ISSN 3041-1564 (Online), ISSN 3041-1556 (Print)

УДК 81’373.21:004.056:32.019.51
DOI https://doi.org/10.32782/modernph-2025.4.17

МЕНЕДЖМЕНТ КІБЕРЗАХИСТУ ТА МОВНА ПОЛІТИКА: РОЛЬ УКРАЇНСЬКОЇ ПРОФЕСІЙНОЇ ТЕРМІНОЛОГІЇ

Кузьманенко Аліса Валеріївна,
кандидат філологічних наук,
доцент кафедри журналістики і мовної комунікації
Національного університету біоресурсів і природокористування України
ORCID ID: 0009-0008-1245-7821

У статті досліджується взаємозв’язок між менеджментом у сфері кіберзахисту та мовною політикою, з акцентом на роль української професійної термінології у забезпеченні ефективної комунікації між фахівцями. Проаналізовано сучасний стан української терміносистеми кіберзахисту, визначено поширені проблеми перекладу та наведено приклади стандартизованих відповідників для широко вживаних англомовних термінів. Особливу увагу приділено ризикам, що виникають через термінологічну неузгодженість, яка може спричиняти непорозуміння у процесі реагування на інциденти та міжнародної співпраці. У роботі підкреслюється необхідність розроблення єдиних стандартів перекладу, створення офіційних глосаріїв і впровадження української кіберзахисної термінології в освітні та нормативні документи. Зроблено висновок, що мовна уніфікація є не лише технічною потребою, а й важливим чинником національної безпеки та цифрового суверенітету.

Ключові слова: *менеджмент кіберзахисту, мовна політика, українська професійна термінологія, кіберзагрози, стандартизація термінології, цифровий суверенітет, реагування на інциденти.*

Kuzmanenko Alisa. Cybersecurity Management and Language Policy: The Role of Ukrainian Professional Terminology

The article explores the interrelation between cybersecurity management and language policy, emphasizing the role of Ukrainian professional terminology in ensuring effective communication among specialists. The author analyzes the current state of Ukrainian cyber terminology, identifies common translation issues, and provides examples of standardized equivalents for widely used English terms. A special focus is placed on the risks of inconsistent terminology, which can lead to misunderstandings in incident response and international cooperation. The study highlights the need for unified translation standards, the development of official glossaries, and the integration of Ukrainian cyber terminology into educational and regulatory documents. It concludes that linguistic unification is not only a technical necessity but also an essential element of national security and digital sovereignty.

Key words: *cybersecurity management, language policy, Ukrainian professional terminology, cyber threats, terminology standardization, digital sovereignty, incident response.*

Вступ. У сучасному світі кіберзагрози стали одним із ключових викликів для держав, бізнесу та приватних користувачів. Ефективний менеджмент кіберзахисту вимагає не лише впровадження новітніх технологій, а й чіткої, стандартизованої комунікації між фахівцями. Українська професійна мова кібербезпеки є важливим елементом цифрового суверенітету та інформаційної безпеки держави. Її розвиток тісно пов’язаний із мовною політикою, яка визначає, яким чином формуються, стандартизуються та впроваджуються терміни у практичну діяльність і навчальний процес.

Метою статті є обґрунтування значення української професійної мови кібербезпеки як чинника ефективного управління у сфері інформаційної безпеки, а також виявлення проблем та шляхів стандартизації термінології з урахуванням мовної політики України.

Виклад основного матеріалу. Менеджмент кіберзахисту – це система організації,

планування та контролю заходів, спрямованих на запобігання кіберзагрозам, реагування на інциденти та відновлення після атак [1; 2]. Успішне управління потребує координації між технічними спеціалістами, аналітиками, юристами та керівництвом. Без єдиної термінологічної бази існує ризик непорозумінь, що може призвести до затримок у реагуванні на загрози.

Сьогодні, в умовах війни та глобальної цифрової інтеграції, мовна політика стає одним із ключових чинників забезпечення інформаційної безпеки та цифрового суверенітету держави. Використання української мови у сфері кіберзахисту має не лише комунікативний, а й стратегічний вимір, адже мова термінології визначає рамки правового регулювання, професійної підготовки й міждержавної взаємодії. У цьому контексті доречно звернутися до поняття мовної політики, адже саме вона задає засади для унормування й розвитку професійної лексики, включно з терміносистемою кіберзахисту.

За визначенням, запропонованим О. Тараненком, мовна політика – це «система цілеспрямованих заходів держави та суспільних інституцій щодо регулювання функціонування мов у різних сферах суспільного життя» [3]. Саме в такому контексті вона постає не лише як культурний чи освітній інструмент, а як фундаментальний чинник формування цифрової безпеки. Як слушно підкреслює Л. Масенко [4], мовна політика завжди пов'язана з питаннями державності й суверенітету, а у цифрову добу вона безпосередньо впливає на якість і незалежність національної інформаційної інфраструктури.

Мовна політика у кіберзахисті передбачає впровадження стандартів використання термінів, адаптацію міжнародних понять до українського контексту та формування власної терміносистеми. Це важливо не лише для внутрішньої комунікації, але й для міжнародної взаємодії, адже фахівці повинні коректно розуміти одне одного під час обміну інформацією з партнерами. Розвиток української термінології кіберзахисту тісно пов'язаний з інтеграцією у міжнародний простір та гармонізацією стандартів. На глобальному рівні значний вплив мають документи Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC), зокрема стандарт ISO/IEC 27032:2023 що визначає засади кібербезпеки як комплекс заходів для захисту від інцидентів у кіберпросторі (ISO/IEC, 2012). Його положення стосуються не лише технічних засобів, але й організаційних, управлінських та лінгвістичних аспектів, оскільки правильне розуміння термінів є запорукою узгодженості дій між різними суб'єктами.

В українському контексті прийнято низку нормативних актів, що покликані адаптувати міжнародні підходи. Наприклад, оновлений стандарт ДСТУ ISO/IEC 27032:2004 «Інформаційні технології. Методи захисту ДСТУ ISO/IEC 27032:2024 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2023, IDT)», встановлює термінологію засобів контролю інформаційної безпеки та сприяє гармонізації української практики з міжнародними нормами [5]. Проте навіть за наявності цього документу проблема варіативності термінів залишається актуальною.

Сьогодні більшість термінів у сфері кіберзахисту має англомовне походження. Частина з них використовується без перекладу, інші – адаптовані українською, але часто з кількома варіантами перекладу. Це створює ситуацію, коли одне поняття може називатися по-різному, що шкодить однозначності сприйняття.

У багатьох наукових дослідженнях підкреслюється, що в Україні бракує єдиного механізму координації термінотворення у сфері кібербезпеки, що призводить до використання відмінних варіантів перекладу одного й того ж терміна в різних інституціях [6]. Наприклад, терміни *cyberthreat* та *cyber risk* у деяких джерелах передаються як «*кіберзагроза*» та «*кіберризик*», а в інших – як «*загроза у кіберпросторі*» та «*ризик інформаційної безпеки*». Це ускладнює вироблення єдиної стратегії комунікації між фахівцями та створює ризики непорозумінь під час реагування на інциденти.

Т. Ботвин у своєму дослідженні щодо термінології кіберзахисту переконливо доводить, що сліпе перенесення іншомовних моделей не лише ускладнює сприйняття термінів широким колом користувачів, а й знижує точність та однозначність фахової комунікації [7]. Кальки часто сприймаються як «жаргонізми», що віддаляє професійну

мову від академічного стандарту та створює додаткові бар'єри для міждисциплінарної взаємодії.

Окрім того, однією з ключових проблем формування української професійної мови кібербезпеки є надмірне калькування англомовних термінів, що часто призводить до виникнення термінологічного «суржику». Така ситуація характерна не лише для початкових етапів становлення терміносистеми, але й для сучасного етапу, коли швидкість появи нових понять у цифровій сфері перевищує можливості офіційної стандартизації. Наприклад, термін *firewall* довгий час уживався в українських текстах у вигляді кальки «*фаєрвол*», тоді як у сучасних офіційних словниках та нормативних документах закріплено відповідник «*міжмережевий екран*». Аналогічна ситуація спостерігається із термінами *phishing* («*фішинг*»), *spoofing* («*спуфінг*») та *backdoor* («*бекдор*»), де іншомовні варіанти співіснують із нормативними перекладами «*шахрайство з використанням електронної пошти*», «*підміна даних*» та «*прихований канал доступу*».

Ще однією проблемою є дублювання термінів через намагання одночасно закріпити кілька варіантів перекладу. Так, наприклад поняття *cybersecurity awareness* може перекладатися як «*усвідомлення кібербезпеки*», «*поінформованість з кібербезпеки*» та «*культура кіберзахисту*». Відсутність єдності у термінужитку ускладнює створення навчальних програм і нормативної документації.

З метою ілюстрації зазначеної проблеми у таблиці 1 подано приклади англомовних термінів у сфері кіберзахисту та їхні офіційні українські відповідники, унормовані у чинних нормативних документах і відображені в наукових джерелах. Додатково наведено коментарі щодо особливостей їхнього практичного функціонування, які відображають актуальні тенденції професійного вжитку. Такий підхід не лише фіксує сучасний стан професійного вжитку, але й створює підґрунтя для розробки рекомендацій щодо подальшого унормування та розвитку української термінології у сфері кіберзахисту.

Представлений матеріал демонструє, що уніфікація термінології виступає не

Таблиця 1

Приклади вживання англомовних термінів кіберзахисту та їх українських відповідників

№	Англійський термін	Український відповідник	Коментарі щодо вживання
1	Firewall	Мережевий екран	Інколи у мові зустрічається використання «міжмережевий екран»; варто уникати кальки «фаєрвол»
2	Phishing	Фішинг	Можливо використовувати описовий варіант: шахрайське виманювання даних
3	Malware	Шкідливе програмне забезпечення	Радимо уникати використання варіанту «малваре» як неадаптованого запозичення
4	Spoofing	Підміна даних	Необхідна конкретизація як метод перекладу: підміна IP-адреси, підміна електронної пошти
5	Endpoint	Кінцева точка	На наш погляд, доцільнішим є переклад «кінцевий вузол», проте за певних умов переклад цього терміна залежить від контексту
6	Cyber threat intelligence	Розвідка кіберзагроз	Термін використовується у сфері воєнної кібербезпеки
7	Intrusion detection system	Система виявлення вторгнень	Абревіатура IDS може вживатися паралельно з перекладом
8	Data breach	Порушення цілісності даних	Також використовують переклад «витік даних» (у вузькому контексті)
9	Zero-day vulnerability	Уразливість нульового дня	Нерідко вживають поряд з англомовним терміном
10	Penetration testing	Тестування на проникнення	Часто використовується абревіатура pentest; можливий варіант перекладу: «перевірка на проникнення»
11	Security policy	Політика безпеки	Доцільно вживати у множині, якщо йдеться про набір політик («політики безпеки»)
12	Incident response	Реагування на інциденти	Подекуди вживається у вигляді «план реагування на інциденти»

лише необхідною передумовою ефективної комунікації між фахівцями та підвищення рівня національної цифрової безпеки, але й інструментом подолання наслідків надмірного калькування англомовних понять, запобігання поширенню термінологічного «суржику» та забезпечення належного функціонування української професійної мови у сфері кіберзахисту. У цьому контексті важливим завданням є системна робота над упорядкуванням термінів шляхом укладання офіційних глосаріїв і словників, заснованих на лінгвістичних принципах і національних традиціях термінотворення. Прикладом такої роботи є «Англо-український словник термінів з інформаційних технологій та кібербезпеки» [8], що містить не лише переклади, але й обґрунтування вибору термінів, що суттєво підвищує їхню наукову й практичну цінність. Це сприятиме уніфікації комунікації між фахівцями та мінімізує ризик помилок у критичних ситуаціях.

Однак традиційні методи термінотворення, засновані на тривалій експертній роботі, обговореннях та затвердженні науковими комісіями, потребують значного часу й людських ресурсів. У той же час динаміка розвитку цифрових технологій і поява нових кіберзагроз відбувається настільки стрімко, що класичні підходи часто не встигають за потребами практики. Ця суперечність актуалізує потребу у використанні сучасних технологічних інструментів, насамперед штучного інтелекту. Інтелектуальні системи здатні автоматизувати процес створення, аналізу та стандартизації термінів, спираючись на міжнародну практику та водночас адаптуючи її до норм української мови. Такий підхід відкриває нові можливості для поєднання наукової обґрунтованості з оперативністю реагування на глобальні виклики, що особливо важливо у сфері кіберзахисту, де навіть невелика термінологічна неточність може мати серйозні наслідки для безпеки.

Проте автоматизоване термінотворення не може замінити освітнього складника, адже ефективність будь-якої термінологічної системи визначається рівнем її засвоєння фахівцями. Саме тому важливим кроком є розробка навчальних курсів з української мови для спеціалістів у сфері кібербезпеки. Такі програми, орієнтовані на опанування спеціалізованої термінології та практичних комунікативних навичок, сприятимуть підвищенню мовної грамотності ІТ-фахівців та менеджерів кіберзахисту. Вони також забезпечать інтеграцію української мови в міжнародні проєкти та дослідження з кібербезпеки, створюючи умови для повноцінної участі України у світовому цифровому просторі.

Разом із тим розвиток української професійної мови у сфері кіберзахисту неможливий без налагодження міждисциплінарної співпраці. Лінгвісти забезпечують точність і системність термінотворення, менеджери формують організаційні моделі впровадження стандартів у практику, а ІТ-експерти гарантують технологічну релевантність нових понять. Спільні дослідницькі та практичні ініціативи цих груп створюють необхідні передумови для комплексного розвитку термінології, яка стає не лише мовним, а й стратегічним інструментом національної безпеки. У результаті українська мова кіберзахисту набуває подвійного значення: як засіб професійної комунікації та як чинник зміцнення цифрового суверенітету держави.

Висновки. Проведений аналіз засвідчив, що менеджмент кіберзахисту невіддільний від мовної політики, адже точність, уніфікованість і зрозумілість термінології безпосередньо впливають на ефективність реагування на сучасні цифрові загрози. Українська професійна терміносистема у сфері кібербезпеки перебуває на етапі активного становлення й потребує подальшої стандартизації, офіційного закріплення та широкого впровадження в освітню і практичну площини. Це завдання має не лише технічне, а й стратегічне значення, оскільки мовна точність і єдність формують основу інформаційної безпеки та цифрового суверенітету держави.

Розвиток української мови у сфері кіберзахисту не може обмежуватися суто лінгвістичними напрацюваннями: він вимагає комплексного підходу, що включає співпрацю науковців, перекладачів, ІТ-фахівців і управлінців. Системна мовна політика в цій галузі повинна забезпечувати поєднання національних традицій термінотворення з міжнародними стандартами, створюючи підґрунтя для незалежного й безпечного розвитку цифрового суспільства в Україні.

Перспективи дослідження. Перспективними напрямами подальших досліджень є розроблення галузевого стандарту укра-

їнської терміносистеми кібербезпеки, створення інтерактивних термінологічних баз даних із можливостями штучного інтелекту, а також аналіз взаємодії мовної політики України з міжнародними процесами гармонізації кіберзахисних норм. Окремої уваги потребує розробка україномовних навчальних програм, підручників і курсів підвищення кваліфікації для перекладачів та фахівців у сфері кіберзахисту, що забезпечить інтеграцію української мови в глобальний цифровий простір і зміцнить позиції держави у світовій системі інформаційної безпеки.

Література:

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization. URL: https://www.iso.org/standard/27001 (дата звернення: 05.08.2025)
2. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT) URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795 (дата звернення: 07.08.2025)
3. Тараненко О. О. Мовна ситуація і мовна політика в Південно-Східному регіоні України. *Вісник університету внутрішніх справ*. Вип. 7(2). 1999. С. 163-170. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_1999_7(2)__26. (дата звернення: 03.08.2025)
4. Масенко Л. Т. Мовна політика України у 2017–2019 роках. *Українська мова*. № 3. 2019. С. 40-51. URL: http://nbuv.gov.ua/UJRN/Ukrm_2019_3_6 (дата звернення: 06.08.2025)
5. ДСТУ ISO/IEC 27032:2024 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2023, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=112376 (дата звернення: 05.08.2025)
6. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Збірник наукових праць Київського національного університету імені Тараса Шевченка*. Вип. № 30. 2011. С. 165–172.
7. Ботвин Т. М. Щодо англомовної термінологічної системи сектора кібербезпеки України в умовах воєнного стану: аналіз дефініцій. *Вчені записки ТНУ імені В. І. Вернадського*. Серія: Філологія. Соціальні комунікації. № 33(2). 2022. С. 23–28. URL: https://sci.ldubgd.edu.ua/handle/123456789/11604 (дата звернення: 08.08.2025)
8. Англо-український словник термінів з інформаційних технологій та кібербезпеки / Гладун А. Я. та ін. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/handle/123456789/45895/ (дата звернення: 07.08.2025)

References:

1. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva: ISO. Retrieved from: https://www.iso.org/standard/27001
2. Derzhspozhyvstandart Ukrainy. (2019). *DSTU ISO/IEC 27000:2019 Informatsiini tekhnolohii. Metody zakhystu. Systemy keruvannia informatsiinoiu bezpekoiu. Ohliad i slovnyk terminiv (ISO/IEC 27000:2018, IDT)* [Information technology – Security techniques – Information security management systems – Overview and vocabulary]. Kyiv. Retrieved from: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795
3. Taranenko, O.O. (1999). *Movna sytuatsiia i movna polityka v Pivdenno-Skhidnomu rehioni Ukrainy* [Language situation and language policy in the South-Eastern region of Ukraine]. *Visnyk universytetu vnutrishnikh sprav* [Bulletin of the University of Internal Affairs], 7(2), 163–170. Retrieved from: http://nbuv.gov.ua/UJRN/VKhnuvs_1999_7(2)__26
4. Masenko, L.T. (2019). *Movna polityka Ukrainy u 2017–2019 rokakh* [Language policy of Ukraine in 2017–2019]. *Ukrainska mova* [Ukrainian Language], (3), 40–51. Retrieved from: http://nbuv.gov.ua/UJRN/Ukrm_2019_3_6
5. Derzhspozhyvstandart Ukrainy. (2024). *DSTU ISO/IEC 27032:2024 Informatsiini tekhnolohii. Metody zakhystu. Nastanovy shchodo kiberbezpeky (ISO/IEC 27032:2023, IDT)* [Information technology – Security techniques – Guidelines for cybersecurity]. Kyiv. Retrieved from: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=112376
6. Melnyk, S.V., Tykhomyrov, O.O., & Lienkov, O.S. (2011). *Do problemy formuvannia poniatiino-terminolohichnoho aparatu kiberbezpeky* [On the problem of formation of the conceptual and terminological apparatus of cybersecurity]. *Zbirnyk naukovykh prats Kyivskoho natsionalnoho universytetu imeni Tarasa*

Shevchenka [Collection of Scientific Works of Taras Shevchenko National University of Kyiv], (30), 165–172.
7. Botvyn, T.M. (2022). *Shchodo anhlomovnoi terminolohichnoi systemy sektora kiberbezpeky Ukrainy v umovakh voiennoho stanu: analiz definitsii* [On the English-language terminological system of the cybersecurity sector of Ukraine under martial law: Definition analysis]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Filolohiia. Sotsialni komunikatsii* [Scientific Notes of V. I. Vernadsky Taurida National University. Series: Philology. Social Communications], 33(2), 23–28. Retrieved from: https://sci.ldubgd.edu.ua/handle/123456789/11604
8. Hladun, A. Ya., Puchkov, O. O., Subach, I. Yu., & Khala, K. O. (2018). *Anhlo-ukrainskyi slovnyk terminiv z informatsiinykh tekhnolohii ta kiberbezpeky* [English-Ukrainian dictionary of terms in information technologies and cybersecurity]. Kyiv: ISSZZI KPI im. Ihoria Sikorskoho. Retrieved from: https://ela.kpi.ua/handle/123456789/45895

Стаття надійшла до редакції 16.08.2025
Стаття прийнята 21.09.2025
Статтю опубліковано 27.10.2025