***А. Левус**, студентка бакалаврату*
***О. Бабелюк**, д-р філол. н., проф.*
Львівський державний університет безпеки життєдіяльності

АДАПТАЦІЯ АНГЛОМОВНИХ ТЕКСТІВ З КІБЕРБЕЗПЕКИ У ФАХОВОМУ ДИСКУРСІ

У сучасному інформаційному просторі кібербезпека виступає одним із ключових напрямів міждисциплінарних досліджень та практичної діяльності. Переважна більшість міжнародних стандартів, нормативних документів, наукових статей і навчальних курсів у цій сфері створюється англійською мовою, що зумовлює необхідність їх адекватної адаптації для українського фахового дискурсу. В умовах активної цифровізації державних і приватних структур, а також зростання кількості кібератак, питання структурованого та коректного за єдиним принципом відтворення термінології набуває особливої актуальності.

Як зазначає О.Бабелюк, глобальні трансформаційні процеси та впровадження цифрових освітніх технологій змінюють характер професійної комунікації та вимагають нових підходів до роботи з іншомовними ресурсами, [2, с. 5]. Незважаючи на те, що цитована праця присвячена дистанційній освіті, окреслена тенденція до цифровізації професійного середовища є актуальною і для сфери кібербезпеки, де англомовні матеріали становлять основу нормативного та методичного опертя.

За джерельну базу дослідження взято матеріали про міжнародний стандарт *NIST Cybersecurity Framework*, навчальний курс *Cybersecurity Essentials (Cisco)*, наукові статті журналу *Computers & Security*, а також українські рекомендації з кібергігієни *CERT-UA*. Метою роботи є впорядкування стратегій адаптацій англомовних текстів з кібербезпеки в українському фаховому дискурсі беручи до уваги їх термінологічну, структурну та прагматичну специфіку.

Фаховий дискурс кібербезпеки характеризується високим ступенем стандартизації, термінологічною насиченість та функціональною точністю формулювань. У документі *NIST Cybersecurity Framework* модель управління ризиками структурується навколо п’яти базових функцій: *Identify, Protect, Detect, Respond, Recover* [1, с. 6]. Всі ці категорії мають концептуальну природу і формують цілісну систему управління кіберризиками. Їх буквальний переклад («ідентифікувати», «захищати», «виявляти», «реагувати», «відновлювати») не завжди відображає повноту функціонального навантаження. Наприклад, функція *Identify* поєднує процеси управління активами, оцінювання ризиків та визначення критичних ресурсів, що потребує детального тлумачення в українському контексті [1, с. 7].

У процесі адаптації таких англомовних текстів домінує калькування, яке дозволяє зберігати концептуальну симетрію терміносистем. Наприклад, *cybersecurity risk management* – управління ризиками кібербезпеки; *threat intelligence* – розвідка кіберзагроз; *access control* – контроль доступу. Використання методу калькування забезпечує структурну відповідність, проте потребує дотримання нормативних правил відповідно до української термінографічної традиції.

Навчальний курс *Cybersecurity Essentials (Cisco)* характеризується іншою жанровою специфікою. Він поєднує академічний стиль і популярні елементи, що спрямовані на трактування складних процесів широкій аудиторії. Автори наголошують на ключових поняттях, зокрема конфіденційності, цілісності та доступності (CIA triad) [3, с. 25]. Під час адаптації такого англомовного матеріалу важливо зберігати термінологічну точність, паралельно спрощуючи синтаксичні конструкції згідно з нормами українського науково-навчального стилю.

Беручи до уваги статті журналу *Computers & Security*, в яких репрезентовано академічний науковий дискурс із чіткою структурою: *abstract – methodology – results – discussion*. У таких текстах активно використовують складні іменникові словосполучення (*zero-day vulnerability exploitation, machine learning-based intrusion detection system*), для яких в українській мові необхідні трансформації через перестановку компонентів або додавання елементів для уточнення. Наприклад: *zero-day vulnerability exploitation* – вразливість нульового дня; *machine learning-based intrusion detection system* – система виявлення на основі машинного навчання. Такі трансформації належать до лексико-граматичних і забезпечують функціональну еквівалентність перекладу.

Мають прикладний характер також й українські рекомендації *CERT-UA*. Вони спрямовані на формування безпечної поведінки користувачів у цифровому середовищі. У них широко застосовують терміни, запозичені з англійської мови: *фішинг, ботнет, malware*. У цьому випадку використання стратегії транскрипції або транслітерації є доречним, оскільки це забезпечує впізнаваність понять у міжнародному професійному середовищі. Водночас CERT-UA зазвичай супроводжує подібні запозичення поясненнями, що відповідає принципу функціональної релевантності тексту [5].

Значну складність становить адаптація абревіатур. У документах міжнародного типу активно використовують скорочення, як-от *SOC* (*Security Operations Center*), *IDS* (*Intrusion Detection System*), *MFA* (*Multi-Factor Authentication*). Під час процесу адаптації доцільним вважаємо збереження англомовної абревіатури з поданням розшифрування українською мовою при первинному згадуванні, що відповідає принципам стандартизованої професійної комунікації [1, с. 12]. Як підкреслює О.Бабелюк, ефективність використання цифрових ресурсів у професійному середовищі залежить від рівня методичної адаптації та відповідності матеріалу контексту до його застосування [2, с. 9]. Відповідно, адаптація англомовних текстів з кібербезпеки охоплює не лише трансформацію мовної форми, а й врахування інституційних, правових та культурних особливостей функціонування термінів.

Отже, адаптація англомовних текстів кібербезпекового дискурсу є складним багаторівневим процесом, що передбачає використання калькування, усталених еквівалентів, транскрипції, описового перекладу та лексико-граматичних трансформацій. Її метою вважаємо забезпечення термінологічної стандартизації, концептуальної точності та функціональної адекватності в українському фаховому дискурсі. Адекватна адаптація забезпечує інтеграцію української кібербезпекової спільноти у міжнародний науково-професійний простір, а також сприяє формуванню узгодженої національної терміносистеми.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stine K., Quinn S., Witte G., Gardner R. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg: National Institute of Standards and Technology, 2018. – 48 p.
2. Babelyuk O. Using Distance EdTech for Remote Foreign Language Teaching During the COVID-19 Lockdown in Ukraine. Arab World English Journal (AWEJ). Special Issue on the English Language in Ukrainian Context, 2020. – P. 4–15. DOI: https://dx.doi.org/10.24093/awej/elt3.1
3. Brooks C.J., Grow C., Short D., Craig P. Cybersecurity Essentials. Hoboken, NJ: John Wiley & Sons Ltd, 2018. – 784 p.
4. ENISA. Threat Landscape Report 2023. Luxembourg: Publications Office of the European Union, 2023. – 120 p.
5. CERT-UA. Основні правила кібергігієни. – Київ: Державна служба спеціального зв'язку та захисту інформації України, 2023. – 32 с.