

**Безушко О. Є.,**  
*здобувач першого (бакалаврського) рівня вищої освіти*  
*факультету менеджменту*  
**Науковий керівник: Хилько І. І.,**  
*старший викладач кафедри економічної кібернетики,*  
*комп'ютерних наук та інформаційних технологій*  
*Миколаївський національний аграрний університет*  
*м. Миколаїв, Україна*

## **ІННОВАЦІЇ У БІЗНЕСІ ТА ЦИФРОВА БЕЗПЕКА ПІДПРИЄМСТВА**

У сучасних умовах стрімкого розвитку цифрових технологій питання щодо, інформаційної безпеки для бізнесу набуває особливого значення. Інновації є провідним драйвером для бізнесу, вони дозволяють оптимізувати роботу та зменшити витрати. В наш час інноваційні технології інтегруються в усі сфери діяльності бізнесу, підвищуючи ефективність роботи, але при цьому виникають і значні ризики кіберзагроз. Саме тому, моделювання цифрової безпеки є ключовим елементом стратегічного управління бізнесу.

Метою роботи є аналіз впливу інноваційних технологій на бізнес та аналіз підходів до моделювання цифрової безпеки для ефективного управління щодо кіберзагроз.

Впровадження інноваційних технологій в наш час стало необхідним задля забезпечення конкурентоспроможності, ефективності та розвитку бізнесу. Ось деякі технології нашого часу які вже впровадили у свій бізнес більшість великих компаній:

- CRM Система: дозволяє зберігати дані про кожного клієнта в базі, надаючи швидкий доступ до історії клієнтського кабінету. Також дозволяє автоматизувати бізнес-процеси, такі як відстеження лідів, персоналізованих пропозицій.

- ERP Система: програмне забезпечення, яке дозволяє організувати роботу різних відділів в єдиний простір. ERP є дуже хорошою інновацією саме для малих бізнесів, адже допомагає зібрати різні інформаційні системи в єдину базу даних.

- Хмарні технології: якісний варіант для обробки даних в онлайн, чим і полегшує доступ до інформації. Дозволяє мінімізувати витрати бізнесу.

- Аналітика даних: є невід'ємною частиною сучасного бізнесу та використовується для виявлення тенденцій і залежностей, які можуть бути неочевидними при першочерговому аналізі даних.

- IoT або ж інтернет речей: дозволяє компанії відстежувати як і стан обладнання, так і покращити взаємозв'язок компанії з клієнтами через «розумні» нововведення.

Але, попри всі вище перераховані інновації, не слід забувати про кібербезпеку. Кібербезпека передбачає сукупність технологій, процесів і заходів, спрямованих на захист комп'ютерних систем, мереж і даних від

несанкціонованого доступу, тобто кібератак, пошкоджень або викрадення інформації [1]. Також кібербезпека має дуже великий вплив для забезпечення безперебійної роботи компаній, захисту даних.

Створення цифрової безпеки є невирішеною проблемою більшості підприємств. У 2023 році в Україні кількість кібератак, порівняно з 2022 роком, зростає майже на 16% до 2543 інцидентів [2].

Наразі в Україні цифрова безпека знаходиться на дуже низькому рівні порівняно з іншими країнами. Попри досить успішні показники компанії та на її вклад до розвитку цифрової безпеки, аналіз показує що знищити підприємство всередині можна лише за кілька кроків. Саме тому рекомендують використовувати математичну модель цифрової безпеки.

Основна мета моделювання цифрової безпеки полягає в забезпеченні надійного рівня захисту даних і цифрових активів організації. Тому розробляють багатокритеріальні схеми, які дозволяють ідентифікувати три основні елементи моделі, а саме:

- Цифрове середовище підприємства за категоріями: доступність інформації, місце її зберігання тощо.
- Потенційного «зловмисника» з урахуванням його мотивації.
- Цифрову атаку з позиції застосування різних інструментів і необхідних для її здійснення ресурсів [3].

Отже, інноваційний розвиток є необхідною складовою не тільки для розвитку підприємства, але і задля його оптимізації та мінімізації витрат. В наш час новітні технології розвиваються з дуже швидким темпом, тому потрібно з часом змінювати інноваційний підхід до бізнесу, адже це дасть результат не тільки всередині виробничого процесу, але й надасть компанії нових клієнтів через те, що значна частина обирає те що зручно. Але не варто забувати про цифрову безпеку яка є невід'ємною при створенні бізнесу, адже швидке встановлення загроз надає можливість вжити необхідних заходів задля усунення небезпеки.

### Список використаних джерел:

1. Коваль П. О. Кібербезпека – засіб захисту інформації. Глобальні цілі сталого розвитку – безпека світу, соціально-економічні та екологічні прояви, можливості активізації партнерства : тези доповідей - здобувачів вищої освіти денної й заочної форм навчання за результатами щорічного тематичного «круглого столу» на обліково-фінансовому факультеті, м. Миколаїв, 12 листопада 2020 р. Миколаїв : МНАУ, 2020. С. 32-34. URL: <https://dspace.mnau.edu.ua/jspui/bitstream/123456789/8264/1/32-34.pdf> (дата звернення: 06.11.2024).
2. Жарикова А. Кількість кібератак у 2023 році зростає на 16% - Держспецзв'язку. *Економічна правда*. URL: <https://www.epravda.com.ua/news/2024/01/31/709355/> (дата звернення: 06.11.2024).
3. Касьянова Н. В., Біличенко М. М., Севериненко А. О. Моделювання цифрової безпеки підприємства. *Modern Economics*. 2023. № 39 (2023). С. 54-61. DOI: [https://doi.org/10.31521/modecon.V39\(2023\)-08](https://doi.org/10.31521/modecon.V39(2023)-08) (дата звернення: 06.11.2024).