УДК 81’25
DOI https://doi.org/10.32782/tps2663-4880/2025.40.1.11

НЕОЛОГІЗМИ ДИСКУРСУ КІБЕРБЕЗПЕКИ: ПЕРЕКЛАДАЦЬКИЙ АСПЕКТ

CYBERSECURITY DISCOURSE NEOLOGISMS: TRANSLATIONAL ASPECT

Ємельянова О.В.,
orcid.org/0000-0002-3277-1227
кандидат філологічних наук, доцент,
доцент кафедри германської філології
Сумського державного університету

Шевченко Є.В.,
orcid.org/0009-0006-6089-4909
студент І курсу магістратури факультету іноземної філології та соціальних комунікацій
Сумського державного університету

У статті здійснено ґрунтовний аналіз неологізмів, що активно формуються у дискурсі кібербезпеки – надзвичайно динамічної галузі, яка стрімко розвивається під впливом цифровізації, штучного інтелекту, глобальних інформаційних викликів та зростання ролі інформаційних технологій у всіх сферах життя. Було виконано дослідження специфіки новітньої лексики, що виникає у зв’язку з потребами опису нових загроз, інструментів захисту, протоколів взаємодії та форм комунікації. З урахуванням, що неологізми часто не мають усталених перекладацьких відповідників, що створює суттєві труднощі для перекладачів, особливо в умовах відсутності загальноприйнятої термінологічної стандартизації. У роботі проаналізовано основні стратегії перекладу неологізмів: транскрипцію, транслітерацію, калькування, адаптацію, описовий переклад і комбіновані підходи. Окрема увага приділена аналізу конкретних прикладів перекладу технічних текстів, зокрема документації міжнародного стандарту ISO/IEC 27001, публіцистичних матеріалів, аналітичних звітів, нормативних актів та статей. Виявлено поширені проблеми, серед яких – багатозначність термінів, надмірне буквальне калькування, вживання запозичень без належної адаптації, розбіжності між професійною і масовою інтерпретацією термінів. Обґрунтовано потребу в міждисциплінарному підході до перекладу, який би враховував технічний, юридичний, культурний та лінгвістичний контексти. Зроблено висновок, що переклад у сфері кібербезпеки є складним і водночас креативним процесом, який має вирішальне значення для ефективної міжнародної взаємодії, інформаційної безпеки держави та формування фахової мови українською. Запропоновано конкретні рекомендації для підвищення якості перекладу, розвитку лексичного ресурсу, гармонізації термінологічної бази, а також інтеграції української фахової мови у глобальний кіберпростір.

Ключові слова: кібербезпека, неологізм, переклад, термінологія, адаптація, калькування, транскрипція.

The article provides a thorough analysis of the neologisms that are actively being formed in the discourse of cybersecurity, an extremely dynamic field that is rapidly developing under the influence of digitalization, artificial intelligence, global information challenges, and the growing role of information technology in all spheres of life. The study of the specifics of the newest vocabulary, which arises in connection with the need to describe new threats, security tools, interaction protocols and forms of communication, was carried out. It is considered that neologisms often do not have established translation equivalents, which creates significant difficulties for translators, especially in the absence of generally accepted terminological standardization. The paper analyzes the main strategies for translating neologisms: transcription, transliteration, calquing, adaptation, descriptive translation, and combined approaches. Particular attention is paid to the analysis of specific examples of translation of technical texts, including ISO/IEC 27001 documentation, journalistic materials, analytical reports, regulations, and articles. Common problems have been identified, including ambiguity of terms, excessive literal translation, use of borrowings without proper adaptation, and differences between professional and popular interpretation of terms. The need for an interdisciplinary approach to translation that would consider technical, legal, cultural and linguistic contexts is substantiated. It is concluded that translation in the field of cybersecurity is a complex and at the same time creative process that is crucial for effective international cooperation, information security of the state and the formation of a professional language in Ukrainian. Specific recommendations are offered to improve the quality of translation, develop the lexical resource, harmonize the terminology base, and integrate the Ukrainian professional language into the global cyberspace.

Key words: cybersecurity, neologism, translation, terminology, adaptation, calque, transcription.

Постановка проблеми. У сучасному цифровому середовищі кібербезпека стала ключовим елементом забезпечення інформаційної стійкості держав, організацій і приватних осіб. Розвиток технологій сприяє активному формуванню нових понять, процесів і методів, що у свою чергу генерує численні неологізми в цій галузі. Враховуючи глобальний характер кіберзагроз, потреба у точному, швидкому й адекватному перекладі цих термінів стає критично важливою. Це підкреслює актуальність вивчення не лише мовних особливостей новітньої термінології кібербезпеки, але

й розробки ефективних перекладацьких стратегій для їх трансляції українською мовою.

Дослідження неологізмів привертало увагу знаних вітчизняних науковців: Шванова О. В. [1] займалася питанням образності та багатозначності неологізмів, Мосієвич Л. В. [2] досліджував лінгвальні особливості термінів кібербезпеки та визначав низку проблем, що з ними виникають, Слободський Р. [3] є автором унікальних робіт з перекладу арабських термінів в галузі кібербезпеки, через розгляд яких можна створити уявлення про глобальну проблематику питання перекладу в цій галузі. Особливості перекладу термінів кібербезпеки на українську мову розглядав Тараненко О. Ю. [4]. Загалом у науковому просторі сформувалася низка підходів до перекладу неологізмів, проте все ще залишається низка невирішених питань. Передусім це стосується недостатньої стандартизації перекладених термінів, труднощів адаптації лексики до українського мовного середовища без втрати технічного змісту, а також проблем багатозначності, омонімії та швидкоплинності мовних новацій у сфері кібербезпеки, що обумовлює актуальність роботи. Невизначеність у виборі між буквальним перекладом і адаптацією ускладнює якісну комунікацію між фахівцями.

Об'єктом дослідження виступає нова лексика, яка виникає в дискурсі кібербезпеки. Предметом – особливості перекладу лексики українською мовою.

Метою статті є окреслення основних труднощів, що виникають при перекладі неологізмів у сфері кібербезпеки, та аналіз перекладацьких стратегій, які застосовуються для забезпечення адекватної трансляції технічної лексики.

Основні завдання передбачають класифікацію типових підходів до перекладу неологізмів у технічному дискурсі; аналіз проблем, які виникають у процесі перекладу; виявлення впливу перекладу на формування нових лексичних одиниць в українській мові.

Виклад основного матеріалу. Переклад неологізмів у сфері кібербезпеки є складним завданням, що вимагає глибокого розуміння не лише мовних процесів, а й самої галузі як такої. Використання відповідних стратегій перекладу дозволяє зберігати термінологічну точність та забезпечувати адекватну комунікацію між фахівцями. Завдання, яке стоїть перед перекладачем, – це забезпечення прозорості термінології, яка передає складні поняття. При перекладі неологізмів загалом використовуються наступні ключові стратегії, кожна з яких має свої переваги та недоліки.

Транскрипція та транслітерація

Переклад неологізмів за допомогою цього способу полягає в заміні складових частин морфем чи слів одиницями оригіналу – їхніми лексичними відповідниками мовою перекладу [5, с. 236]. Потрібно зауважити, що при такому способі перекладу можна втратити цінність слова, що перекладається [6, с. 167]. А основною перевагою є збереження точності та впізнаваності терміна. Проте серед недоліків можна відмітити більшу складність для розуміння непідготовленими користувачами, оскільки іншомовні корені не завжди можуть бути інтуїтивно зрозумілими. Наприклад: *phishing* → фішинг; *hactivism* → хактивізм; *backdoor* → бекдор.

Калькування

Калькування в кіберпезпеці є одним з найпоширеніших підходів для перекладу неологізмів, хоч ним і передається переважно еквівалента лексика [7, с. 187]. Калькування передбачає буквальний переклад складових частин терміна. Цей метод використовується для термінів, структура яких дозволяє логічно передати зміст українською мовою. Калькування передбачає існування двосторонніх міжмовних відповідностей між елементарними лексичними одиницями, які і використовуються як матеріал для відтворення внутрішньої форми нового слова. Тут основною перевагою є прозорість терміну для носіїв мови, але втрачається природність звучання і може виникати необхідність додаткового пояснення терміну. Наприклад: *firewall* → брандмауер; *zero trust architecture* → архітектура нульової довіри; *honeypot* → медова пастка.

Адаптація та осучаснення

Адаптація та осучаснення є більш гнучким методом, проте не завжди доцільним. За допомогою адаптації можна уникати складних іншомовних форм, але якщо надалі переклад термінів, які перекладаються таким чином, не пройде стандартизацію, цей метод втрачає всі переваги і лише створює непорозуміння. Наприклад: *denial of service attack* → атака на відмову в обслуговуванні; *ransomware* → вірус-вимагач.

Описовий переклад

За неможливості використання інших методів завжди можна перекласти термін використовуючи описовий переклад. Звичайно, це – не найкращий спосіб донести ідею терміну до адресата, але в довгостроковій перспективі ним не можна замінити утворення неологізмів. Також останнім часом при перекладі неологізмів застосовується також прийом прямого включення, який полягає у використанні оригі-

нального написання англійського слова в українському тексті [8, с. 243].

Наприклад: *phishing* → шахрайство з метою отримання конфіденційної інформації; *Keylogger* → програма для непомітного запису натискань клавіш.

Різноманітні гібридні підходи

Через складність і бурхливу природу кібербезпеки як сфери діяльності часто використовуються різноманітні змішані стратегії. Наприклад, термін може спочатку запозичуватися у вигляді транслітерації, а пізніше – адаптуватися, або отримати описовий варіант. Наприклад, неологізм *ransomware* спочатку часто використовувався у перекладах як *рансомвар*, але зараз у текстах частіше зустрічається *вірус-вимагач*. Тобто в перекладах з одного терміну виникло 2 неологізми, один з яких був цілком актуальним і підпорядковувався загальним методам перекладу, але з певних причин був замінений іншим.

Проаналізуємо переклади з огляду на важливість їх узгодження відповідно до вимог міжнародного стандарту ISO/IEC 27001, який встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки організацій. Переклад виконаний перекладачами І. Івченко, М. Карнаух, Т. Тищенко.

Проаналізуємо текст оригіналу з офіційного видання [10, с. 7] та з його перекладом [9, с. 6] (таб. 1).

В проаналізованому матеріалі зустрічаємо наступні особливості перекладу термінів кібербезпеки:

externally provided processes – процеси, віддані на аутсорсинг.

У запропонованому перекладі використано уточнення та запозичення. Застосування для перекладу терміну *аутсорсинг* можна виправдати, оскільки він активно використовується у кібербезпеки. Альтернативними перекладами могли б бути «*зовнішні процеси*» або «*процеси, виконані третьою стороною*».

Information security risk assessment – оцінювання ризиків інформаційної безпеки.

Перекладач використав калькування з трансформацією. Термін є відносно усталеним, альтернативою може бути «*аналіз ризиків інформаційної безпеки*».

Таблиця 1

Текст оригіналу	Переклад
8 Operation 8.1 Operational planning and control The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: – establishing criteria for the processes; – implementing control of the processes in accordance with the criteria. Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. 8.2 Information security risk assessment The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments. 8.3 Information security risk treatment The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	8 ФУНКЦІОНУВАННЯ 8.1 Робоче планування й контроль Організація повинна планувати, впроваджувати й контролювати процеси, необхідні для виконання вимог інформаційної безпеки, а також впроваджувати дії, визначені в 6.1. Організація також повинна впроваджувати плани для досягнення цілей інформаційної безпеки, визначених в 6.2. Організація повинна зберігати документовану інформацію в обсязі, необхідному для впевненості, що процес виконується як було заплановано. Організація повинна контролювати заплановані зміни та переглядати наслідки непередбачених змін, застосовуючи дії для усунення будь-яких шкідливих дій, за потреби. Організація повинна гарантувати, що процеси, віддані на аутсорсинг, визначені й контрольовані. 8.2 Оцінювання ризиків інформаційної безпеки Організація повинна виконувати оцінювання ризиків через заплановані інтервали або коли запропоновані чи відбуваються суттєві зміни з урахуванням критеріїв, визначених в 6.1.2 a). Організація повинна зберігати задокументовану інформацію стосовно результатів оцінюван ня ризиків інформаційної безпеки. 8.3 Оброблення ризиків інформаційної безпеки Організація повинна впровадити план оброблення ризиків інформаційної безпеки. Організація повинна зберігати задокументовану інформацію стосовно результатів оброблення ризиків інформаційної безпеки.

Прикладами з інших частин перекладу документації ISO/IEC 27001 є:

compliance – комплаєнс. Перекладач використовує транскрипцію англійського слова, без адаптації, через, що можуть викликати труднощі його сприйняття за межами контексту кібербезпеки. Для подальшого покращення перекладів можна схилятися до варіантів «*відповідність нормативам*» або «*регуляторна відповідність*».

Fault tolerance – відмово стійкість.

Термін означає здатність системи продовжувати роботу навіть у разі відмови деяких компонентів. Перекладач використовує калькування з адаптацією. Альтернативними варіантами, які могли б покращити загальне звучання, могли б бути «*стійкість до збоїв*» або «*неперервність функціонування*».

Vulnerability threat – загроза вразливості.

Термін означає потенційну загрозу, яка може скористатися вразливістю в інформаційній системі. Переклад є дослівним і зрозумілим, проте створює логічну неточність і звучить неприродно. Альтернативними варіантами можуть бути «*ризик вразливості*», «*загроза безпеці через вразливість*».

Authentication – автентифікація.

Вже досить поширений термін, що означає процес підтвердження особи користувача або пристрою в системі. В українській мові саме переклад через транслітерацію цього терміну вкорінився через поширення слова автентичний. Серед альтернативних перекладів існують «*підтвердження особи*» або «*перевірка достовірності даних*».

Traceability – відстежуваність.

Термін означає здатність відстежити зміну або рух даних у системі. Це – приклад перекладу через калькування з морфологічною адаптацією, через що може потенційно втрачатися сенс оригінального слова за межами контексту кібербезпеки і в той же час звучати штучно для фахівців. Проте переклад через транслітерацію був би невиправданим, і, як альтернативу, можна запропонувати «*можливість відстеження*».

Cryptographic resilience – криптостійкість.

Термін означає здатність криптографічних алгоритмів протистояти атакам. Перекладач використав калькування з елементами словотворення, шляхом поєднання «*крипто-*» та «*стійкість*». Загалом створений варіант є дуже вдалим, він зберігає оригінальну суть терміну, при цьому завдяки поєднанню елементів може бути зрозумілим широкій аудиторії. В інших контекстах природніше міг би звучати альтернативний варіант, словосполучення «*криптографічна стійкість*».

Роблячи аналіз перекладу стандарту ISO/IEC 27001:2015, можна зазначити, що він переважно є точним та відповідає вимогам термінологічної стандартизації в Україні. Структура та зміст здебільшого залишається ідентичними оригінальному англійському тексту, що забезпечує відповідність міжнародним нормам. Загалом серед позитивних аспектів перекладу можна визначити: збереження формальної структури документу; нумерація, загальна структура та порядок пунктів та їхній зміст повністю відповідають оригіналу; активне застосування вже стандартизованих термінів; перекладачі дотримуються термінології, що вже була узгоджена в інших стандартах; зрозумілість та формальну точність.

Більшість термінів є адаптованими до української мови, а пояснення збережено у вигляді прямих кальок або пояснювальних перекладів.

В той же час можна виділити низку пунктів, що вимагають покращення, а саме: терміни, що перекладаються через калькування місцями звучать неприродно;

запозичення, що перекладались без адаптації, не будуть зрозумілими для людей, які не є безпосередньо частиною сфери кібербезпеки; частина речень мають надто буквальний і дослівний переклад.

Висновки та перспективи подальших досліджень. Ґрунтовний аналіз свідчить, що переклад неологізмів у сфері кібербезпеки вимагає балансування між термінологічною точністю та адаптацією до мовних норм. Найбільш поширеними методами залишаються калькування, транскрипція та описовий переклад. Проте відсутність уніфікованих стандартів перекладу, а також мовна і технічна варіативність понять ускладнюють процес трансляції нової лексики. Перспективу дослідження вбачаємо у глибокому аналізі перекладу новітніх термінів та формуванні рекомендацій для перекладачів у галузі кібербезпеки. Вельми актуальною є розробка глосаріїв нової термінології.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Шванова О. В. Особливості перекладу термінів із кібербезпеки : Науковий вісник Міжнародного гуманітарного університету. Сер.: Філологія. Том 3, 2023. С. 180–183.

2. Мосієвич Л. В. Лінгвальні особливості англомовних термінів кібербезпеки та їх переклад українською мовою, Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика, 2024, С. 242–247.

3. Слободський Р. Переклад комп'ютерних термінів сфери кібербезпеки з арабської мови українською : Вісник Київського національного університету імені Тараса Шевченка. Літературознавство. Мовознавство. Фольклористика, 2018, С. 49–50.

4. Тараненко О. Ю. Особливості перекладу на українську мову англійських термінів з Кібербезпеки (на матеріалі англомовного наукового дискурсу) URL: http://rep.knlu.edu.ua/xmlui/handle/787878787/6068.

5. Стефанюк М. Гулян Б. Особливості перекладу неологізмів : Філологічні студії та перекладознавчий дискурс, 2024, С. 235–237.

6. Козаченко І. В. Особливості перекладу неологізмів англійської мови Науковий вісник Міжнародного гуманітарного університету. Філологія, 2016 URL: http://www.vestnik-philology.mgu.od. ua/archive/v25/part_2/50.pdf

7. Приходько Є. С. Особливості перекладу англійських семантичних неологізмів : Науковий вісник Міжнародного гуманітарного університету, 2016, С. 186–188.

8. Данкевич. Т. Переклад авторських неологізмів в англійській мові : Київський національний лінгвістичний університет, Київ, 2014. С. 341–344.

9. Івченко І., Карнаух М., Тищенко Т. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) : ДП «УкрНДНЦ», Київ, 2016.

10. Information security, cybersecurity and privacy protection – Information security management systems – Requirements, International Organization for Standardization, Switzerland, 2014.

11.Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності : Інформація і право, 2012 С. 162–175.