

світу, щоб переймати їхні найефективніші практики та форми навчання [2]. Це допомагає українцям адаптуватися й налаштуватися на нові формати освіти, обрати для себе найкращий варіант.

## ЛІТЕРАТУРА

1. Закон України «Про освіту» № 2145-VIII від 05.09.2017 (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text> (дата звернення – 30.03.2024).

2. Найкращі школи світу: як вони навчають та чим дивують? URL: <https://osvitoria.media/experience/najkrashhi-shkoly-svitu-yak-vony-navchayut-ta-chym-dyvuyut/> (дата звернення – 30.03.2024).

**ЛИТВИНСЬКА Світлана**

*канд. філол. наук, доцент, Київ*

**МАРЧУК Роман**

*Національний авіаційний університет, Київ*

## ВИКОРИСТАННЯ ПРИРОДНОЇ МОВИ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У КОМУНІКАЦІЯХ

У сучасному цифровому світі загрози кібербезпеці можуть бути приховані в різноманітних комунікаціях, що ставить під загрозу безпеку особистих даних, фінансову стабільність та навіть національну безпеку. Використання природної мови для виявлення кіберзагроз стає дедалі більш актуальним та ефективним методом ідентифікації потенційних небезпек.

1. *Природна мова як ключовий інструмент.* Природна мова [1] є основним засобом спілкування для більшості людей та, отже, вона широко використовується в онлайн-спілкуванні через *соціальні мережі, електронну пошту та інші цифрові канали.* Це робить її ідеальним об'єктом для аналізу на предмет кіберзагроз.

2. *Аналіз тексту для виявлення аномалій.* Автоматизовані системи оброблення природної мови [2] можуть аналізувати

текстові дані для виявлення аномалій, а саме: *загрози безпеці, шахрайство чи шпигунство*. Вони аналізують *лексику, синтаксис та семантику тексту* для виявлення ненормальних патернів (схем-образів).

3. *Використання машинного навчання*. Машинне навчання [3] відіграє провідну роль у розвитку систем виявлення кіберзагроз із використанням природної мови. Моделі глибокого навчання задіюють на великих обсягах даних для виявлення складних патернів та змін у комунікаціях, які можуть свідчити про потенційні загрози.

4. *Мультимодальний аналіз* [4]. Крім тексту, системи можуть аналізувати інші форми медіа, такі як *зображення, аудіо та відео*, для отримання додаткових доказів кіберзагроз. Інтеграція цих різних джерел даних дозволяє створити більш повну картину загрози.

Використання природної мови для виявлення кіберзагроз у комунікаціях є актуальною та ефективною стратегією, яка допомагає вчасно виявляти потенційні небезпеки та запобігати їхнім негативним наслідкам. Із зростанням обсягу цифрових даних та загроз кібербезпеці, цей підхід стає невід'ємною складовою заходів із захисту від кібератак.

## ЛІТЕРАТУРА

1. Формальні і природні мови: веб-сайт. URL: <https://disted.edu.vn.ua/courses/learn/579> (дата звернення: 22.03.2024).

2. Що таке обробка природної мови (NLP) та як вона може використовуватися у бізнесі: веб-сайт. URL: <https://metinvest.digital/ua/page/1052> (дата звернення: 22.03.2024).

3. Nils J. Nilsson, *Introduction to Machine Learning*: веб-сайт. URL: <https://ai.stanford.edu/people/nilsson/mlbook.html> (дата звернення: 22.03.2024).

4. Що таке мультимодальний ШІ: вебсайт. URL: <https://skimai.com/uk/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BC%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%BC%D0%BE%D0%B4%D0%B0%D0%BB%D1%8C%>