Секція 1

АНАЛІЗ МЕТОДІВ КІБЕРБЕЗПЕКИ У СФЕРІ ДЕРЖАВНИХ ПОСЛУГ

Федоренко Д. Д.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко Г. А.

Актуальність. Цифровізація державних послуг, таких як електронні документи, записи та медичне страхування, значно розширило доступ громадян до життєво важливих послуг, але водночас підвищило ризик кібератак. Успішні атаки можуть призвести до витоку персональних даних, порушення роботи критично важливої інфраструктури та втрати довіри до державних інституцій, що загрожує приватності громадян та економічній стабільності [1].

Щоб протистояти еволюціонуючим кіберзагрозам, держави повинні вживати гнучких і проактивних оборонних заходів, інвестуючи в технології штучного інтелекту для виявлення аномалій і систем аналізу загроз. Важливо також навчати персонал ефективно реагувати на нові типи атак, що підвищить загальний рівень кібербезпеки [2].

Метою даної роботи є аналізу сучасних методів забезпечення кібербезпеки у сфері державних послуг.

Основні положення. З огляду на стрімку цифровізацію та залежність громадян від державних сервісів, важливість їхнього захисту є критичною. Поряд з перевагами, які надають цифрові технології, зростають і кіберризики, що ставлять під загрозу національну безпеку та приватність громадян. Тому захист таких сервісів є необхідністю для забезпечення стабільності державних інфраструктур. Сучасні кіберзагрози для комунальних підприємств різноманітні та включають як зовнішні атаки, так і внутрішні порушення безпеки. До основних загроз належать DDoS-атаки, фішинг, SQL-ін'єкції та сучасні методи соціальної інженерії, спрямовані на викрадення персональних даних та компрометації систем [2]. Уразливості в системах контролю доступу, незахищені канали зв'язку та недосконалі механізми аутентифікації підвищують ризик успішних атак [3]. Зловмисники часто включають як окремих хакерів, так і організовані групи кіберзлочинців, які прагнуть отримати несанкціонований доступ до урядових даних і підірвати довіру громадськості до цифрових послуг [4, 5]. Для підвищення рівня кібербезпеки державних сервісів необхідно впроваджувати комплексний підхід, що включає як технічні, так і

організаційні заходи. Важливим елементом є застосування моделей безпеки, таких як Zero Trust, що передбачає мінімізацію доступу до ресурсів та постійну перевірку користувачів і пристроїв [5]. Використання багатофакторної автентифікації, методів шифрування даних, а також систем виявлення та запобігання вторгненням (IDS/IPS) дозволяє значно знизити вразливості в системах. Крім того, регулярні тренінги для персоналу, постійний моніторинг систем на предмет аномалій та впровадження стандартів безпеки, є необхідними кроками для забезпечення стійкості до кібератак.

Висновки. Аналіз показує, що диджиталізація державних послуг збільшує ризик атак і вразливостей, загрожуючи національній безпеці та приватності громадян. Для забезпечення належного захисту необхідна модель нульової довіри, багатофакторна автентифікація, використання сучасних технологій спостереження та шифрування, підвищення стандартів безпеки, навчання персоналу та розробка ефективних методів реагування на кіберзагрози.

Список літератури

1. Arief A. R. An analysis of cybersecurity policies and practices in public administration. *Journal of public representative and society provision*. 2022. Volume 2(2). Page 56–62. DOI: https://doi.org/10.55885/jprsp.v2i2.211.

2. Understanding Local Government Cybersecurity Policy: A Concept Map and Framework / S. T. Hossain et al. *Information*. 2024. Volume 15(6). Page 342. DOI: https://doi.org/10.3390/info15060342.

3. Cyber threats and advisories | cybersecurity and infrastructure security agency CISA. *CISA*. URL – https://www.cisa.gov/topics/cyber-threats-and-advisories (дата звернення: 10.11.2024).

4. ENISA Threat Landscape 2024. *ENISA*. URL – https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 10.11.2024).

5. The world economic forum. *World Economic Forum*. URL – https://www.weforum.org (дата звернення: 10.11.2024).

Відомості про авторів

Федоренко Дар'я Дмитрівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.d.fedorenko@student.csn.khai.edu

Землянко Георгій Андрійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезбеки, g.zemlynko@csn.khai.edu