3. Довженко Н., Іваніченко Є., Аушева Н., Шевчук Ю., Луковський Т. Дослідження архітектури дата-центрів з інтеграцією IoT-компонентів для забезпечення енергоефективності та кіберстійкості. *Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка*. 2025. Т. 4, № 28. С. 547–564. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/835 (дата звернення: 31.03.2026).
4. Цифровий апетит, який недооцінюють: правда про енергоспоживання ЦОД. *Denovo.ua*. URL: https://denovo.ua/blog/energy-dc-metrix-2025 (дата звернення: 31.03.2026).

УДК 004.738.5

БЕЗПЕКА ТА ЗАХИСТ БЕЗДРОТОВИХ МЕРЕЖ: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ

Безчасний М. С.
hazardloka112@gmail.com
Черкаський державний фаховий бізнес-коледж
Люта М. В.
м. Черкаси, Україна

Бездротові мережі сьогодні є невід’ємною частиною сучасної інформаційної інфраструктури, що активно використовується у навчальних закладах, організаціях та побуті. Основною перевагою таких мереж є мобільність і зручність доступу до ресурсів без використання кабелів. Водночас зростання їх популярності супроводжується підвищенням кількості загроз інформаційній безпеці, що обумовлює необхідність дослідження вразливостей і методів захисту бездротових мереж [1].

Бездротові мережі, зокрема технологія Wi-Fi, забезпечують швидкий обмін даними та підтримують підключення великої кількості пристроїв, однак передача інформації через радіоканал створює передумови для її перехоплення [4]. Це зумовлює появу різноманітних атак, спрямованих на порушення конфіденційності та цілісності даних.

Однією з основних загроз є несанкціонований доступ до мережі, що може виникати через слабкі паролі або відсутність шифрування. У таких випадках зловмисники можуть отримати доступ до конфіденційної інформації користувачів [2].

Серед найбільш поширених атак виділяють перехоплення трафіку, підбір паролів, атаки типу «людина посередині» (Man-in-the-Middle) та створення підроблених точок доступу [5]. Перехоплення трафіку дозволяє отримувати передані дані, тоді як атаки підбору паролів базуються на автоматизованому переборі комбінацій. Особливо небезпечними є атаки з використанням фальшивих точок доступу, що вводять користувачів в оману.

Для забезпечення безпеки бездротових мереж застосовуються сучасні методи захисту, зокрема використання протоколів шифрування WPA2 та WPA3, які забезпечують надійний рівень захисту переданих даних. Важливим є також правильне налаштування мережевого обладнання, зокрема зміна стандартних паролів, оновлення програмного забезпечення та обмеження доступу до мережі [5].

Додатковими заходами безпеки є використання фільтрації MAC-адрес та систем моніторингу мережі, які дозволяють виявляти підозрілу активність і своєчасно реагувати на загрози. Аналіз вразливостей мережі здійснюється за допомогою спеціалізованих інструментів, що дозволяють оцінити рівень захисту та визначити потенційні ризики.

Отже, бездротові мережі є важливою складовою сучасної інформаційної інфраструктури, однак вони залишаються вразливими до різноманітних кіберзагроз. Забезпечення їх безпеки потребує комплексного підходу, що включає використання сучасних методів шифрування, належне налаштування обладнання та постійний моніторинг мережі. Реалізація цих заходів дозволяє суттєво знизити ризики несанкціонованого доступу та забезпечити захист інформації користувачів [3].

Список використаних джерел:

1. Гізун А. І., Гнатюк С. О., Щербина В. П. Сучасні технології захисту інформації в бездротових мережах: навч. посіб. Київ: НАУ, 2021. 240 с.
2. Бурячок В. Л., Корченко О. Г., Ткач Ю. М. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: ДУТ, 2022. 352 с.
3. OpenAI. GPT-4 Technical Report. 2023. URL: https://openai.com/research (дата звернення: 19.03.2026).
4. Комп'ютерні мережі: підручник / А. Г. Микитишин та ін. Тернопіль: ТНТУ ім. І. Пулюя, 2020. 256 с.
5. Жебка В. В., Сєрих С. О. Аналіз методів автентифікації та шифрування у бездротових мережах стандарту IEEE 802.11. Кібербезпека: освіта, наука, техніка. 2023. № 2(14). С. 45–58.

УДК 004.8:81'243

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИВЧЕННІ АНГЛІЙСЬКОЇ МОВИ

Прозоровська І.М.
zorovarina08@gmail.com
Черкаський державний фаховий бізнес-коледж
м. Черкаси, Україна

Поява інтернету декілька десятиліть тому змінила життя людей у багатьох сферах. Згодом, завдяки розвитку «міжнародної мережі», був створений штучний інтелект (ШІ), який набув своєї максимальної актуальності за останні декілька років. У вивченні іноземних мов, штучний інтелект на сьогодні стає необхідним потужним помічником, як для студентів, так і для викладачів.

Серед найважливіших складових у вивченні мови, можна виділити такі, як зворотній зв'язок (feedback), поступове навантаження у навчання (scaffolding), практика відтворення (retrieval practice) й інтервальне повторення (spaced practice).