

КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ БІЗНЕСУ

Вінницький національний технічний університет

Анотація

Цифрова трансформація відкриває нові можливості для бізнесу, але водночас створює серйозні виклики у галузі кібербезпеки. У роботі розглянуто загрози, пов'язані з IoT, хмарними сервісами та обробкою великих даних. Увагу приділено використанню міжнародних стандартів (ISO/IEC 27001, NIST Cybersecurity Framework, GDPR) і новітніх підходів, таких як Zero Trust Architecture, штучний інтелект та автоматизовані системи моніторингу. Запропоновано рекомендації для підвищення стійкості бізнесу до сучасних кіберзагроз.

Ключові слова: кібербезпека, цифрова трансформація, IoT, ISO/IEC 27001, Zero Trust, великі дані.

Abstract

Digital transformation opens up new opportunities for businesses but also creates serious challenges in the field of cybersecurity. This paper examines threats related to IoT, cloud services, and big data processing. Special attention is paid to the use of international standards (ISO/IEC 27001, NIST Cybersecurity Framework, GDPR) and innovative approaches such as Zero Trust Architecture, artificial intelligence, and automated monitoring systems. Recommendations are proposed to enhance business resilience to modern cyber threats.

Keywords: cybersecurity, digital transformation, IoT, ISO/IEC 27001, Zero Trust, big data

Вступ

Цифрова трансформація бізнесу пришвидшує процеси, підвищує ефективність і створює нові бізнес-моделі. Проте впровадження таких технологій, як IoT, хмарні сервіси та штучний інтелект, водночас підвищує вразливість підприємств до кібератак. Забезпечення кібербезпеки в таких умовах вимагає системного підходу, інтеграції міжнародних стандартів і використання сучасних адаптивних технологій.

Результати дослідження

Цифрова трансформація суттєво розширює поверхню атак для зловмисників. Інтернет речей (IoT), що активно впроваджується в різні сфери бізнесу, є особливо вразливим через відсутність єдиних стандартів безпеки та використання слабких механізмів автентифікації. Чимало IoT-пристроїв мають заводські налаштування (налаштування за замовчуванням), які не передбачають включення механізмів безпеки (наприклад, шифрування даних), що відкриває можливості для атак типу "людина всередині" (Man-in-the-Middle) або компрометації мережі через несанкціонований доступ тощо [1].

Використання хмарних сервісів, які стали основою для зберігання та обробки корпоративних даних, також породжує зростання ризиків кібербезпеки. Основні загрози пов'язані з неналежним контролем доступу, атакою на API та можливими витокami через недостатній рівень сегментації користувачів [2]. Важливим фактором залишається і те, що часто компанії не впроваджують багатофакторну автентифікацію, що значно полегшує компрометацію облікових записів.

Широке використання технологій великих даних також створює нові виклики. Масштабність та складність аналітичних процесів потребують застосування потужних механізмів захисту, зокрема для шифрування та моніторингу транзакцій у режимі реального часу. Відсутність чіткої політики управління доступом до конфіденційної інформації може

призвести до масштабних витоків даних, що ставить під загрозу фінансову та репутаційну стабільність підприємств.

Рекомендації для бізнесу

В умовах зростаючих кіберризиків підприємства мають впроваджувати комплексні заходи для захисту своїх цифрових активів. Серед ключових кроків можна виділити:

1) **Zero Trust Architecture.** Цей підхід забезпечує мінімізацію довіри до будь-яких внутрішніх та зовнішніх користувачів і застосовує принцип перевірки кожного доступу до корпоративних ресурсів [1].

2) **Захист даних.** Використання багаторівневого шифрування та політики обмеження доступу мінімізує ймовірність витоку конфіденційної інформації.

3) **Автоматизація кібербезпеки.** Використання SIEM-систем дозволяє ідентифікувати загрози в реальному часі, зменшуючи час реакції на інциденти [3].

4) **Підвищення кібергігієни співробітників.** Більшість атак базується на людському факторі, тому компанії повинні регулярно проводити навчальні програми для персоналу, щоб знизити ризики соціальної інженерії [1].

5) **Впровадження міжнародних стандартів.** Дотримання ISO/IEC 27001 та NIST Cybersecurity Framework дозволяє формалізувати процеси управління ризиками та відповідати регуляторним вимогам [4].

Висновок

Цифрова трансформація змінює підходи до ведення бізнесу, проте зростання рівня автоматизації, використання IoT та хмарних сервісів створює додаткові ризики для кібербезпеки. Відсутність належних заходів захисту може призвести до серйозних наслідків, таких як витоки конфіденційної інформації, фінансові втрати та підрив репутації. Інтеграція сучасних підходів до захисту, включаючи Zero Trust, автоматизовані системи моніторингу та впровадження міжнародних стандартів, є важливими умовами для створення стійкої кіберзахисної системи підприємств.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Лісовий І. В., Войтович О. П., Волинець О. Ю. Рекомендації забезпечення безпеки бездротових з'єднань інтернету речей // Матеріали LIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 20-22 березня 2024 р. Електрон. текст. дані. 2024. URI: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2024/paper/view/20423>.
2. Sarcea (Manea), O.A. How digital transformation and cyber security affect companies' performance? // Strategica. – 2023. – DOI: 10.25019/STR/2023.039.
3. Краус, К. М., Краус, Н. М., Штепа, О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану // Innovation and Sustainability. – 2022. – № 3. – С. 26–37.
4. Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E., Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations // Sensors. – 2023. – Vol. 23, No. 15. – P. 6666. DOI: <https://doi.org/10.3390/s23156666>

Волинець Віталій Володимирович — аспірант групи 125-24а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: volynets1026@gmail.com

Войтович Олеся Петрівна — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.vk.vntu.edu.ua

Volynets Vitalii V. — Faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: volynets1026@gmail.com

Voytovych Olesya P. — Ph.D., Associate Professor of the Department of Information Protection,
Vinnytsia National Technical University, Vinnytsia, e-mail voytovych.vk.vntu.edu.ua