кібербезпеки в систему управління вимагає поєднання технологічних рішень, організаційних заходів та підготовки персоналу, що дозволяє підприємствам ефективно адаптуватися до сучасних викликів цифрового середовища та забезпечувати сталий розвиток бізнесу.

Список використаних джерел:

1. Шостак Л., Більо І., Микитюк Є. Потенціал цифровізації вітчизняного бізнес-середовища. *Економічний аналіз*. 2021. Том 31. № 1. С. 245–251.
2. Полторак А.С., Сухорукова А. Л., Бурковська А. І. Кібербезпека в системі трансформації управління бізнес-організацією. Трансформація менеджменту бізнес-організацій: сучасні тренди та виклики : колективна монографія. Київ : *Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана*. 2021. С. 158-176. URL: <http://dSPACE.mnau.edu.ua/jspui/bitstream/123456789/10893/1/17.pdf>
3. Шостак Л. В., Більо І. О., Уляницький А. О. Бізнес-моделі підприємства у цифрову епоху: зарубіжний досвід. *Економіка та суспільство*. 2024. № 60. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/3702>.
4. Burkovska A., Burkovska A. Semantic approach to food marketing: the influence of sustainable development narratives on the Ukrainian market. *Agricultural and Resource Economics*. 2025. Vol.11. No.1. Pp.317–347. <https://doi.org/10.51599/are.2025.11.01.12>.
5. Вerezomska I., Bovsh L., Prihodko K., Baklan H. Кіберзахист готельних брендів. *Ресторанний і готельний консалтинг. Інновації*. 2022. 5(2), 190-209. URL: <https://doi.org/10.31866/2616-7468.5.2.2022.270089>.

