

УДК 811.111'373.612:004.056

**Животченко О. М.,
студент,
Національний університет «Запорізька політехніка»**

**Кузнєцова І. В.,
кандидат філологічних наук, доцент,
доцент кафедри «Іноземна філологія та переклад»,
Національний університет «Запорізька політехніка»**

МЕТАФОРИЧНІ ТЕРМІНИ АНГЛОМОВНОЇ СФЕРИ КІБЕРБЕЗПЕКИ

У сучасному англомовному дискурсі кібербезпеки метафора виступає не лише стилістичним засобом, а й когнітивним інструментом, який формує розуміння технологічних процесів. Зазвичай метафору можна відкинути як тему, яка стосується лише гуманітарних наук або літературних критиків, але вона не особливо важлива для фахівців з кібербезпеки. Однак, як бачимо, навіть така прагматично орієнтована галузь, як кібербезпека, здатна взаємодіяти з метафоризацією, що зазвичай не є характерним для точних наук. Однак розгляд кібербезпеки з метафоричної точки зору може призвести до кращого розуміння

існуючих методів кіберзахисту та, для полегшеного розуміння цієї абстрактної сфери пересічною людиною.

Ця влучна ідея західних учених створила проблему перекладу метафор на іноземні мови. У перекладацькій практиці було обрано переважно калькувальний підхід, що передбачає буквальне відтворення термінологічних одиниць мови-джерела. Наприклад, *Phishing* (фішинг) вид шахрайства; *Patch* (патч) виправлення в системі; *Login* (логін) ідентифікатор користувача комп'ютера; *Hacker* (хакер) зловмисник, який зламує системи.

Розглядаючи терміни кібербезпеки в цілому, можна зробити спостереження, що здебільшого вони відносяться до чотирьох основних доменів: війни, здоров'я, екосистеми та інфраструктури [1]. Такий напрям вибору метафор може свідчити про те, що кіберпростір сприймається як вразлива та водночас надзвичайно важлива система, з якою слід поводитися обережно не лише на рівні окремих користувачів, а й на рівні держав. Метафоричне осмислення кіберпростору як «поля бою», «організму» чи «екосистеми» формує уявлення про необхідність його захисту, підтримання «здоров'я» цифрових мереж і забезпечення стабільності всієї кіберінфраструктури. Таким чином, метафори не просто відображають технічну реальність, а й задають стратегічне бачення ролі кіберпростору в сучасному світі як простору, що вимагає колективної відповідальності, етичного підходу та міжнародної співпраці. Такий вибір метафор формує певний фокус і задає специфічне ставлення до явища кібербезпеки.

Метафора «війни» у сфері кібербезпеки зосереджує увагу на ідеї постійного протистояння, конфлікту та необхідності оборони від ворожих держав чи зловмисних акторів. Вона формує уявлення про кіберпростір як про поле бою, де існують чітко визначені сторони нападник і захисник, а головною метою є нейтралізація загрози та збереження контролю над «територією» цифрового середовища [2]: *Cyberattack* (кібератака) цілеспрямована дія, спрямована на порушення, знищення або захоплення даних у комп'ютерній системі; *Defense in depth* (багаторівнева оборона) стратегія кіберзахисту, що передбачає створення кількох незалежних рубежів безпеки; *Vulnerability* (вразливість) слабе місце системи «дірка в обороні».

Метафора «здоров'я» у сфері кібербезпеки акцентує увагу на профілактиці, підтриманні «цифрового добробуту» та зниженні системних ризиків, подібно до підходів, що застосовуються у сфері громадського здоров'я [1]: *Virus* (вірус) шкідлива програма, що проникає у файли; *Antivirus* (антивірус) програмне забезпечення, яке «виявляє», «лікує» або «ізолює» шкідливі програми; *Quarantine*

(карантин) ізоляція заражених файлів або пристроїв для запобігання подальшому поширенню вірусу; *Health check* (перевірка стану системи) діагностика стану безпеки мережі.

Метафори «екосистеми» у сфері кібербезпеки розглядає кіберпростір як складну взаємопов'язану систему, у якій кожен елемент користувач, пристрій, програма чи організація впливає на загальний стан цифрового середовища [2]: *Environment* (середовище) цифровий простір, у якому функціонує програмне або апаратне забезпечення; *Cyber ecosystem* (кіберекосистема) сукупність взаємопов'язаних пристроїв, програм, користувачів і мережевих процесів, які взаємодіють між собою.

Різні підходи до аналізу метафоричних термінів англomовної сфери кібербезпеки дають змогу побачити багаторівневу природу цього явища. Метафоризація в технічному дискурсі не є випадковою: вона відображає особливості людського мислення, що прагне осмислити складні цифрові процеси через знайомі концепти.

Проведений аналіз метафоричних доменів війни, здоров'я, екосистеми демонструє, що мова кібербезпеки функціонує не лише як інструмент опису, а й як механізм концептуалізації реальності. Кожен домен формує окрему когнітивну модель: воєнна метафора – модель протистояння, біологічна – профілактики, екосистемна – співіснування. Разом вони створюють цілісну систему уявлень про цифровий простір, у якому людина виступає не лише користувачем, а й активним учасником глобальної мережевої взаємодії.

Таким чином, метафоричні терміни кібербезпеки є не просто лексичними одиницями, а знаковими елементами сучасного технокультурного мислення. Їхній аналіз відкриває можливості для глибшого розуміння того, як мова відображає соціальні, політичні та етичні виміри цифрової епохи. Отже, дослідження метафоричних моделей у сфері кібербезпеки не лише збагачує лінгвістичну науку, але й сприяє усвідомленню ролі мови як чинника формування колективного уявлення про безпеку, технології та відповідальність у глобальному інформаційному суспільстві.

Література

1. Lapointe A. When Good Metaphors Go Bad: The Metaphoric 'Branding' of Cyberspace. *Center for Strategic & International Studies*. 2011. URL : <https://www.csis.org/analysis/when-good-metaphors-go-bad-metaphoric-branding-cyberspace> (дата звернення: 24.09.2025).
2. National Institute of Standards and Technology Glossary. *NIST Computer Security Resource Center*. URL :

<https://csrc.nist.gov/glossary?sortBy-lg=relevance&ipp-lg=100> (дата
звернення: 24.09.2025).