МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
Кафедра «Іноземна філологія та переклад»

КВАЛІФІКАЦІЙНА РОБОТА

АНГЛОМОВНА ПРОФЕСІЙНА ЛЕКСИКА КІБЕРБЕЗПЕКИ: СТРУКТУРА, СЕМАНТИКА, ПЕРЕКЛАД

Виконав	студент групи ГФ-314м **Животченко Олександр Миколайович**
Рівень вищої освіти	Другий (магістерський)
Галузь знань	03 Гуманітарні науки
Спеціальність	035 Філологія
Спеціалізація	035.041 Германські мови та літератури (переклад включно), перша – англійська
Керівник	к.філол.н, доц. І. В. Кузнєцова

Запоріжжя – 2025

Національний університет «Запорізька політехніка»

Факультет гуманітарний
Кафедра «Іноземна філологія та переклад»
Ступінь вищої освіти другий (магістерський)
Спеціальність 035 «Філологія»
Освітня програма (спеціалізація) 035.041 Германські мови та літератури (переклад включно), перша – англійська»

«ЗАТВЕРДЖУЮ»
В.о. завідувачки кафедри
доц. Н. М. Жукова
_____
«____» грудня 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Животченка Олександра Миколайовича

1. Тема кваліфікаційної роботи: **АНГЛОМОВНА ПРОФЕСІЙНА ЛЕКСИКА КІБЕРБЕЗПЕКИ: СТРУКТУРА, СЕМАНТИКА, ПЕРЕКЛАД**
керівник кваліфікаційної роботи *Кузнєцова Ірина Володимирівна, к. філол. н., доцент кафедри «Іноземна філологія та переклад»*
затверджені наказом закладу вищої освіти від «13» листопада 2025 р. № 508.

2. Строк подання студентом кваліфікаційної роботи: 18 грудня 2025 р.

3. Вихідні дані кваліфікаційної роботи: *теоретичні та критичні праці вітчизняних та зарубіжних дослідників (Білозерська Л. П., Вдовенко С., Даник Ю., Ботвин Т., Гладун А., Кияк Т., Фараон С., Шванова О., Liu H, Johansen A., Schatz D. ін.), а також суцільна вибірка термінів досліджуваної тематики з відповідних текстів та лексикографічних джерел.*

4. ЗМІСТ розрахунково-пояснювальної записки (перелік питань, що їх належить розробити): *ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ АСПЕКТИ ВИВЧЕННЯ АНГЛОМОВНОЇ ТЕРМІНОЛОГІЇ КІБЕРБЕЗПЕКИ. Загальна характеристика терміна та суміжних понять. Англомовні терміни кібербезпеки. Історія розвитку англомовної терміносистеми кібербезпеки. Методика добору та аналізу матеріалу. СТРУКТУРНО-СЕМАНТИЧНІ ОСОБЛИВОСТІ АНГЛОМОВНИХ ТЕРМІНІВ КІБЕРБЕЗПЕКИ. Морфологічні особливості англомовної терміносистеми кібербезпеки. Семантичні особливості англомовних термінів кібербезпеки. ОСОБЛИВОСТІ ПЕРЕКЛАДУ АНГЛОМОВНОЇ ТЕРМІНОЛОГІЇ КІБЕРБЕЗПЕКИ. Переклад простих та складних англомовних термінів кібербезпеки.Переклад*

англомовних термінів-словосполучень кібербезпеки. Труднощі перекладу скорочень англомовної термінології кбербезпеки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):

6. Консультанти розділів кваліфікаційної роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
I	Кузнєцова І.В, к. філол. н., доцент		
II	Кузнєцова І. В., к. філол. н., доцент		
III	Кузнєцова І. В., к. філол. н., доцент		
Нормоконтроль	Лещенко Г. А., к. філол. н., доцент		

7. Дата видачі завдання «11» вересня 2025 року.

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів кваліфікаційної роботи	Примітка
1.	Вибір теми кваліфікаційної роботи	вересень 2025	виконано
2.	Розробка завдання на кваліфікаційну роботу	вересень 2025	виконано
3.	Складання календарного плану кваліфікаційної роботи	вересень 2025	виконано
4.	Збирання матеріалу	жовтень 2025	виконано
5.	Підготовка розділу 1	жовтень 2025	виконано
6.	Підготовка розділу 2	жовтень 2025	виконано
7.	Підготовка розділу 3	листопад 2025	виконано
8.	Написання вступу і загальних висновків роботи	листопад – грудень 2025	виконано
9.	Оформлення кваліфікаційної роботи	грудень 2025	виконано
10.	Проходження нормоконтролю	грудень 2025	виконано
11.	Рецензування кваліфікаційної роботи	грудень 2025	виконано
12.	Захист кваліфікаційної роботи	грудень 2025	виконано

Студент Животченко О. М.

Керівник проєкту (роботи) Кузнєцова І. В.

РЕФЕРАТ

Кваліфікаційна робота: 232 с., 3 додатка, 114 джерел.

Об’єкт дослідження – англомовні терміни кібербезпеки.

Мета роботи – вивчення та опис англомовних термінів кібербезпеки, їх структурних та семантичних особливостей й способів перекладу українською мовою.

Методи дослідження – описово-аналітичний; тезаурусний; структурний; контекстуальний; семантичний; діахронічний аналіз; етимологічний аналіз; історичний аналіз; перекладацький аналіз.

У першому розділі кваліфікаційної роботи розкрито теоретичні засади термінознавства, зокрема визначено сутність понять «термін», «термінологія» та «терміносистема». Простежено етапи становлення та розвитку англомовної терміносистеми кібербезпеки, сформованої під впливом технологічного прогресу та глобальних викликів. Також розглянуто методологічні підходи до дослідження галузевої термінології. Другий розділ присвячено дослідженню структурно-семантичних особливостей англомовних термінів кібербезпеки. Визначено основні словотворчі моделі, механізми та засоби утворення цих термінів. Проаналізовано їх частиномовну структуру. Особливу увагу приділено ключовим семантичним процесам у терміносфері: термінологізації загальновживаної лексики, детермінологізації та ретермінологізації. У третьому розділі здійснюється детальний аналіз способів перекладу англомовних термінів кібербезпеки з урахуванням структурних, семантичних особливостей; досліджуються лексико-семантичні та граматичні трансформації, що застосовувані при перекладі речень із вказаними одиницями, та розглядаються труднощі перекладу англомовних термінів кібербезпеки.

ТЕРМІН, ТЕРМІНОЛОГІЯ КІБЕРБЕЗПЕКИ, ТЕРМІНОСИСТЕМА, СТРУКТУРА, СЕМАНТИКА, СКОРОЧЕННЯ, ПЕРЕКЛАД, ЛЕКСИЧНІ ТРАНСФОРМАЦІЇ, СПОСОБИ ПЕРЕКЛАДУ

ЗМІСТ

ВСТУП

Стрімка цифровізація суспільства зумовлює посилення значення кібербезпеки як ключового чинника захисту інформаційних ресурсів, критичної інфраструктури та персональних даних. Оскільки англійська мова виконує роль основного засобу фахової комунікації в галузі інформаційних технологій, саме вона формує потужну та динамічну терміносистему кібербезпеки. Значний масив цієї термінології активно запозичується українською мовою, часто без належного урахування структурно-семантичних особливостей оригіналів, що призводить до семантичних неточностей, термінологічної розпорошеності та помилок у професійній комунікації. Зазначені чинники зумовлюють необхідність системного аналізу структурно-семантичних характеристик англомовних термінів кібербезпеки та розробки науково обґрунтованих принципів їх перекладу українською мовою.

Останнім часом спостерігається значне зростання наукового інтересу до термінології кібербезпеки як спеціалізованого лексичного шару. Лінгвісти все більше уваги приділяють питанням формування, структурної організації та семантичної специфіки цієї термінології, а також проблемам її перекладу та стандартизації в умовах прискореної цифровізації. Незважаючи на зростаючу кількість наукових праць, структурно-семантичні особливості англомовної термінології кібербезпеки залишаються недостатньо дослідженими.

Сучасна термінологічна система кібербезпеки формується під впливом інтенсивного розвитку технологій, що знаходить відображення у постійному поповненні термінології новими одиницями, утворенні багатокомпонентних термінологічних сполучень та активній інтернаціоналізації лексики. Проте в українському мовознавстві відзначається дефіцит комплексних досліджень, присвячених перекладу та адаптації англомовних термінів кібербезпеки.

Існуючі праці таких учених, як І. Асмукович [2], А. Басова [5], Р. Лук'янчука [44], Л. Тарасова [65], Л. Халіновської [68], С. Фараон [66], О. Шванової [70], В. Черновола [69], О. Баранова [4], С. Вдовенка [13], Ю. Даника [17–19], Т. Ботвина [3], з української сторони, та G. Atul [74], I. Rezawana [87], E. Friginal [80], А. Йохансен [79] поклали початок вивченню окремих аспектів цієї термінології. Однак спеціальні дослідження, спрямовані на виявлення структурно-семантичних особливостей англомовних термінів кібербезпеки та розробку оптимальних стратегій їх перекладу українською мовою, залишаються необхідними.

Тому, **актуальність дослідження** зумовлена необхідністю ґрунтовного вивчення англомовної термінології кібербезпеки, що пов'язано з недостатньою науковою розробленістю цієї проблематики та стрімким зростанням корпусу галузевих термінів, з перспективністю досліджень щодо особливостей перекладу англомовних термінів кібербезпеки, зокрема у контексті постійного оновлення термінологічного фонду. Необхідність подальшого лінгвістичного аналізу зумовлюється як практичними потребами професійної комунікації, так і науковим завданням впорядкування національної терміносистеми відповідно до сучасних світових тенденцій. Важливим також є дослідження термінології кібербезпеки як носія наукового знання та визначення її структури, способів утворення, специфічних особливостей, складу та відсутністю українсько-англійських фахових словників.

Зв'язок роботи з науковими темами. Дипломну роботу виконано в межах ініціативної наукової теми кафедри «Іноземна філологія та переклад» Національного університету «Запорізька політехніка» № 06124 «Лінгвосеміотичні параметри міжкультурної комунікації». Тема роботи затверджена наказом ректора № 508 від 13 листопада 2025 р.

Об'єкт дослідження – англомовні терміни кібербезпеки.

Предмет дослідження – структурно-семантичні особливості англомовних термінів кібербезпеки та способи їхнього перекладу українською мовою.

Мета роботи – вивчення та опис англомовних термінів кібербезпеки, їх структурних та семантичних особливостей й способів перекладу українською мовою.

Для досягнення поставленої мети у роботі вирішуються такі завдання:

- уточнити зміст базових понять «термін», «термінологія», «терміносистема» та охарактеризувати їх структуру й семантичні ознаки;
- простежити основні етапи становлення та розвитку англомовної термінології кібербезпеки в історичному та технологічному аспектах та здійснити системний опис термінологічного складу лексики кібербезпеки, виокремивши її структурні компоненти та функціональні особливості;
- окреслити критерії визначення англомовної термінології кібербезпеки та зробити структурно-семантичний аналіз зазначених термінів;
- дослідити прийоми перекладу термінів кібербезпеки та надати рекомендації щодо їх перекладу.

Матеріалом роботи слугували лексикографічні джерела сучасної англійської мови – як загальні (A. Gadsby [101], Cambridge Dictionary [100], Glossary of Cyber Security Terms [102] тощо), та і спеціальні словники з кібербезпеки (*Англо-український словник термінів з інформаційних технологій та кібербезпеки під ред. А. Гладун* [95]). Крім того, в роботі було використано окремі сайти з мережі Інтернет, присвячених мовним інноваціям, а також такі автентичні періодичні видання, як: *The Hacker News* [114], *Krebs on Security* [106], *BleepingComputer* [110], *CSO Online* [111], *Dark Reading* [112] тощо. Із цих видань було відібрано шляхом цілеспрямованого лінгвістичного пошуку 1333 англомовних термінів кібербезпеки.

У роботі були використані такі **методи дослідження:** *описовий* – для надання загальної характеристики поняттям «термін», «термінологія», «терміносистема» та опису лексичних одиниць англомовної терміносистеми

кібербезпеки; *тезаурусний* – для розкриття змісту нових лексичних одиниць через словникові дефініції; *словотвірний* – для визначення структурних типів, шляхів, способів і механізмів творення англомовних термінів кібербезпеки; *контекстуальний* – для з'ясування семантики термінів кібербезпеки у конкретному мовленнєвому оточенні; *компонентний* – для виявлення складників семної структури термінів кібербезпеки; *перекладацького аналізу* – спрямовано на виявлення способів перекладу англомовних термінів кібербезпеки у контексті й перекладацьких трансформацій, задіяних у цьому процесі. Допоміжними є методи *етимологічного* та *кількісного аналізу* залученого фактичного матеріалу.

Наукова новизна роботи полягає у тому, що вперше на матеріалі цілісної вибірки англомовних термінів кібербезпеки здійснено комплексний опис їхніх структурно-семантичних характеристик та запропоновано системні підходи до їхнього перекладу українською мовою з урахуванням сучасних тенденцій розвитку інформаційних технологій і норм українського термінотворення.

Теоретичне значення роботи полягає в уточненні лінгвістичних принципів формування та еволюції термінології кібербезпеки як динамічного фрагмента сучасної англомовної техносфери. Проаналізовані моделі термінотворення, семантичні процеси та структурні параметри галузевої лексики поглиблюють розуміння механізмів розвитку спеціальних мов у цифрову епоху. Отримані результати сприяють удосконаленню теоретичної бази термінознавства та перекладознавства, зокрема у сфері нормування й уніфікації новітніх інформаційно-технологічних назв.

Практичне значення одержаних результатів полягає в тому, що вони можуть бути використані для вдосконалення мовної підготовки фахівців у галузі інформаційної безпеки та суміжних ІТ-напрямів. Систематизовані моделі термінотворення й перекладу англомовних термінів кібербезпеки становлять основу для створення навчально-методичних матеріалів, спеціалізованих модулів з професійної англійської мови та тренінгових

програм для перекладачів технічного профілю. Результати дослідження можуть бути застосовані у розробленні рекомендацій з нормування та уніфікації українських еквівалентів кібербезпекової термінології, а також у практиці фахового перекладу в державних структурах, бізнес-секторі та освітньо-наукових установах. Отримані напрацювання здатні сприяти формуванню сучасних глосаріїв, галузевих словників і довідкових ресурсів, що підвищує точність і стандартизованість професійної комунікації в сфері кібербезпеки.

Апробація робота. Результати й висновки роботи були заслухані на засіданні кафедри іноземної філології та перекладу (листопад 2025 р.) та оприлюднені у доповідях на двох наукових конференціях: а) науково-практична конференція «Тиждень науки-2025»; б) І Міжнародна науково-практична конференція «Актуальні проблеми дискурсології, перекладознавства та методики викладання» (Запоріжжя: НУ ЗП, 2025). Доповіді оприлюднено у двох наукових публікаціях [28; 27] – див Додаток В.

Структуру роботи зумовлено науковою логікою дослідження, його метою та поставленими завданнями. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел (114 найменувань). Загальний обсяг роботи 232 сторінки.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИВЧЕННЯ АНГЛОМОВНОЇ ТЕРМІНОСИСТЕМИ КІБЕРБЕЗПЕКИ

1.1. Загальна характеристика терміна та суміжних понять

Наукове осмислення мовних явищ у будь-якій сфері передбачає насамперед створення теоретико-методологічної бази та чітке визначення основних категорій, що становлять основу для їх аналізу. Це особливо актуально у вивченні спеціальної лексики, зокрема англомовної терміносистеми кібербезпеки, яка розвивається надзвичайно динамічно та безпосередньо реагує на технологічні інновації. Її дослідження потребує не лише опису мовного матеріалу, а й ґрунтовного теоретичного розуміння таких понять, як *термін*, *термінологія*, *терміносистема*.

З огляду на це, дослідження природи термінології зберігає свою актуальність і в сучасний період. Однією з ключових задач є визначення термінів, що знайшло відображення в наукових працях таких учених, як А. Романенко [58], Р. Гільченко [15], Г. Єнчева [22], Т. Дячук [21], G. Atul [74], I. L. Rezawana [87], C. Tonoy [91], E. Friginal [80], S. Stubelius [90] та ін.

Історично поняття «термін» зафіксоване в Німеччині з 1876 року, проте його походження залишається предметом наукових дискусій. У лінгвістиці існують різні підходи до розмежування загальновживаної технічної лексики та термінів. Загальновживана лексика функціонує в повсякденному мовленні, тоді як професійна термінологія (професіоналізми) використовується фахівцями певної галузі і може бути незрозумілою поза її межами. Професіоналізми часто розглядаються як неформальні аналоги термінів.

Хоч поняття «термін» і є центральним для термінознавства, у науковому середовищі досі не існує єдиного його тлумачення. У загальному розумінні термін розглядається як слово або словосполучення, що точно позначає певне поняття в науці, техніці чи іншій сфері знань. І. Ментинська

згадує, що термін – це мовний знак, який реалізує своє значення лише в межах відповідної терміносистеми, тобто існує не ізольовано, а в системі логічно пов’язаних понять [45, с. 38]. За Г. Сергєєвой, термін розглядається як словесне позначення наукового поняття, що має закріплену дефініцію та функціонує у спеціальній сфері вжитку [61, с. 45]. А. Крижанівська підкреслює, що термін – це одиниця мови, яка виражає ідеї з різних сфер, таких як наука, техніка та інші [42, с. 21]. Термін є важливою частиною лексичної системи природної мови і допомагає виконувати свою пізнавально-інформативну функцію, пов’язану з фіксуванням і збереженням накопиченого людством знання.

У зарубіжному термінознавстві подібну позицію займають класики школи Е. Вюстера, які у праці *Einführung in die allgemeine Terminologielehre und terminologische Lexikographie* [93] визначають термін як «мовну одиницю, що точно відображає наукове поняття та має визначене місце в системі понять галузі» [93, с. 85]. С. Кабре у межах комунікативного підходу підкреслює функціональний аспект терміна, вважаючи, що термін – це не лише мовна форма, а насамперед елемент комунікативної системи, який забезпечує точність, однозначність і стандартизацію у спеціальному спілкуванні [77, с. 165]. І. Квітко формулює подібну думку, зазначаючи, що «термін – це лінгвістична одиниця, яка позначає концепт у межах певної галузі знань і гарантує точність комунікації» [33, с. 21].

У сучасному українському термінознавстві також існують різні підходи до визначення поняття «термін». Л. Білозерська розглядає термін як мовну одиницю, яка виражає спеціалізовані поняття та застосовується в процесі пізнання наукових і технічних об'єктів [7, с. 23]. Є. Скороходько визначає термін як слово або словосполучення, що точно та однозначно визначає спеціальне поняття будь-якої галузі знань [64, с. 12].

А. Д’яков акцентує увагу на тому, що термін є спеціальним словом, основним призначенням якого є розмежування понять [20, с. 61].

Український мовознавець Є. Кротевич наголошує на чітко окреслених семантичних межах терміна, який виражає спеціальні поняття [43, с. 4].

Сучасні дослідники пропонують динамічний підхід до вивчення термінів. О. Селіванова розглядає термін як функціональне явище, що матеріалізується в дискурсі [60, с. 666], тоді як В. Карабан вивчає терміни як лінгвістичні символи, що репрезентують поняття в спеціальних галузях знань [32, с. 315].

Особливий інтерес представляє підхід І. Квітко, який розглядає термін не як особливе слово, а як слово з особливою функцією – функцією назви науково-технічних понять [33, с. 19]. Ця концепція суттєво відрізняється від поглядів Т. Саворі, який наголошує на спеціалізованому характері термінів та їх зв'язку з професійними поняттями [88, с. 34].

Різноманітність підходів до визначення терміна свідчить про складність цього явища та необхідність подальших досліджень у галузі термінознавства.

Узагальнюючи підходи, можна сказати, що термін – це мовний знак, який через взаємозв’язок із поняттям і предметом певної професійної галузі є невід’ємною частиною відповідної терміносистеми. Саме цей взаємозв’язок визначає його лінгвістичну природу та функціональне призначення.

За структурно-семантичним підходом, термін є особливим словом або словосполученням, що відрізняється від загальновживаної лексики специфікою значення та граматичної будови. Прихильник функціонального підходу О. Васковець [11, с. 86], наголошуює, що термін не становить окремого типу мовної одиниці, а лише виконує специфічну функцію – позначення наукового поняття. Дослідження С. Шелова можливо тлумачить, що відмінність терміна полягає не у формі, а в характері його зв’язку з поняттям і дефініцією [71, с. 36].

Важливою є думка О. Янковеця, який підкреслює, що термінологічна одиниця повинна бути не лише точною і стандартизованою, а й семантично прозорою, тобто такою, що дозволяє вивести значення з її структурних

компонентів [72, с. 26]. Це особливо актуально для термінів англомовної кібербезпеки (*firewall, spyware, keylogger*), де мотивація значення часто є очевидною.

Є. Єнікеєва звертає увагу на те, що термін одночасно позначає і поняття, і предмет, оскільки зв’язок між словом і об’єктом відбувається через поняття. Вона спирається на семантичний трикутник, згідно з яким мовний знак пов’язаний з предметом лише опосередковано – через поняття, що узагальнює його ознаки [23, с. 84]. Таким чином, термін не може функціонувати без понятійного посередника.

Терміни відрізняються низкою характеристик, серед яких – точність визначення, однозначність, інформативна щільність, експресивна нейтральність та стандартизація, що закріплюється у спеціальних словниках, довідниках і державних стандартах. О. Пономарев визначає термін як історично сформовану одиницю термінологічної системи, що виражає спеціальне поняття, функціонує в професійному спілкуванні, належить до словникового складу мови і підпорядковується її структурним законам [55, с. 127].

Сучасна наука про термінологію демонструє різноманітні підходи до визначення поняття «термін», його природи та характерних ознак, що продовжує викликати наукові дискусії. Дослідники продовжують сперечатися про лінгвістичний статус терміна, критерії його відокремлення від нетермінологічної лексики та специфічні характеристики. Класичне термінознавство характеризується множинністю дефініцій термінологічних одиниць, запропонованих різними вченими.

У сучасних термінологічних дослідженнях спостерігається зрушення акценту на вимоги до термінів, що включають семантичні, формальні та практичні аспекти. Семантичні вимоги охоплюють: точність відповідності між терміном і його дефініцією; системність зв'язків у межах термінологічної системи; чіткість значення; повноту відображення суттєвих ознак поняття;

однозначність у межах галузі; відсутність синонімії; контекстуальну незалежність; емоційну нейтральність.

Формальні вимоги включають відповідність мовним нормам, словотворчі можливості та стабільність форми. Прагматичні аспекти передбачають інтернаціоналізацію, поширеність вживання та евфемістичність.

Важливим є положення про те, що термін не є ізольованою мовною одиницею, а володіє специфічними ознаками, що дозволяють його ідентифікацію. Л. Халіновська зазначає, що традиційні критерії терміна (однозначність, точність, нейтральність) часто виявляються недостатньо чіткими для класифікації [68, с. 92]. Науковці виділяють термінологічність значення як ключову характеристику, що визначає здатність терміна описувати спеціальні поняття в системі фахових знань.

Для термінологічної системи кібернетики особливої актуальності набуває визначення І. Квітко, який розглядає термін як лексичну одиницю, пов'язану з поняттями галузі знань, що формує системні зв'язки, характеризується високою інформативністю, однозначністю, точністю та експресивною нейтральністю в конкретний часовий період [33, с. 32]. Це визначення є особливо корисним для аналізу динамічно розвиваючої термінології кібернетики, що постійно оновлюється через швидкий технологічний прогрес. Наприклад, термін *phishing* означає конкретний вид кібератаки, має чітку дефініцію, системно пов’язаний із поняттями *social engineering* і *scam*, а також позбавлений експресивності. Інші приклади – *firewall, ransomware, encryption* – демонструють системність та логічну впорядкованість терміносистеми, що відображає структуру самої галузі.

Ця сукупність термінів, що формує цілісну систему, і становить суть більш широкого поняття – термінології, яка є одним із ключових понять термінознавства. У науковій літературі її визначають як сукупність термінів певної галузі знань, які використовуються для позначення понять і забезпечення точності професійного спілкування. В. Перебийніс трактує

термінологію як «лексичну підсистему мови, що забезпечує номінацію спеціальних понять» [54, с. 3]. У цьому розумінні термінологія становить своєрідну підсистему лексикону, функціонально зорієнтовану на передачу наукової інформації.

С. Кабре пропонує комунікативне визначення термінології, підкреслюючи, що вона є не лише списком термінів, а системою, у межах якої здійснюється обмін знаннями між фахівцями [77, с. 172]. Таким чином, термінологія поєднує мовну, когнітивну та прагматичну компоненти.

У сфері кібербезпеки термінологія охоплює лексичні одиниці, що позначають поняття, пов’язані із захистом інформації, мережевими протоколами, кібератаками, методами шифрування, ідентифікації тощо (*encryption, authentication, breach detection, intrusion prevention*). Вона характеризується високою динамічністю, адже розвиток технологій постійно породжує нові терміни (*blockchain, zero-day exploit, quantum cryptography*).

У сучасній науці існують різні підходи до розуміння термінології. Деякі вчені розглядають термінологію як синонім термінологічної системи, наголошуючи на їхній спільній основі – лексичних одиницях, що функціонують у спеціальних сферах та підпорядковуються нормам мови. Вважається, що терміни кібербезпеки, описуючи строго системний світ інформаційних технологій, закономірно мають системний характер. Однак поширеною є думка, що один термін може входити до складу різних термінологічних систем, особливо в суміжних дисциплінах, таких як кібербезпека, криптографія та комп’ютерні мережі. Це підкреслює необхідність розмежування понять: термінологія розглядається як структурована підсистема загальної лексики, тоді як термінологічна система є більш впорядкованим утворенням.

Інший погляд полягає в тому, що термінологічна система – це високоорганізована сукупність термінів із чітко визначеними зв’язками, що являє собою вищий рівень організації, ніж термінологія [58, с. 45; 64, с. 18]. Прихильники цієї позиції часто розглядають термінологію як динамічну,

дещо хаотичну сукупність слів, що історично сформувалася в галузі кібербезпеки та постійно збагачується, у тому числі за рахунок запозичень із загальновживаної лексики (наприклад, «*cloud*», «*blockchain*», «*protection*») [42, с. 45; 60, с. 203].

Ще одна концепція виокремлює глосарій як практичний набір найменувань для професійної комунікації [59; 95]. У цьому контексті сучасну термінологію кібербезпеки розуміють як відносно сталу, але постійно вдосконалювану систему, тоді як термінологічна система – це вже впорядкована та стандартизована сукупність термінів [34, с. 15; 72, с. 112]. Важливо, що будь-яка термінологічна система кібербезпеки містить як ядро (наприклад, «*encryption*», «*firewall*»), так і периферійні терміни, запозичені з інших галузей (наприклад, «*legal protection*»), що може породжувати багатозначність.

Таким чином, логічно виходити з того, що **термінологія** – це динамічне поняття, сукупність лексичних одиниць галузі, яка розвивається під впливом зовнішніх чинників: нових загроз, технологічних проривів та законодавчих змін. На противагу цьому, **термінологічна система** – це штучно впорядкований набір специфічних термінів, створений фахівцями. Завданням сучасного лінгвіста чи термінолога в галузі кібербезпеки є аналіз стихійної термінології для формування чітких термінологічних систем. Термінологія є ширшим поняттям, що охоплює всі лексичні одиниці галузі, включаючи професійний жаргон, тоді як термінологічні системи – це строгі, окремі конструкції, побудовані для конкретних підгалузей (наприклад, для стандартів шифрування). Це пояснює, чому термін (наприклад, «*key*») може бути багатозначним у загальній термінології, але набуває чіткого однозначного значення в конкретній термінологічній системі.

Отже, термінологічна система в кібербезпеці – це сукупність усіх термінів певної концептуальної галузі (наприклад, *data storage / data repository* – «сховище даних»), між якими існують логічні зв’язки. Вона служить інструментом для уніфікації, стандартизації та систематизації

термінів, забезпечуючи точність і однозначність у професійній комунікації, що є критично важливим для ефективного протидії кіберзагрозам.

Терміносистема кібербезпеки включає базові терміни (*encryption, authentication*), похідні (*end-to-end encryption, two-factor authentication*), а також численні акроніми (*VPN, DDoS, IDS*). Вона перебуває у стані постійного оновлення: нові технології породжують нові поняття, а отже – і нові терміни. Її структура відкрита, гнучка, із виразною ієрархічною організацією, що забезпечує цілісність і логічну впорядкованість.

У терміносистему кібербезпеки, окрім власне термінів, входять також суміжні мовні явища, які тісно з нею взаємодіють, проте мають специфічні характеристики. Передусім це стосується професійного жаргону (сленгу), який охоплює неформальні, часто образні назви на кшталт *backdoor, bug* чи *zero-day*. Ці одиниці функціонують переважно у вузькому середовищі фахівців і відзначаються емоційно-експресивним забарвленням, що відрізняє їх від нейтральних термінів. Водночас професійний жаргон характеризується певною динамічністю: окремі жаргонізми можуть з часом інтегруватися в офіційну термінологію, втрачаючи свою первісну неформальність та набуваючи статусу загальновизнаних термінів.

Поряд із жаргонною лексикою важливу роль у терміносистемі відіграють абревіатури та акроніми, такі як *VPN, APT, SQL, HTTPS*. Ці мовні одиниці є особливим різновидом термінів і виконують насамперед функцію економії мовних засобів у професійній комунікації. На відміну від жаргонізмів, абревіатури та акроніми належать до офіційного термінологічного апарату й характеризуються стандартизованістю та чіткою семантикою. Крім того, до складу терміносистеми входить номенклатура – перелік назв конкретних об'єктів або продуктів, наприклад *Wireshark, Cisco ASA*, які не утворюють системи понять, а слугують для позначення окремих технічних рішень чи програмних продуктів. Отже, терміносистема кібербезпеки постає як складне утворення, що об'єднує різнорідні, але взаємопов'язані елементи професійної мови.

Підсумовуючи, розгляд понять «термін», «термінологія» та «терміносистема» демонструє істотну розбіжність у наукових підходах. Ідеалізована модель, що вимагає від терміна абсолютної точності, стабільності та позаконтекстності, протиставляється сучасному розумінню терміна як динамічної, гнучкої та адаптивної одиниці. Ця динаміка обумовлена потребою термінології постійно відповідати викликам швидкозмінних галузей знань, де критично важливими стають не лише внутрішня системність, але й здатність до інтеграції та розвитку.

1.2. Англомовні терміни кібербезпеки

Історія розвитку цифрових технологій наочно демонструє, що поява комп'ютерних мереж сприяла зародженню мережевої безпеки, а стрімке зростання Інтернету та його технологій стало стартовим майданчиком для формування комплексної кібербезпеки [10, с. 91; 13, с. 19]. Цей історичний контекст безпосередньо вплинув і на термінологічний апарат галузі. Оскільки кібербезпека виросла з фундаментів комп'ютерної та мережевої безпеки, її понятійна основа успадкувала та трансформувала відповідні терміни [70, с. 181]. Процес цієї термінологічної еволюції найкраще простежити на прикладі ключового поняття, яке консолідувало галузь – власне, терміна «кібербезпека».

Як свідчить етимологічний аналіз, термін «кібербезпека» походить від англійського *cybersecurity*, утвореного шляхом поєднання префікса *cyber-*(від *cybernetics – кібернетика*) та слова *security (безпека*) [28, с. 94]. Префікс *cyber-*, що почав активно вживатися в другій половині XX століття, став маркером простору, пов'язаного з комп'ютерними технологіями, телекомунікаціями та мережевими системами [60, с. 301]. Семантика самого поняття зазнала значної трансформації: спочатку *cybersecurity* охоплювало переважно технічні аспекти захисту інформації, однак із часом його зміст

розширився, почавши включати правові, організаційні, соціальні та навіть етичні складники [18, с. 113; 89, с. 89].

Ця динаміка знайшла своє відображення і в українському науковому та правовому полі. У вітчизняний дискурс термін «*кібербезпека*» повноцінно увійшов наприкінці 1990-х – на початку 2000-х років, що було обумовлено інтенсивним розвитком інформаційного суспільства та необхідністю адаптації міжнародних стандартів [11, с. 245; 44, с. 112]. Саме на цьому етапі відбулося активне формування лексикона кібербезпеки, яке характеризувалось двома ключовими процесами: з одного боку, масовим запозиченням англомовних термінів (наприклад, *firewall, malware, phishing, hacking*), а з іншого – їх поступовою інтеграцією та адаптацією до української мовної системи, що й поклало початок становленню власне української термінологічної системи в цій галузі [29, с. 156; 38, с. 50].

Сучасний етап розвитку кібербезпеки супроводжується активним впорядкуванням її термінології на глобальному рівні. Цей процес знаходить відображення у міжнародних стандартах, таких як серія ISO/IEC 27000, та рамкових документах на кшталт NIST Cybersecurity Framework. Подібна стандартизація сприяє чіткому визначенню понять та розмежуванню термінів [63, с. 31].

Лінгвістичний аналіз підкреслює роль англійської мови як основи для міжнародної професійної комунікації в галузі кібербезпеки. Сучасне розуміння кібербезпеки акцентує увагу на забезпеченні конфіденційності (*confidentiality*), цілісності (*integrity*) та доступності (*availability*) інформації. Ці три принципи утворюють фундаментальну концепцію, відому як «*тріада CIA*». Таке трактування перетворює кібербезпеку з технічного поняття на комплексну багатовимірну систему.

Англомовна термінологія кібербезпеки має низку характерних рис. По-перше, вона демонструє інтегративність, запозичуючи поняття з інших галузей. Наприклад, з бізнесу прийшли терміни «*personal data breach*»,

«*business continuity*», «*identity theft*», з правового поля – «*compliance*» і «*liability*».

По-друге, термінології властива інтернаціональність. Багато слів зберігають однакове написання та значення в різних мовах. До таких слів належать *cache, domain, host, spam, phishing, blockchain , bitcoin.*

По-третє, спостерігається тенденція до економії мовних засобів. Фахівці активно використовують акроніми та скорочення. Серед найпоширеніших – *DDoS (Distributed Denial-of-Service), VPN (Virtual Private Network), IDS/IPS (Intrusion Detection/Prevention System), MITM (Man-in-the-Middle), URL (Uniform Resource Locator) або POP3 (Post Office Protocol, Version 3).*

Окремої уваги заслуговує метафоричність термінології. Для опису складних концепцій використовуються різноманітні образи. Військова метафорика представлена термінами «*firewall» і «zero-day attack»*. Кримінальна лексика присутня у словах «*hacker*» і «*trojan horse*». Побутові метафори реалізуються через такі поняття як «*cloud*» і «*worm*».

Системність терміна проявляється у його функціонуванні в межах певної терміносистеми, де він набуває специфічного значення залежно від галузі застосування. Так, термін *Trojan Horse* у кібербезпеці позначає тип шкідливого програмного забезпечення, яке маскується під легітимну програму, тоді як у літературі чи історії той самий вираз асоціюється з троянською війною та хитрістю Одіссея. Це свідчить про те, що термін функціонує не ізольовано, а в системі понять конкретної предметної галузі, де він співвідноситься з іншими термінами та займає чітко визначене місце в ієрархії спеціальних понять [78].

Дефінітивність забезпечує чітке та однозначне визначення термінів, що є критично важливим для точної професійної комунікації. Наприклад, термін *Applet* має конкретну дефініцію: це програма на мові Java, яка використовує веб-браузер клієнта для створення інтерфейсу користувача. Таке визначення

не допускає вільного тлумачення чи розмитості значення, що відрізняє термін від загальновживаних слів.

Контекстуальна незалежність означає, що термін зберігає своє значення незалежно від контексту вживання. Так, термін *network mapping* завжди позначає *процес мережного картографування – виявлення та документування топології комп'ютерної мережі, її вузлів та зв'язків між ними.* На відміну від багатозначних загальновживаних слів, які можуть змінювати значення залежно від контексту, термін залишається семантично стабільним у різних професійних текстах.

Точність проявляється у прагненні до максимально коректного відображення поняття, попри існування певних неточностей у професійних субмовах. Наприклад, англійський термін *hub* у фаховій українській мові перекладається як «*концентратор*», що точно відображає функцію пристрою, а не калькується як «*хаб*», хоча таке запозичення є поширеним у неформальному спілкуванні. Подібно до цього, термін *router* перекладається як «*маршрутизатор*», а не «*роутер*», що забезпечує термінологічну точність.

Стислість передбачає лаконічність термінів, що сприяє ефективності професійної комунікації. Прикладами стислих термінів є *bit* (*одиниця інформації)*, *browser* (*програма для перегляду веб-сторінок*), *cookie* (*файл даних на комп'ютері користувача*), *filter* (*засіб фільтрації трафіку*). Водночас ця вимога інколи може суперечити вимозі точності, що призводить до появи багатокомпонентних термінів, як – от *Internet Control Message Protocol* (*протокол міжмережних керувальних повідомлень) або Open Shortest Path First (протокол маршрутизації з вибором найкоротшого шляху*) [78].

Моносемантичність означає, що термін у межах однієї терміносистеми має лише одне значення. Наприклад, термін *spam* у галузі кібербезпеки однозначно пов'язаний із поняттям масової розсилки небажаних електронних повідомлень чи публікацій у групах новин, і це значення не варіюється в різних фахових контекстах. Подібно, термін *firewall* завжди позначає

систему захисту мережі від несанкціонованого доступу, не допускаючи інших тлумачень.

Обмежена синонімія є характерною особливістю термінології кібербезпеки, оскільки існування кількох термінів для одного поняття може призводити до плутанини. Проте у деяких випадках синоніми все ж зустрічаються: наприклад, *cracker* та *intruder* можуть позначати зловмисника, який несанкціоновано проникає в комп'ютерні системи. Втім, фахівці прагнуть мінімізувати таку синонімію, надаючи перевагу одному усталеному терміну.

Експресивна нейтральність передбачає, що терміни мають бути вільними від емоційного забарвлення та оцінного компонента. Так, термін *vulnerability* (*вразливість*) є нейтральним позначенням слабкого місця в системі безпеки, без емоційних конотацій, які могли б бути притаманні розмовній лексиці. Це забезпечує об'єктивність та професійність фахового дискурсу.

Нарешті, евфонічність означає, що терміни повинні звучати милозвучно та відповідати фонетичним нормам мови. Терміни мають уникати діалектизмів, надмірних жаргонізмів чи варваризмів, які порушують естетику професійної мови. Англомовні терміни часто відрізняються милозвучністю та фонетичною зручністю, що сприяє їх легкому засвоєнню та активному використанню в міжнародній професійній комунікації. Наприклад, лаконічні та ритмічні терміни, такі як *patch*, *spam* чи *blockchain*, органічно вписуються в мовну систему.

Водночас, довгі або фонетично важкі акроніми часто переходять у скорочену вимову, що робить їх більш еуфонічними. Спрощення вимови *SQLi* (/ˈsiːkwəl aɪ/) замість повного *Structured Query Language Injection* або *DDoS* (/diː.dɒs/) замість *Distributed Denial-of-Service* є яскравими прикладами такої природної оптимізації [78]. Так, і україномовні терміни «*маршрутизатор*», «*брандмауер*», «*шифрування*» є евфонічними та природно вписуються у фонетичну систему української мови, на відміну від

незграбних запозичень. Таким чином, евфонічність в англомовній термінології не лише підвищує естетику мови, але й слугує практичній меті – забезпечує ефективність та швидкість професійного спілкування.

Як наслідок цього процесу, сформувалася динамічна термінологічна система, здатна до швидкої адаптації. Вона успішно поєднує інтернаціональні характеристики з функціональністю, що забезпечує ефективну комунікацію в умовах прискореного технологічного прогресу. Ця адаптивність дозволяє системі адекватно реагирувати на нові виклики та задовольняти потреби глобальної спільноти фахівців з кібербезпеки.

Структурно терміносистема включає кілька взаємопов'язаних пластів лексики, що охоплюють технічні аспекти захисту, правове регулювання та організаційні процедури. Така багатоаспектність є закономірним наслідком комплексного характеру самої галузі кібербезпеки, що поєднує технологічні рішення з правовими нормами і управлінськими підходами. Терміносистема кібербезпеки в англійській мові сформувалася на базі лексики, пов'язаної з інформатикою, програмуванням, мережевими технологіями та правом. Її розвиток зумовлений потребою чіткого позначення процесів, об'єктів і явищ у сфері захисту інформації, що особливо актуалізувалося з появою глобальних комп'ютерних мереж та зростанням кількості кіберзагроз.

Фундаментом терміносистеми є загальні поняття, які окреслюють основні напрями діяльності у цій галузі. До них належать *cybersecurity* (кібербезпека) як узагальнювальне поняття для всієї сфери, *information security* або скорочено *infosec* (інформаційна безпека), що охоплює ширший спектр заходів із захисту інформації в різних формах, а також *data protection* (захист даних), яке акцентує на збереженні конфіденційності та цілісності даних [113]. Поряд із ними функціонують терміни *network security* (мережна безпека), що стосується захисту комп'ютерних мереж від зловмисних втручань, та *digital safety* (цифрова безпека), який підкреслює безпечне використання цифрових технологій користувачами [81, с. 45].

Значний сегмент терміносистеми становлять одиниці, що позначають види кіберзагроз, оскільки ідентифікація та класифікація загроз є першим кроком до їх нейтралізації. Узагальнювальним терміном тут виступає *malware* (шкідливе програмне забезпечення), до підвидів якого належать *virus* (комп'ютерний вірус) – програма, що самовідтворюється та інфікує файли, *worm* (мережний черв'як) – шкідлива програма, яка поширюється мережею без втручання користувача, та *Trojan horse* або скорочено *Trojan* («троянський кінь») – програма, що маскується під легітимне програмне забезпечення [112]. Окрему групу утворюють терміни, пов'язані із соціальною інженерією та обманом: *phishing* (фішинг) означає шахрайство з метою отримання конфіденційних даних через підроблені повідомлення, тоді як *spoofing* (підміна даних) позначає фальсифікацію ідентифікаційної інформації. До цієї ж категорії належать терміни *hacking* (злам, несанкціонований доступ), що описує процес отримання неавторизованого доступу до системи, а також *cyberattack* (кібератака) та *cybercrime* (кіберзлочин), які позначають відповідно атаку на інформаційні системи та злочинну діяльність у кіберпросторі [69, с. 73].

Не менш важливою є група термінів, пов'язаних із засобами та методами захисту інформації. Серед них виділяється *firewall* (*міжмережевий екран або брандмауер) – система контролю мережного трафіку, encryption (шифрування) – процес перетворення інформації у нечитабельний формат для захисту від несанкціонованого доступу* та *authentication (автентифікація) – процес перевірки ідентичності користувача чи системи.* Важливу роль відіграють також *backup* (*резервне копіювання*), що забезпечує збереження даних у разі їх втрати, *antivirus software* (*антивірусне програмне забезпечення*), призначене для виявлення та знешкодження шкідливих програм, *intrusion detection system* або *IDS* (*система виявлення вторгнень*), яка моніторить мережу на предмет підозрілої активності, а також *security patch* (*оновлення безпеки*) – програмний код для усунення вразливостей у системі.

Окремий пласт термінології складають одиниці, що позначають суб'єктів діяльності у сфері кібербезпеки та їхні ролі. Центральним тут є термін *hacker* (хакер), який у різних контекстах може мати як нейтральне, так і негативне значення. Для уточнення намірів хакера використовуються терміни *ethical hacker* або *white hat* (етичний хакер, «білий капелюх») на позначення фахівця, який тестує системи безпеки легально, та *black hat* (*зловмисник, «чорний капелюх»*), що означає хакера з криміналними намірами. До професійних ролей належать також *cybersecurity analyst* або *cybersecurity specialist* (аналітик або фахівець із кібербезпеки), *system administrator* або скорочено *sysadmin* (системний адміністратор), який відповідає за підтримку та безпеку IT-інфраструктури, а також *end user* (*кінцевий користувач*) – особа, яка безпосередньо використовує інформаційні системи.

Нарешті, терміносистема включає одиниці, що описують процеси та політики забезпечення безпеки в організаціях. До них належать *risk assessment* (*оцінювання ризиків*) – систематичний аналіз потенційних загроз та їхнього впливу, *incident response* (*реагування на інциденти*) – комплекс заходів для виявлення, аналізу та усунення наслідків порушень безпеки, *access control* (*контроль доступу*) – система обмеження доступу до ресурсів залежно від прав користувача, *security policy* (*політика безпеки*) – документ, що визначає правила та процедури захисту інформації в організації, та *vulnerability management* (*управління вразливостями*) – процес виявлення, оцінювання та усунення слабких місць у системах безпеки.

Аналіз наведених термінів свідчить, що лексика кібербезпеки англійської мови характеризується кількома особливостями. По-перше, вона має переважно англо-латинське походження, що типово для наукової та технічної термінології. По-друге, ця терміносистема активно поповнюється неологізмами, які виникають у відповідь на появу нових технологій та загроз. По-третє, значна частина термінів функціонує у формі скорочень та абревіатур, що забезпечує економію мовних засобів. По-четверте, більшість

одиниць є інтернаціоналізмами, що функціонують у фаховому мовленні різних мов світу, хоча й можуть зазнавати певної адаптації при запозиченні. Така міжнародна уніфікація термінології сприяє ефективній професійній комунікації фахівців із різних країн та забезпечує швидке поширення нових знань у глобальному масштабі.

1.3. Історія розвитку англомовної термінології кібербезпеки

Формування англомовної термінології кібербезпеки стало природним наслідком технологічної революції другої половини XX століття. Подібно до того, як мрія про політ знайшла своє втілення в авіаційній термінології, прагнення до створення безпечного цифрового простору породило цілу систему спеціальних понять. Ця система, однак, формувалася не миттєво, а пройшла чітко визначені фази становлення [18, с. 113]. На основі проведеного аналізу можна виділити чотири основні етапи розвитку цієї терміносистеми, кожен з яких характеризується специфічними особливостями формування термінологічного апарату.

Перші передумови виникли ще в 1960-1970-х роках разом із появою багатокористувацьких комп'ютерних систем, коли з'явилися такі фундаментальні поняття як *access control* (*контроль доступу*) та *password protection* (*захист паролем*). Проте справжній поштовх до розвитку термінології відбувся з розповсюдженням мережевих технологій та Інтернету, коли традиційні поняття безпеки набули нового виміру [82, с. 107].

Знаковим моментом стало активне запозичення лексики з суміжних галузей: з мовознавства прийшов термін *phishing* (*фішинг*), з транспортної лексики – *traffic* (*трафік*), з військової термінології – *firewall* (*брандмауер*).

На початковому етапі термінологія кібербезпеки ще не існувала як окрема система. Цей період характеризувався активним розвитком

кібернетики, інформатики та теорії управління, які стали підґрунтям для формування майбутньої термінології цифрової безпеки. До найуживаніших термінів належали *cybernetics* (*кібернетика*), *computer* (*комп'ютер*), *data processing* (*обробка даних*), *information system* (*інформаційна система*). У цей же час з'являється слово *hacker*, яке спочатку мало позитивне значення – «*ентузіаст програмування*». Лексика цього періоду мала переважно технічний характер, без безпосереднього зв'язку з поняттям захисту інформації. Термінологія була локальною та обмеженою, оскільки комп'ютерні мережі тільки починали розвиватися в університетських і дослідницьких середовищах США та Великої Британії, а кількість користувачів комп'ютерних систем була незначною. Перший комп'ютерний вірус *Creeper*, створений у 1971 році для мережі ARPANET, поклав початок усвідомленню потреби в захисті цифрових систем, що призвело до розробки першого антивірусу *Reaper* [82, с. 108].

Другий етап (1980–1990 рр.) став періодом становлення базової термінології кібербезпеки.Це було обумовлено тим, що з появою персональних комп'ютерів, локальних мереж і збільшенням кількості зламів виникла нагальна потреба у створенні спеціальної термінології для опису нових загроз і способів захисту [89, с. 88]. Саме тоді до активного вжитку входять ключові терміни, що сформували фундамент терміносистеми: *computer virus* (*комп'ютерний вірус*), *worm* (*мережевий черв'як*), *Trojan horse* (*троянський кінь*), *firewall* (*міжмережевий екран*), *data encryption* (*шифрування даних*), *antivirus software* (*антивірусне програмне забезпечення*), *password* (*пароль*). У цей період формувалися базові категорії кібербезпеки, що пізніше стали міжнародними термінами. Поширенню англомовної термінології сприяв факт того, що більшість програмного забезпечення і комп'ютерних стандартів розроблялися в англомовних країнах, зокрема в США, що зумовило глобальне використання цих термінів. Проблема кібербезпеки набула особливої актуальності після нападу на ARPANET у 1988 році за допомогою вірусу *Morris Worm*, що вважається однією з перших

великих кібератак у світі. Паралельно розроблялися перші віруси для операційної системи Microsoft DOS, а також почало набувати популярності шифрування даних із вимогою викупу, тобто *ransomware* (*програма-вимагач*) [89, с. 89].

Отже, лінгвістичні особливості термінології цього періоду виявляються у кількох ключових аспектах:

По-перше, спостерігається активне використання метафоризації як основного механізму термінотворення. Такі поняття, як *worm* (*черв'як*) для самореплікуючої програми, що «проповзає» через мережу, чи *firewall* (*вогнестіна*) для захисного бар'єру, що відокремлює мережі, створювали зрозумілі образи для нових технічних явищ. Ця образність значно сприяла швидкій адаптації термінів у професійному середовищі.

По-друге, характерним явищем стало формування складних термінів-словосполучень. Такі конструкції, як *data encryption* (*шифрування даних*) та *password protection* (*захист паролем*), дозволяли точно визначити спеціалізовані поняття шляхом поєднання існуючих лексичних одиниць. Цей механізм забезпечив гнучкість та системність термінології.

По-третє, важливу роль відіграли мовні запозичення. Зокрема, грецька мова надала префікс *crypto-* (від грец. κρυπτός – *прихований*), що став основою для таких термінів, як *cryptography* (*криптографія*), а латинська мова подарувала поняття *virus* (від лат. *virus* – *отрута*), яке набуло нового технологічного значення.

Цей період заклав міцні основи міжнародної термінології кібербезпеки, що було обумовлено технологічним лідерством англомовних країн, особливо США, у розробці програмного забезпечення та встановленні комп'ютерних стандартів [78]. Саме через домінування англійської мови в технологічній сфері створені терміни швидко поширилися й увійшли до глобального вжитку, сформувавши уніфікований понятійний апарат для фахівців з кібербезпеки по всьому світу.

Третій етап (1990 – 2000 рр.) ознаменувався експансією термінології та формуванням системності. Це було обумовлено подальшим розвитком мережевих технологій, появою Інтернету, електронної комерції та соціальних медіа зумовили виникнення нових явищ у цифровому просторі, які потребували номінації. Саме в цей період термін *cybersecurity* набуває широкого вжитку, позначаючи вже не лише технічний, а й організаційний аспект захисту інформації. З'являються похідні одиниці *cyberattack* (*кібератака*), *cybercrime* (*кіберзлочин*), *cyberterrorism* (*кібертероризм*), які розширюють межі терміносистеми. До активного вжитку входять терміни *phishing* (*фішинг*), *spam* (*спам*), *spyware* (*програма-шпигун*), *malware* (*шкідливе програмне забезпечення*), *authentication* (*автентифікація*), *security patch* (*оновлення безпеки*), *backup system* (*система резервного копіювання*). Початок XXI століття став часом інтенсивного збагачення термінології кібербезпеки, у якій префікс *cyber-* почав відігравати роль системоутворювального елемента. Виникла необхідність у стандартизації термінів, пов'язаних із захистом даних і конфіденційністю користувачів. Терміни, які спочатку функціонували в професійних колах, згодом увійшли у широку публічну лексику. У 2000-х роках відбулися численні масштабні кібератаки на вебсайти Yahoo!, Amazon, eBay та інші, а також з'явилися перші масові шкідливі програми *ILOVEYOU* та *Code Red*, що швидко поширювалися через електронну пошту [78]. Цей період характеризується також активним запозиченням термінів із інших мов, особливо латинської та німецької, і адаптацією їх під англомовну фонетику та морфологію.

Лінгвістичні процеси цього періоду відзначалися значним різноманіттям і динамікою. Спостерігалося кілька ключових явищ, що формували термінологічний апарат кібербезпеки.

Яскравим прикладом семантичної трансформації став термін *spam*. Спочатку це слово позначало торгову марку м'ясних консервів, але в 1990-х роках набуло нового значення – *масової небажаної електронної*

кореспонденції. Ця зміна значення відбулася під впливом відомого скетчу Монті Пайтона, де слово «*spam*» повторювалося нав'язливо та безперервно.

Метафоричне запозичення реалізувалося в таких термінах, як *phishing*. Це поняття виникло шляхом творчої адаптації слова «*fishing*» (*риболовля*), де заміна літери «f» на «ph» вказувала на комп'ютерний контекст. Образ рибалки, що виловлює конфіденційну інформацію, точно відображав суть цього виду кіберзлочинності.

Скорочення та акроніми стали надзвичайно продуктивним способом термінотворення. Широке поширення набули такі скорочення, як *VPN (Virtual Private Network), ISP (Internet Service Provider) та SSL (Secure Sockets Layer).* Ці лаконічні форми дозволяли ефективно спілкуватися в професійному середовищі.

Процес складання слів продемонстрував свою ефективність у створенні таких термінів, як *username* (*ім'я користувача*), *password-protected* (*захищений паролем), malware analysis (аналіз шкідливого ПЗ), ransomware attack (атака програмою-вимагачем)* тощо. Цей спосіб дозволяв поєднувати існуючі лексичні одиниці для точного опису нових явищ і понять.

Важливим явищем стала інтенсивна стандартизація термінології, зумовлена потребою в єдиному понятійному апараті для міжнародної співпраці. Терміни, що раніше використовувалися переважно фахівцями, почали активно проникати в загальновживану лексику. Цьому сприяли гучні кібератаки на великі корпорації, а також поширення руйнівних вірусів [73, с. 120].

Мовні запозичення цього періоду відображали глобалізацію кіберпростору. Поряд із традиційними запозиченнями з німецької та латинської мов, спостерігалася адаптація слів з японської та китайської, що свідчило про формування справді міжнародної термінології. З німецької мови прийшли такі важливі поняття: *Blitzkrieg* – для позначення швидких масивних атак; *Gestalt* – поняття з німецької психології, яке адаптували для аналізу кіберзагроз у цілому; *Zeitgeist* – використовується для опису

загальних тенденцій у розвитку кібербезпеки тощо. Латинська мова продовжувала залишатися важливим джерелом термінології: *quid pro quo* (*тип соціально-інженерної атаки*), *modus operandi* (*спосіб дій кіберзлочинців*), *per se* – термін, що увійшов до академічного дискурсу кібербезпеки. З японської мови були запозичені такі терміни: *tsunami* – (*для позначення масових хвиль кібератак*), *kamikaze* (*саморозповсюджувальний вірус*), *zen* – у контексті простих та елегантних рішень безпеки. Китайські запозичення включали: *Yin-yang* – для опису балансу між захистом та доступністю, *Tao* – щодо комплексного підходу до безпеки, *Guanxi* – у контексті мережевих зв'язків у кіберпросторі. Особливо цікавими були транслітеровані терміни: *Jīngshén* – для опису «духу» систем безпеки, *Bǎohù* – щодо захисту критичної інфраструктури [84, с. 67].

Ці запозичення демонструють, як технологічний розвиток поєднувався з культурним обміном, створюючи багату та різноманітну термінологічну систему. Більшість цих термінів зберегли оригінальне написання латиницею, що підкреслювало їхнє міжнародне походження та сприяло глобальній стандартизації.

Цей етап сформував міцну основу сучасної термінології кібербезпеки, встановивши основні принципи її подальшого розвитку. Лінгвістичні процеси 1990-2000-х років продемонстрували здатність англійської мови гнучко адаптуватися до стрімких технологічних змін, створюючи точний і функціональний термінологічний апарат.

Четвертий етап (2010 рр. – сьогодення) характеризується переходом до міждисциплінарності та глобальної стандартизації. Сьогодні кібербезпека розглядається як міждисциплінарна сфера, що об'єднує технологічні, правові, соціальні й етичні аспекти. Відповідно, терміносистема продовжує активно розвиватися, реагуючи на появу нових технологій і типів загроз. Розвиток хмарних технологій, мобільних платформ, Інтернету речей і глобальних мереж забезпечив інтернаціоналізацію термінології кібербезпеки. До сучасних термінів належать *ransomware* (*програма-вимагач*), *zero-day*

vulnerability (*уразливість нульового дня*), *two-factor authentication* або *2FA* (*двофакторна автентифікація*), *cloud security* (*хмарна безпека*), *IoT security (безпека Інтернету речей*), *cyber resilience* (*кіберстійкість*), *threat intelligence* (*розвідка загроз*), *data breach* (*витік даних*), *deepfake detection* (*виявлення дипфейків*), а також технічні поняття *DDoS, VPN, SSL* та терміни, пов'язані з регулюванням і політикою безпеки: *compliance* (*відповідність стандартам*), *cyber governance* (*кіберуправління*). Характерною рисою цього періоду є прагнення до глобальної стандартизації термінів, створення міжнародних глосаріїв і нормативних документів, зокрема ISO/IEC 27000:2022 та NIST Cybersecurity Framework. Поява цих стандартів сприяла формуванню системної термінології з високим ступенем точності та універсальності [109]. Сучасна англомовна терміносистема кібербезпеки характеризується інтегративністю, оскільки охоплює сферу бізнесу, фінансів, освіти та державного управління, а також моносемантичністю і стандартизованістю, що полегшує міжнародну комунікацію. Водночас вона залишається динамічною та відкритою до інтернаціональних впливів, здатною забезпечувати точне й однозначне позначення новітніх явищ у сфері інформаційної безпеки, реагуючи на нові виклики кіберзлочинності, цифрової трансформації та впровадження штучного інтелекту [10, с. 92].

Сьогодні англомовна термінологія кібербезпеки продовжує динамічно розвиватись, інтегруючи поняття зі штучного інтелекту (*machine learning in cybersecurity*), квантових обчислень (*quantum-resistant cryptography*) та соціальних наук (*human factor*), що свідчить про її постійну адаптацію до нових технологічних реалій.

Російсько-українська війна спричинила значні зміни в термінологічному апараті кібербезпеки, породивши низку унікальних неологізмів: *electronic ambush* (*електронна засідка*) – несподівані атаки на ворожі цифрові колони та канали зв'язку, що порушують їхні можливості управління та контролю під час вирішальних операцій; *AI-Propaganda* (*ШІ-пропаганда*) – використання штучного інтелекту для створення та поширення

спеціально підібраного дезінформаційного контенту в соціальних мережах та каналах зв'язку; *quantum jamming* (*квантове глушіння*) – передові методи електронної боротьби, що порушують супутниковий зв'язок і навігаційні системи противника з використанням складного маніпулювання частотами [10, с. 93]; *drone hijacking* (*захоплення дронів*) – перехоплення контролю над безпілотними літальними апаратами шляхом використання вразливостей у їхніх протоколах зв'язку та системах управління; *blockchain intelligence* (*блокчейн-розвідка*) – відстеження та аналіз транзакцій криптовалют для ідентифікації та порушення фінансування ворожих мереж і логістичних ланцюгів; *cyber kamikaze* (*кібер-камікадзе*) – самознищувальне шкідливе програмне забезпечення, розроблене для одноразового проникнення на високовартісні цілі, знищуючи себе після виконання місії; *psychological hacking* (*психологічний злом*) – цілеспрямовані атаки, спрямовані на маніпулювання моральним станом солдатів і цивільних осіб через ретельно підготовлені інформаційні операції; *digital sabotage* (*цифровий саботаж*) – скоординовані атаки на системи промислового контролю та критичну інфраструктуру для порушення виробничих і логістичних можливостей противника.

Ці нові терміни виникли як відповідь на специфічні оперативні потреби та бойовий досвід, відображаючи новітні тенденції у веденні кібервійсь. Формування цієї спеціалізованої лексики демонструє, як реальні бойові умови впливають на розвиток мови кібербезпеки. Одним із ключових понять став термін *cyber-artillery barrage* (*кібер-артобстріл*), який описує координаровані кібератаки, поєднані з фізичними артилерійськими обстрілами. Цей термін виник з практики синхронізації традиційних бойових дій з кібератаками на інформаційну інфраструктуру противника. Значного поширення набуло поняття *digital trench*, що означає *захисні мережеві бар'єри, створені для захисту критично важливих інформаційних ресурсів*. Цей термін аналогічний традиційним інженерним спорудам, але адаптований до умов кіберпростору. У сфері організації оборони з'явився термін *IT-*

territorial defense (*IT-тероборона*), який позначає добровольчі IT-формування, що захищають український кіберпростір. Це поняття поєднує технологічну складову з історичною традицією територіальної оборони.

Аналіз новітньої термінології показує кілька ключових тенденцій. По-перше, спостерігається тісне переплетення традиційної військової лексики з кібернетичними поняттями. По-друге, нові терміни часто мають описовий характер і ґрунтуються на аналогіях з фізичними явищами. По-третє, термінологія швидко адаптується до оперативних потреб і бойового досвіду.

Сучасна термінологія кібербезпеки продемонструвала здатність до швидкої еволюції в умовах реальних бойових дій. Вона продовжує динамічно розвиватися, відображаючи нові виклики та технології, що з'являються на полі бою. Ці неологізми вже увійшли до професійного вжитку і формують основу для подальшого розвитку термінологічної системи кібербезпеки.

Таким чином, лінгвістичні процеси цього періоду відзначаються кількома ключовими тенденціями:

Акронімізація стала одним з найпродуктивніших методів термінотворення. Поряд із вже існуючими *DDoS, VPN та SSL*, з'явилися нові скорочення: *EDR (Endpoint Detection and Response) – виявлення та реагування на кінцевих пристроях; SOAR (Security Orchestration, Automation and Response) – оркестрація, автоматизація та реагування в безпеці; CASB (Cloud Access Security Broker) – безпечний доступ до хмарних сервісів.*

Гібридизація та словоскладання продовжують активно розвиватися, утворюючи складні терміни: *Zero-trust architecture – архітектура нульової довіри; DevSecOps (Development + Security + Operations) – інтеграція безпеки в процеси розробки; crypto-ransomware – криптографічне програмне забезпечення-вимагач.*

Семантична еволюція проявилася в розширенні значень існуючих слів: термін «*resilience*» (стійкість) набув спеціалізованого значення у словосполученні *cyber resilience;* поняття «*intelligence*» (*розвідка*) стало використовуватися в контексті *threat intelligence.* Міждисциплінарне

запозичення значно посилилося: з економіки прийшов термін «*governance*» (*кіберуправління*); з психології – «*behavioral analytics*» (*аналіз поведінки*); з біології – «*immune system*» *(імунна система*) для опису адаптивних систем захисту.

Отже, формування термінології відбувалося етапно, що було обумовлено технологічним прогресом, появою нових загроз та розширенням сфери застосування. Від розрізнених технічних понять на початковому етапі система еволюціонувала до структурованого, міждисциплінарного комплексу термінів, що охоплює технічні, правові, соціальні та управлінські аспекти.

Кожен етап характеризувався своєю специфікою: від зародження базових концепцій та локального вжитку, через становлення ядра термінології у 1980–1990-х, до її стрімкої експансії та систематизації з розвитком Інтернету. Сучасний етап ознаменувався прагненням до глобальної стандартизації, що відображає інтернаціональний характер кіберзагроз та необхідність узгоджених підходів до захисту.

Терміносистема продемонструвала динамічність та здатність до адаптації, активно поповнюючись шляхом власного термінотворення, запозичень із суміжних галузей та іншомовних джерел. Це забезпечило їй здатність адекватно відображати новітні технології, такі як хмарні обчислення, Інтернет речей та штучний інтелект.

Таким чином, англомовна терміносистема кібербезпеки пройшла шлях від вузькоспеціалізованого технічного лексикону до складної, багаторівневої та відкритої для подальшого розвитку системи, що відіграє ключову роль у глобальній комунікації та забезпеченні безпеки цифрового простору.

1.4. Методика добору та аналізу матеріалу

Концепції методології наукових досліджень відіграють ключову роль у забезпеченні об'єктивності та валідності результатів наукової праці. Адекватний підбір методологічних інструментів оптимізує хід дослідження, підвищуючи його ефективність та достовірність підсумкових висновків.

У науковій практиці методи прийнято класифікувати на дві основні групи: загальнонаукові, що мають універсальне застосування в різних дисциплінах, та спеціалізовані (лінгвістичні), адаптовані до вивчення мовних систем. У рамках цього дослідження до загальнонаукових методів належить метод аналізу. Його застосування дозволило провести детальне дослідження об'єкта, зокрема структурно-семантичних особливостей англомовних термінів кібербезпеки та механізмів їх перекладу українською мовою. Завдяки цьому були визначені ключові способи формування та функціонування сучасної англомовної термінології в галузі інформаційної безпеки. Як зазначають фахівці, саме аналітичний метод створює методологічну основу для проведення глибинного компонентного, концептуального та лінгвокультурологічного аналізу мовних явищ [12, с. 56].

Метод синтезу дав можливість інтегрувати окремі складові об'єкта дослідження, які були виділені в процесі аналізу, відновити між ними зв'язок та розглянути англомовну термінологію кібербезпеки як цілісну систему. Як один із базових методів, метод порівняння дозволив виявити спільні та відмінні риси української та англійської мов при передачі термінів кібербезпеки. Метод моделювання був застосований для дослідження формальних структур англомовних термінів, а метод лінгвістичного аналізу – для вивчення їх семантичної організації.

Спеціальні лінгвістичні методи спрямовані на дослідження мови як системи, мовленнєвої діяльності та комунікативних процесів, і володіють власною методологічною специфікою. У теорії мовознавства наявність

унікального методу часто розглядається як ознака становлення самостійного наукового напряму, оскільки саме він визначає підходи до аналізу мовних явищ [11, с. 73]. У цій роботі метод лінгвістичного спостереження був використаний для фіксації та аналізу функціонування лексики кібербезпеки в англомовному дискурсі.

Завдяки застосуванню порівняльно-історичного методу було виокремлено ключові етапи формування та еволюції англомовної термінології кібербезпеки, що зумовлювалися технологічними проривами та соціокультурними чинниками. Зіставний (контрастивний) метод дав змогу виявити структурні та семантичні особливості двох мов у цій галузі, проаналізувати ступінь і механізми мовного впливу в умовах глобалізації, а також конкретизувати типові труднощі, пов'язані з перекладом лексичних одиниць кібербезпеки. Таким чином, цей метод сприяв виявленню як універсальних, так і специфічних рис у неспоріднених мовах. На думку дослідників, саме контрастивний підхід є інструментом для глибинного пізнання системно-функціональних закономірностей мов.

У процесі перекладу англомовних термінів кібербезпеки українською мовою було використано трансформаційний аналіз. Він був спрямований на виявлення змін у структурі та формі термінів під час міжмовної передачі. Цей аналіз також застосовувався для дослідження процесів термінотворення, а також лексичної та граматичної семантики. За його допомогою було систематизовано основні способи утворення термінів та проінтерпретовано окремі значення (семи) на основі дефініцій з авторитетних тлумачних словників англійської мови.

Окрім якісних характеристик, мова виявляє й кількісні закономірності, які реалізуються в мовленні та тексті. У ході дослідження було проведено власні підрахунки частотності різних лінгвістичних явищ, що розширило розуміння функціонування термінології та дозволило виявити глибинні закономірності. За допомогою статистичного методу було встановлено кількісні параметри лексики англомовної терміносистеми кібербезпеки та

визначено найпоширеніші способи її перекладу, що дало змогу встановити об'єктивні тенденції в адаптації цієї лексики.

Запропонована методологія дослідження терміносистеми кібербезпеки та її окремих одиниць в англійській мові передбачає реалізацію п'яти послідовних етапів аналізу.

На першому етапі дослідження було зосереджено увагу на основних категоріях термінознавства, щодо визначення яких у науковому середовищі досі тривають дискусії, – термін, термінологія, терміносистема. Було проаналізовано сучасні наукові підходи до дефініції цих понять із метою виокремлення їхніх суттєвих характеристик та сформульовано власні операційні визначення для потреб цієї роботи.

Отже, на стартовій фазі дослідження були залучені класичні загальнонаукові методи: аналіз, синтез, пояснення, спостереження, індукція, дедукція, порівняння, зіставлення, узагальнення та аналогія. Основою методології став системний підхід, що дозволяє досліджувати мову та її складові як цілісні організовані структури.

На другому етапі методи аналізу, спостереження, узагальнення та пояснення були спрямовані на комплексний опис терміносистеми кібербезпеки англійською мовою та її базових одиниць. Для реконструкції історії формування та еволюції цієї термінології, визначення ключових етапів її розвитку та аналізу інноваційної лексики були використані елементи діахронічного аналізу, метод опису та аналіз механізмів термінотворення.

У сучасному мовознавстві пріоритетним є саме системний підхід до вивчення мовних явищ. У рамках цього дослідження він передбачає розгляд термінології кібербезпеки як спеціальної знакової системи, а терміносистеми – як сукупності мовних одиниць, що впорядковано відображають систему понять відповідної галузі знань на різних стадіях її становлення, структурної організації та функціонального вдосконалення.

На третьому етапі дослідження було застосовано словотвірний метод. Сучасна англомовна термінологія кібербезпеки знаходиться у стані

постійного оновлення, що відбувається через ретермінологізацію, термінологізацію загальновживаної лексики, а також завдяки морфологічним та синтаксичним способам словотворення або запозиченню з інших мов.

Актуальність вивчення структури термінів зумовлена стрімким науково-технічним прогресом, який постійно генерує нові поняття. Мова стикається з необхідністю асимілювати цю «новизну», оскільки робота з застарілим термінологічним апаратом стає неможливою. У відповідь на це деякі терміни ускладнюються, стаючи багатокомпонентними, а потім піддаються процесу абревіації, що відповідає принципу мовної економії. Для аналізу цих процесів було використано структурний та компонентний методи. Структурна організація терміна має важливе значення для ефективної комунікації фахівців. Чим складнішою є форма терміна, тим складнішим стає процес його декодування, що може ускладнювати обмін інформацією. Метод лінгвістичного аналізу дозволив виявити найпродуктивніші моделі термінотворення, що є основою для рекомендацій щодо формування нових одиниць та систематизації існуючих. Метод кількісного аналізу фактичного матеріалу було застосовано для дослідження лексичного складу, семантики та встановлення об'єктивних закономірностей, що підтверджує системний, цілісний і динамічний характер термінології кібербезпеки.

На четвертому етапі дослідження були використані словотвірний, семантичний, компонентний аналіз та аналіз безпосередніх складників. Увагу було приділено семантичним особливостям термінів кібербезпеки, зокрема механізмам семантичної деривації, завдяки яким відбувається збагачення лексики. Терміни можуть розширювати своє значення, виходити за межі вихідної терміносистеми або функціональної сфери, зазнавати процесів ретермінологізації та детермінологізації. Лінгвістичний підхід дозволив проаналізувати, якими саме лексичними одиницями (з точки зору їх форми та семантики) репрезентовані поняття цієї галузі, а також вивчити метафоричні та метонімічні моделі у термінотворенні. Сфера кібербезпеки охоплює

різноманітні види діяльності, кожен з яких формує власний термінологічний пласт. Шляхом лексикографічного аналізу та методу суцільної вибірки з сучасних англомовних джерел було виокремлено шість ключових тематичних груп термінів, що відображають основні напрями галузі. Застосування кількісного аналізу дозволило отримати статистично валідні результати щодо частотності та розподілу лексичних одиниць у цих групах.

На п'ятому етапі дослідження був застосований метод перекладацького аналізу. У межах цієї роботи даний метод розглядається як комплекс стратегій і прийомів, спрямованих на досягнення адекватного перекладу, що передбачає точну передачу змісту оригіналу з урахуванням його граматичних, лексичних, стилістичних та синтаксичних особливостей. У роботі детально аналізуються способи передачі термінології кібербезпеки українською мовою, серед яких транскрибування, транслітерація, калькування, описовий переклад та контекстуальні заміни.

За допомогою низки спеціальних прийомів, спрямованих на розв'язання завдань зі збереження смислового навантаження та комунікативного впливу вихідного тексту, а саме: методів сприйняття та інтерпретації, що залежать від індивідуального досвіду перекладача, а також методів, що базуються на його фахових мовних та текстових знаннях (знання когнітивної, інформаційної та термінологічної сфери) – було здійснено аналіз перекладацьких трансформацій. Це дозволило визначити типові труднощі перекладу англомовних скорочень та термінологічних комплексів у сфері кібербезпеки та запропонувати шляхи їх подолання.

Отже, системне застосування викладеної методології підтверджує статус англомовної термінології кібербезпеки як повноцінного об'єкта лінгвістичного дослідження. Використані методи мають як суто мовознавчу, так і загальнонаукову природу. Таким чином, у вивченні термінології кібербезпеки ефективно поєднуються методологічні підходи точних та гуманітарних наук, що забезпечує глибокий та об'єктивний аналіз мовного матеріалу.

РОЗДІЛ 2
СТРУКТУРНО-СЕМАНТИЧНІ ОСОБЛИВОСТІ АНГЛОМОВНИХ ТЕРМІНІВ КИБЕРБЕЗПЕКИ

2.1. Морфологічні особливості англомовної терміносистеми кібербезпеки

Формування термінології будь-якої галузі знань, зокрема кібербезпеки, є динамічним процесом, що відображає її розвиток і ускладнення. Одним з ключових аспектів вивчення терміносистеми є аналіз її морфологічної структури, який дозволяє виявити основні шляхи поповнення лексичного складу та домінуючі моделі словотвору. У контексті англомовної термінології кібербезпеки такий аналіз набуває особливої актуальності через її швидке зростання та мінливість.

Аналіз структури англомовної термінології кібербезпеки дозволяє виокремити п'ять основних морфологічних моделей словотвору, що формують її ядро. Кожен із цих способів має різний ступінь продуктивності та виконує специфічні функції в номінації понять. Нижче наведено детальний огляд цих механізмів із зазначенням статистичних даних, отриманих шляхом аналізу корпусу із 1333 найуживаніших термінів сфери кібербезпеки.

Дослідження структурних особливостей англомовної термінології кібербезпеки ґрунтувалося на загальноприйнятій лінгвістичній класифікації, згідно з якою терміни поділяються на прості, складні, терміносполучення та скорочення [21, с. 46]. У межах цієї системи прості терміни класифікуються на кореневі (основа яких збігається з коренем) та афіксальні. Терміносполучення, в свою чергу, аналізуються за кількістю компонентів (дво-, три-, багатокомпонентні) та їх формально-граматичними зв'язками

Розглянемо англомовні терміни кібербезпеки з погляду цієї класифікації:

Проведений аналіз демонструє різноманітність структурних моделей у термінології кібербезпеки:

- однокомпонентні терміни (22%): *firewall – захисний екран; malware – шкідливе програмне забезпечення; phishing – викрадення конфіденційних даних; ransomware – шантажувальне програмне забезпечення; botnet – мережа заражених комп'ютерів. The company installed a new firewall to protect its internal network* [111]. *– Компанія встановила новий межовий екран для захисту внутрішньої мережі* [107]. *Malware detection requires regular system scanning* [112]. *– Виявлення шкідливого ПЗ вимагає регулярного сканування системи* [103];

- двокомпонентні терміни (35%): *data encryption – шифрування даних; access control – контроль доступу; security audit – перевірка безпеки; network scanning – сканування мережі; threat analysis – аналіз загроз. Data encryption ensures confidentiality of sensitive information* [112]. *– Шифрування даних забезпечує конфіденційність важливої інформації* [103]. *Effective access control prevents unauthorized entry to systems* [111]. *– Ефективний контроль доступу запобігає несанкціонованому доступу до систем* [107]*;*

- трикомпонентні терміни (25%): *intrusion detection system – система виявлення вторгнень; advanced persistent threat – розвинена стійка загроза; security information management – управління інформацією безпеки; data loss prevention – запобігання втраті даних. The intrusion detection system alerted administrators about suspicious activity* [114]. *– Система виявлення вторгнень попередила адміністраторів про підозрілу активність* [103]. *Advanced persistent threat attacks require sophisticated defense strategies* [114]. *– Атаки розвинених стійких загроз вимагають складних стратегій захисту* [103];

- багатокомпонентні терміни (15%): *multifactor authentication system – система багатофакторної автентифікації; zero-day vulnerability*

exploitation – використання вразливостей нульового дня; cloud security posture management – управління станом хмарної безпеки. Multifactor authentication system significantly enhances account security [111]. *– Система багатофакторної автентифікації значно підвищує безпеку облікових записів* [107];. *Zero-day vulnerability exploitation poses serious risks to unprotected systems* [111]. *– Використання вразливостей нульового дня становить серйозні ризики для незахищених систем* [107];

- абревіатури та скорочення (3%): *IDS/IPS [Intrusion Detection/Prevention System] – система виявлення/відбиття вторгнень; SIEM [Security Information and Event Management] – управління інформаційною безпекою та подіями; DDoS [Distributed Denial of Service] – розподілена атака типу «відмова в обслуговуванні»; VPN [Virtual Private Network] – віртуальна приватна мережа. The IDS/IPS successfully blocked the network attack* [114]. *– Система виявлення/відбиття вторгнень успішно заблокувала мережеву атаку* [107]. *DDoS attacks can paralyze online services for hours* [111]. *– Атаки типу «відмова в обслуговуванні» можуть паралізувати онлайн-сервіси на години* [107].

Перевага двокомпонентних та трикомпонентних термінів пояснюється потребою у точному визначенні складних понять кібербезпеки, що вимагає уточнення об'єкта, типу дії та контексту. Однокомпонентні терміни часто є базовими поняттями, тоді як багатокомпонентні відображають спеціалізовані технології та процеси. Низька частка абревіатур пов'язана з їхньою специфічністю та професійним характером використання.

За будовою англомовні терміни кібербезпеки поділяються на такі категорії [20, 74]:

1. прості терміни (30%) – складаються з одного слова: *malware – шкідливе програмне забезпечення; phishing – викрадення конфіденційних даних; ransomware – шантажувальне програмне забезпечення; encryption – шифрування; virus – комп'ютерний вірус*. *Phishing attacks often use fake emails to steal login credentials* [111]. *– Фішингові атаки часто використовують*

підроблені електронні листи для крадіжки облікових даних [107]. *Malware infection can cause significant data loss and system damage* [113]. – *Зараження шкідливим ПЗ може спричинити значну втрату даних і пошкодження системи* [104].

2. складні терміни (25%) – утворені шляхом складання двох основ: cybersecurity – *кібербезпека, username – ім'я користувача*; *password – пароль; keylogger – клавіатурний шпигун; spyware – шпигунське ПЗ; adware – рекламне ПЗ. Strong passwords are essential for account security* [113]. – *Надійні паролі є важливими для безпеки облікових записів* [104]. *Spyware collection personal information without user consent* [110]. – *Шпигунське ПЗ збирає особисту інформацію без згоди користувача* [107].

3. терміни-словосполучення (45%) – складаються з декількох окремих слів: *intrusion detection system – система виявлення вторгнень; two-factor authentication - двофакторна автентифікація; data loss prevention – запобігання втраті даних; advanced persistent threat – розвинена стійка загроза; security information and event management – управління інформаційною безпекою та подіями. The intrusion detection system immediately alerted administrators about the breach* [114]. – *Система виявлення вторгнень негайно повідомила адміністраторів про порушення* [105]. *Two-factor authentication provides an additional layer of security for user accounts* [111]. – *Двофакторна автентифікація забезпечує додатковий рівень безпеки для облікових записів користувачів* [106].

Перевага термінів-словосполучень пояснюється потребою у точному визначенні складних понять кібербезпеки, що часто вимагає вказівки на конкретний об'єкт, тип дії та технологію. Прості терміни зазвичай позначають базові фундаментальні поняття, тоді як складні часто виникають шляхом поєднання існуючих термінів для утворення нових концепцій.

До простих термінів кібербезпеки належать:

1) *слова загальновживаної лексики, що набули спеціалізованого значення (48%): worm – мережевий черв'як (шкідлива програма); virus –*

комп'ютерний вірус; trojan – троянська програма; spam – небажана електронна пошта; patch – оновлення безпеки; host – мережевий пристрій; cookie – файл збереження даних; root – привітований доступ. The security team discovered a new worm spreading through the corporate network [112]. *– Команда безпеки виявила новий мережевий черв'як, що поширювався корпоративною мережею* [105]. *Regular software patches are essential for protecting against known vulnerabilities* [112]. *– Регулярні оновлення програмного забезпечення необхідні для захисту від відомих вразливостей* [105].

2) слова, що переважно використовуються як терміни (52%): *malware – шкідливе програмне забезпечення; ransomware – програма-вимагач; firewall – захисний екран; encryption – шифрування; phishing – викрадення конфіденційних даних; botnet – мережа заражених комп'ютерів; cryptography – криптографія. Ransomware attacks have become increasingly sophisticated and targeted* [114]. *– Атаки програмами-вимагачами стали більш складними та цілеспрямованими. Strong encryption protocols protect data during transmission over the internet* [112]. *– Надійні протоколи шифрування захищають дані під час передачі через Інтернет.*

Конверсія як мовне явище відіграє важливу роль у формуванні термінологічного апарату кібербезпеки. Цей морфолого-синтаксичний спосіб словотворення дозволяє створювати нові терміни шляхом переходу слів з однієї частини мови в іншу без зміни їхньої форми. *V→ N: Security experts constantly monitor network traffic for suspicious activity* [114]. *– Фахівці з безпеки постійно моніторять мережевий трафік на наявність підозрілої активності* [105]. *Continuous monitor of system logs helps detect intrusions early* [112]. *–Постійний моніторинг системних логів допомагає виявляти вторгнення на ранніх стадіях* [105]. *N → V: Cybercriminals often target small businesses with ransomware attacks* [114]. *– Кіберзлочинці часто цілять на малий бізнес з атаками програм-вимагачів* [103]. *The main target of the attack*

was the company's customer database [114]. – *Головною ціллю атаки була база даних клієнтів компанії* [103].

Продуктивність конверсії в кібербезпеці пояснюється швидким розвитком технологій, який вимагає оперативного формування нових термінів. Наприклад, слово «*phish*» спочатку використовувалося як дієсло («*to phish*»), а згодом утворило іменник «*phishing*» для позначення цілого класу кібератак. Аналогічно, термін «*exploit*» може використовуватися як дієсло («*to exploit vulnerabilities*») та як іменник («*zero-day exploit*»), що демонструє гнучкість та адаптивність термінології кібербезпеки до нових викликів цифрового середовища.

Аналіз термінологічного апарату кібербезпеки демонструє чітку структуру за частинами мови, що відображає специфіку цієї галузі знань. Проведене дослідження виявляє таке розподілення:

1) іменники (N) – 82%. Найчисленніша група, що включає найважливіші поняття галузі: *firewall* – захисний екран; *malware* – шкідливе програмне забезпечення; *encryption* – шифрування; *vulnerability* – вразливість; *breach* – порушення безпеки. *A robust firewall is essential for network protection* [110]. – *Надійний межовий екран є необхідним для захисту мережі* [107]. *The company experienced a major data breach last month* [112]. – *Компанія зазнала серйозного порушення захисту даних минулого місяця* [107];

2) дієслова (V) – 11%. Включають терміни, що описують дії та процеси: *to hack* – несанкціоновано проникати; *to scan* – сканувати мережу; *to encrypt* – шифрувати дані; *to authenticate* – перевіряти справжність; *to mitigate* – пом'якшувати наслідки. *Security experts scan networks for vulnerabilities daily* [114]. – *Фахівці з безпеки сканують мережі на наявність вразливостей щодня* [105]. *Companies must encrypt sensitive customer information* [113]. – *Компанії повинні шифрувати конфіденційну інформацію клієнтів* [107];

3) прикметники (Adj) – 6%. Характеризують властивості та стан систем безпеки: *secure* – захищений; *vulnerable* – вразливий; *encrypted* –

зашифрований; *malicious* – зловмисний; *compromised* – скомпрометований. *All passwords should be stored in encrypted form* [110]. – *Усі паролі мають зберігатися у зашифрованому вигляді* [105]. *The system was vulnerable to simple phishing attacks* [111]. – *Система була вразливою до простих фішингових атак* [104];

4) прислівники (Adv) – 1%. Включають нечисленні терміни, що визначають спосіб дії: *securely* – безпечно; *remotely* – віддалено; *maliciously* – зловмисно. *Data must be transmitted securely over the internet* [110]. – *Дані мають передаватися безпечно через Інтернет* [105]. *The attacker remotely accessed the company's servers* [110]. – *Зловмисник віддалено отримав доступ до серверів компанії* [105].

Переважання іменників у термінології кібербезпеки пояснюється необхідністю номінації великої кількості понять, технологій, інструментів та явищ. Дієслова відображають динамічний характер галузі, акцентуючи увагу на процесах та діях, тоді як прикметники та прислівники виконують описову функцію, конкретизуючи характеристики об'єктів та способи виконання дій.

До простих термінів кібербезпеки належать три основні категорії: кореневі (27%), афіксальні (41%) та складні терміни (32%).

Кореневі терміни характеризуються простою морфологічною будовою і становлять помітну групу в термінології: *hack – несанкціоноване проникнення; spam – небажана кореспонденція; patch – оновлення безпеки; host – мережевий пристрій; bug – помилка безпеки; scan – сканування мережі; code – програмний код. The security team prevented an attempt to hack the corporate database* [112]. – *Команда безпеки запобігла спробі зламати корпоративну базу даних* [105]. *The security bug allowed unauthorized access to user accounts* [112]. – *Безпекова помилка дозволяла несанкціонований доступ до облікових записів користувачів* [105].

Переважна більшість кореневих термінів мають англомовне походження, проте спостерігаються і запозичення з інших мов: *virus (з латини) – комп'ютерний вірус; trojan (з грецької) – троянська програма;*

phishing (змодифіковане fishing) – викрадення даних; botnet (від robot + network) – мережа ботів; malware (від malicious + software) – шкідливе ПЗ.

Ці терміни утворюють семантичне ядро термінології кібербезпеки та виконують фундаментальну функцію в професійній комунікації. Їхня структурна простота поєднується з семантичною точністю, що робить їх особливо ефективними для опису базових понять галузі.

Основним механізмом морфологічного словотворення в англомовній термінології кібербезпеки є суфіксація, яка становить приблизно 12% від усіх термінів у вибірці. Різні групи суфіксів спеціалізуються на вираженні належності похідного слова до певної функціональної або семантичної категорії. Процесуальне значення найяскравіше виражають терміни з суфіксом: **-ing**: *scanning – сканування (мережі, систем); phishing – викрадення конфіденційних даних; monitoring – моніторинг (активності, подій); encoding – кодування (даних); cracking – підбір (паролів), злам;* **-tion/-ation**: *encryption – шифрування; authentication – автентифікація; protection – захист; detection – виявлення (вторгнень, загроз); verification – верифікація, підтвердження;* **-ity**: *vulnerability – вразливість; confidentiality – конфіденційність; integrity – цілісність (даних); availability – доступність; security – безпека. Scanning for open ports is a common first step in a cyber attack* [111]. *– Сканування відкритих портів є звичайним першим кроком у кібератаці* [108]. *Continuous monitoring of network traffic helps detect intrusions in real-time* [106]. *– Безперервний моніторинг мережевого трафіку допомагає виявляти вторгнення в реальному часі* [103]. *Data encryption is essential for protecting sensitive information* [106]. *– Шифрування даних є важливим для захисту конфіденційної інформації* [107]. *Multi-factor authentication adds an extra layer of security to user accounts* [106]. *– Багатофакторна автентифікація додає додатковий рівень безпеки обліковим записам користувачів* [109]. *A software update was released to address a critical vulnerability in the system* [108]. *– Оновлення програмного забезпечення було випущене для усунення критичної вразливості в системі*

[107]. *Ensuring data confidentiality is a key principle of information security* [106]. – *Забезпечення конфіденційності даних є ключовим принципом інформаційної безпеки* [107].

Менш поширеним, але все ще вживаним є суфікс **-ability**: *accountability – підзвітність; reliability – надійність; interoperability – взаємодія, сумісність; usability – зручність використання. System reliability is crucial for maintaining business operations during an attack* [106]. – *Надійність системи є вирішальною для підтримання бізнес-операцій під час атаки* [107]. *The usability of a security tool affects how effectively employees will use it* [106]. – *Зручність використання інструменту безпеки впливає на те, наскільки ефективно співробітники будуть його використовувати* [107].

Термінологічні одиниці зі значенням особи, пристрою або інструмента утворюються за допомогою суфікса **-or/-er**: *scanner – сканер (мережевий, вразливостей); monitor – монітор (активності); administrator – адміністратор (системи, мережі); intruder – зловмисник, той, хто вторгається; encryptor – шифрувальний пристрій; protector – захисний механізм; investigator – слідчий (кіберзлочинності). A network scanner identified several unauthorized devices on the corporate network* [112]. – *Мережевий сканер виявив кілька несанкціонованих пристроїв у корпоративній мережі* [103]. *The system administrator is responsible for applying security patches* [113]. – *Адміністратор системи відповідає за встановлення патчів безпеки* [104].

Суфіксальний спосіб передбачає додавання суфіксів для утворення нових термінів із певним категоріальним значенням. Суфікс ***-ware*** активно використовується для позначення різних типів програмного забезпечення, зокрема шкідливого: *malware (шкідливе ПЗ*) – узагальнювальний термін для всіх типів шкідливих програм, *spyware (шпигунське ПЗ)* – програми, що таємно збирають інформацію про користувача, *adware (рекламне ПЗ)* – програми, що показують небажану рекламу, *ransomware (програма– вимагач)* – шкідливе ПЗ, що шифрує дані й вимагає викуп за їх відновлення. *Security*

experts discovered new ***malware*** *that can bypass traditional antivirus protection* [103]. – *Фахівці з безпеки виявили нове шкідливе ПЗ, яке здатне обійти традиційний антивірусний захист* [108]. *The company's network was infected with spyware that collected employees' login credentials* [103]. – *Мережа компанії була заражена шпигунським ПЗ, яке збирало облікові дані співробітників* [104].

Суфікс ***-proof*** використовується для позначення стійкості або захищеності від певних впливів: *tamper-proof (стійкий до втручання*) – захищений від несанкціонованих змін, *bulletproof (підвищено захищений*) – система з максимальним рівнем захисту, *foolproof (надійний, безпечний*) – система, що мінімізує можливість помилок користувача: *Military organizations require bulletproof communication systems that resist cyber attacks* [103]. – *Військові організації потребують надзахищених систем зв'язку, стійких до кібератак* [107]. *The foolproof authentication system prevents common user errors during login* [103]. – *Надійна система автентифікації запобігає поширеним помилкам користувачів під час входу* [109].

Префіксація є важливим, хоча і менш поширеним порівняно з суфіксацією, способом словотворення в англомовній термінології кібербезпеки. Різні префікси допомагають уточнити семантику термінів, вказуючи на характер дії, що є особливо важливим для точної комунікації у цій сфері. Найпродуктивнішим у терміносистемі кібербезпеки є префікс ***cyber-*** , який вказує на зв'язок із цифровим простором або Інтернетом. Цей префікс активно використовується для утворення термінів: *cyberattack* (*кібератака*) – злочинна дія, спрямована на комп'ютерні системи через мережу, *cybersecurity* (*кібербезпека*) – сукупність заходів із захисту цифрових систем, *cybercrime* (*кіберзлочин*) – злочинна діяльність у кіберпросторі, *cyberespionage* (*кібершпигунство*) – несанкціоноване отримання конфіденційної інформації через цифрові канали, *cyberwarfare* (*кібервійна*) – використання цифрових атак у військових цілях. *A sophisticated cyberattack targeted the government's critical infrastructure, causing significant disruptions*

[106]. – *Складна кібератака націлилася на критичну інфраструктуру уряду, спричинивши значні порушення* [109]. *International cooperation is essential to combat the growing threat of cybercrime effectively* [114]. – *Міжнародна співпраця є важливою для ефективної боротьби зі зростаючою загрозою кіберзлочинності* [109]. *The company invested heavily in cybersecurity following a major data breach* [112]. – *Компанія значно інвестувала в кібербезпеку після серйозного витоку даних* [109]. *Cyberespionage campaigns often target intellectual property and trade secrets* [111]. – *Кампанії кібершпигунства часто націлені на інтелектуальну власність та комерційні таємниці* [105].

Іншим продуктивним префіксом є ***multi-*** , який вказує на множинність або комплексність: *multifactor authentication* (*багатофакторна автентифікація*) – метод перевірки ідентичності з використанням кількох незалежних факторів, *multilayer defense* (*багаторівневий захист*) – стратегія безпеки з кількома рівнями захисту, *multitenant architecture* (*багатокористувацька архітектура*) – система, що обслуговує одночасно кількох користувачів або організацій. *Multifactor authentication requires users to provide both a password and a verification code from their mobile device* [112]. – *Багатофакторна автентифікація вимагає від користувачів надання як пароля, так і коду підтвердження зі свого мобільного пристрою* [105]. – *A multilayer defense strategy includes firewalls, intrusion detection systems, and endpoint protection* [111]. – *Стратегія багаторівневого захисту включає міжмережеві екрани, системи виявлення вторгнень та захист кінцевих точок* [109].

Префікс ***re-*** передає значення повторення дії: *re-encryption – повторне шифрування; re-authentication – повторна автентифікація.* У кібербезпеці він часто використовується для опису процесів, які потрібно виконувати регулярно або повторно. *The system requires periodic re-encryption of stored data to maintain security* [106]. – *Система вимагає періодичного перешифрування збережених даних для підтримання безпеки* [105]. *After a session timeout, users must complete re-authentication to access the platform*

[106]. – *Після закінчення сесії користувачі повинні пройти повторну автентифікацію для доступу до платформи* [105].

Префікс ***de-*** має значення «зворотності» або «позбавлення»: *decryption – розшифрування; deauthentication – деавтентифікація (розрив автентифікованого з'єднання)*. Він часто вказує на процеси, зворотні до основних операцій безпеки. *The decryption of the stolen files required a special cryptographic key* [106]. – *Розшифрування викрадених файлів вимагало спеціального криптографічного ключа* [105]. *The access point initiated deauthentication of all connected devices during the attack* [106]. – *Точка доступу ініціювала деавтентифікацію всіх підключених пристроїв під час атаки* [105].

Префікс ***mis-*** вказує на неправильність або помилковість дії: *misdelivery – неправильна доставка (даних); misconfiguration – неправильна конфігурація (системи безпеки)*. У контексті безпеки він часто позначає помилки, які можуть призвести до уразливостей. *The misdelivery of sensitive email to wrong recipients caused a data breach* [112]. – *Неправильна доставка конфіденційного листа не тим одержувачам спричинила витік даних* [105]. *A simple misconfiguration of the firewall allowed attackers to penetrate the network* [112]. – *Проста неправильна конфігурація міжмережевого екрана дозволила зловмисникам проникнути в мережу* [104].

Префікс ***anti-*** виражає значення протидії або запобігання: *antivirus – антивірус; antimalware – антивірусне програмне забезпечення*. Це один з найпоширеніших префіксів у термінології кібербезпеки. *The company installed new antivirus software on all corporate computers* [111]. – *Компанія встановила нове антивірусне програмне забезпечення на всі корпоративні комп'ютери* [104]. *Effective antimalware protection requires regular signature updates* [111]. – *Ефективний захист від шкідливого ПЗ вимагає регулярного оновлення сигнатур* [104].

Префікс ***counter-*** має значення протилежності або протидії: *countermeasure – контр засіб; counterintelligence – контррозвідка (у*

кіберпросторі). Він часто використовується для позначення заходів, спрямованих на протидію загрозам. *As a countermeasure against DDoS attacks, the company implemented traffic filtering* [113]. – *Як контрзасіб від DDoS-атак компанія впровадила фільтрацію трафіку* [105]. *Cyber counterintelligence operations aim to identify and neutralize foreign threats* [114]. – *Операції кіберконтррозвідки спрямовані на виявлення та нейтралізацію іноземних загроз* [105].

Ці префікси допомагають уточнити семантику термінів, вказуючи на характер дії (повторення, зворотність, протидія), що є особливо важливим для точної комунікації у сфері кібербезпеки, де кожен процес має бути чітко визначеним.

Префіксально-суфіксальний спосіб словотворення поєднує використання префіксів і суфіксів для утворення складніших термінів: *decryption – процес розшифрування* (префікс de- + суфікс -tion); *reconfiguration – повторна конфігурація* (префікс re- + суфікс -ation) *disinfection – видалення шкідливого програмного забезпечення* (префікс dis- + суфікс -ion). *The decryption process took several hours due to the strong encryption algorithm* [111]. – *Процес розшифрування зайняв кілька годин через сильний алгоритм шифрування* [109]. *After the security breach, the IT team performed a complete reconfiguration of the network* [112]. – *Після порушення безпеки IT-команда провела повну перенастройку мережі* [109].

У термінології кібербезпеки суфікси часто визначають частину мови та спеціалізацію значення, тоді як префікси переважно модифікують семантику, надаючи їй нового відтінку. Найактивнішими в цій сфері виявилися афікси, що сходять до споконвічного англійського словникового запасу, а також інтернаціональні морфеми, такі як *crypto-, mal-, fire-, -ware, -er, -ing*.

Таким чином, аналіз показує, що в англомовній термінології кібербезпеки домінують афікси, що виражають: агентивність та інструментальність (-er, -or), що відповідає потребі називати суб'єктів атак та засоби захисту; процесуальність (-ing, -tion), що відображає динамічну

природу кіберзагроз і контрзаходів. Ключові семантичні концепції представлено через префікси (*mal-*, *anti-*, *cyber-*), що дозволяє чітко категоризувати явища як шкідливі, захисні або належні до кіберпростору.

Отже, продуктивність афіксації в термінології кібербезпеки демонструє прямий зв'язок із функціональними потребами галузі, де необхідно точно та економно номінувати агенти, процеси та ключові атрибути цифрової безпеки.

Окрему значну групу в англомовній термінології кібербезпеки становлять терміни, утворені шляхом складання слів, які також називають термінами-композитами. Цей спосіб словотворення є високопродуктивним у сучасному термінознавстві та активно сприяє появі нових лексичних одиниць.

Активне використання словоскладання в кібербезпеці пов'язане з кількома факторами. Стрімкий розвиток технологій, поглиблення знань про цифрові загрози та поява нових складних понять вимагають створення термінів, що поєднують ознаки кількох явищ. Терміни-композити є оптимальним засобом для вираження таких комплексних понять, оскільки дозволяють зберігати смислове навантаження обох складових компонентів, одночасно відповідаючи ключовій вимозі термінології – стислості: *malware – узагальнююча назва для всіх типів шкідливого програмного забезпечення; ransomware – програма-вимагач, що шифрує дані та вимагає викуп; spyware – шпигунське програмне забезпечення для таємного збору інформації; keylogger – програма, що фіксує натискання клавіш; botnet – мережа заражених комп'ютерів, керована зловмисниками. Security software detected a keylogger that was recording all keystrokes and sending them to a remote server* [112]. – *Антивірусне програмне забезпечення виявило кейлогер, який записував всі натискання клавіш і відправляв їх на віддалений сервер* [104]. *The botnet of thousands of infected devices was used to launch a massive DDoS attack.* [112]. *Ботнет із тисяч заражених пристроїв був використаний для масової DDoS-атаки* [108].

Частиною складного терміна може бути як корінь слова, так і ціле слово. Наприклад, у терміні *blockchain* поєднує «*block*» і «*chain*» для опису технології ланцюжків блоків; термін *zero-day* поєднує поняття «*zero*» (*нуль*) та «*day*» (*день*), що вказує на вразливість, про яку ще не повідомлено розробнику, а отже, у нього є «нуль днів» на виправлення дефекту до моменту його потенційного використання зловмисниками; термін *deepfake* утворений шляхом поєднання слів «*deep learning*» (*глибоке навчання*) та «*fake*» (*підробка*). Він точно описує технологію, засновану на штучному інтелекті, яка дозволяє створювати реалістичні підроблені відео або аудіо записи; термін *cryptojacking* поєднує «*crypto*» (*від криптовалюта*) та «*jacking*» (*викрадення*). Він описує процес несанкціонованого використання обчислювальних потужностей пристрою жертви для майнінгу крипто валют; термін *whitelisting* утворений від «*white list*» (*білий список*) та суфікса «*-ing*». Він описує метод безпеки, який дозволяє виконання лише заздалегідь схвалених програм або процесів, блокуючи все інше.

Таким чином, словоскладання разом із афіксацією становлять основу термінотворення в кібербезпеці. Складні терміни, утворені шляхом поєднання двох слів (які можуть писатися разом, через дефіс або окремо), забезпечують точність, інформативність та стислість професійної комунікації у цій динамічній галузі знань: *bandwidth, checksum, crimeware, honeymonkey, netmask, ransomware, traceroute, backdoor, smartcard*. Гнучкість і продуктивність словоскладання роблять його оптимальним інструментом для швидкого реагування на нові виклики в динамічній сфері кібербезпеки.

У сучасній англомовній термінології кібербезпеки спостерігається чітко виражена тенденція до домінування багатокомпонентних термінів. Ця структурна особливість безпосередньо пов'язана зі стрімким розвитком технологій та постійною появою нових складних явищ у кіберпросторі. Більшість сучасних понять у сфері кібербезпеки вимагають деталізованого опису, який не може бути забезпечений однокомпонентними термінами.

Статистичний аналіз демонструє значну перевагу багатокомпонентних термінів, які становлять приблизно 68% від загального обсягу термінології. Натомість однокомпонентні терміни займають лише 32% термінологічного апарату. Така диспропорція має логічне пояснення. Швидкий технологічний прогрес постійно генерує нові складні поняття, які потребують точних і детальних позначень. Крім того, специфіка професійної комунікації між фахівцями з кібербезпеки вимагає максимальної однозначності та точності термінів.

Багатокомпонентні терміни часто виражають значення, яке не є простою сумою значень їхніх складових частин. Наприклад, термін «*zero-day vulnerability*» описує специфічний тип вразливості програмного забезпечення, який відрізняється від звичайних вразливостей. Цей термін означає *вразливість, невідому розробникам програмного забезпечення і, відповідно, не має доступного виправлення.* Аналогічним чином термін «*advanced persistent threat*» виражає складне поняття, яке виходить за рамки звичайного визначення загрози. Він описує *цілеспрямовану тривалу кібератаку, яка характеризується використанням складних методів і високим рівнем стійкості*. Семантика таких термінів формує нові поняття, що відображають сучасні реалії кіберпростору.

Багатокомпонентні терміни кібербезпеки можна класифікувати за кількістю складових елементів [75, с. 53]. Двокомпонентні терміни, такі як «*intrusion detection*» або «*data encryption*», є найпоширенішими у професійній комунікації. Вони забезпечують базовий рівень деталізації понять.

Трикомпонентні терміни, наприклад «*security information management*» і «*data loss prevention*», пропонують більш глибоке розкриття семантики. Такі терміни дозволяють точно ідентифікувати складні процеси та механізми захисту інформації. Найскладніші терміни, такі як «*cloud security posture management*», містять чотири і більше компонентів. Вони використовуються для опису спеціалізованих концепцій та архітектурних рішень у сучасних системах кібербезпеки.

Використання багатокомпонентних термінів повністю відповідає основним вимогам сучасної термінології. Кожен компонент такого терміна виконує уточнювальну функцію, що забезпечує високу ступінь однозначності. Ця особливість є особливо важливою у сфері кібербезпеки, де неточності у термінології можуть призвести до серйозних наслідків [81, с. 51].

Точність багатокомпонентних термінів дозволяє чітко ідентифікувати конкретні явища та процеси. Логічна структура таких термінів робить їх семантику зрозумілою та передбачуваною. При цьому зберігається принцип стислості, оскільки багатокомпонентні терміни є оптимальним способом опису складних понять.

Синтаксичні моделі утворення термінів у кібербезпеку постійно ускладнюються, що безпосередньо відображає динамічний розвиток самої галузі. Цей процес демонструє, як мова адаптується до нових викликів і технологій, забезпечуючи точне термінологічне оформлення концепцій, що постійно з'являються у кіберпросторі.

Багатокомпонентна термінологія у сфері кібербезпеки характеризується різноманітною структурою, де найпоширенішими вважаються дво- та трикомпонентні одиниці.

Так, серед двокомпонентних термінів У термінології кібербезпеки модель **N + N** є однією з найпоширеніших і становить приблизно 45% від усіх двокомпонентних термінів. Ця модель дозволяє точно визначати об'єкти та явища шляхом поєднання двох іменників, де перший виконує функцію означення: *data breach – порушення захисту даних; cybersecurity worker (кібер–працівник); security policy – політика безпеки; security breach (порушення безпеки); risk profile (профіль ризику); network traffic – мережевий трафік; access level – рівень доступу; cyber security team (кібер–команда); threat actor – суб'єкт загрози; software lifecycle (життєвий цикл програмного забезпечення); cyber security awareness (культура інформаційної безпеки); risk assessment – оцінка ризиків; application vulnerabilities*

(вразливість додатків); data system (система збору, обробки та зберігання даних).

Модель **Adj. + N** є найпоширенішою серед двокомпонентних термінів кібербезпеки і становить близько 35%. У цій моделі прикметник виконує функцію характеристики, уточнюючи та конкретизуючи значення іменника: *malicious software – шкідливе програмне забезпечення; secure connection – захищене з'єднання; digital signature – цифровий підпис; critical infrastructure – критична інфраструктура; unauthorized access – несанкціонований доступ; national security (національна безпека), corporate networks (корпоративні мережі) та cyber–attacks (кібератаки).*

Модель **Ved + N** становить приблизно 12% двокомпонентних термінів. Дієприкметник минулого часу втрачає темпоральний характер і набуває якісного значення: *encrypted data – зашифровані дані; compromised system – скомпрометована система; protected information – захищена інформація; authenticated user – автентифікований користувач.*

Модель **Ving + N** становить близько 5% двокомпонентних термінів і виражає активну дію або процес: *monitoring system – система моніторингу; learning algorithm – алгоритм навчання; blocking mechanism – блокуючий механізм; scanning tool – інструмент сканування*

Модель **N + preposition + N** становить приблизно 3% двокомпонентних термінів і використовується для вираження складних відношень між поняттями: *protection of data – захист даних; access to information – доступ до інформації; management of risks – управління ризиками; prevention of attacks – запобігання атакам*.

Ці структурні моделі демонструють системність та логічну організацію термінології кібербезпеки, що забезпечує точність та однозначність професійної комунікації у цій галузі. Кожна модель виконує специфічну функцію у формуванні термінів, що дозволяє ефективно описувати складні поняття та процеси у сфері кібербезпеки.

Атрибутивно-препозитивні моделі є характерними для багатокомпонентних термінів кібербезпеки, де підпорядковані слова деталізують різні аспекти значення головного слова. Такі структури дозволяють точно визначати складні поняття та технології.

Модель **«Adj. + N + N»** (19%). Ця модель є однією з найпоширеніших серед трикомпонентних термінів:*advanced persistent threat – розвинена стійка загроза; secure socket layer – захищений рівень сокетів; multi factor authentication – багатофакторна автентифікація; critical security control – критичний контроль безпеки; cyber intrusion attacks – кібер-вторгнення; authoritative data systems – надійні системи даних.*

Модель **«Ved + N + N»** (15%). У цій моделі дієприкметник минулого часу функціонує як прикметник: *encrypted data transmission – передача зашифрованих даних; protected health information – захищена медична інформація; authenticated user session – автентифікована сесія користувача; compromised credential detection – виявлення скомпрометованих облікових даних.*

Модель «N + N + N» (45%). Найпоширеніша модель серед трикомпонентних термінів: *data loss prevention – запобігання втраті даних; intrusion detection system – система виявлення вторгнень; security information management– управління інформацією безпеки; access control list – список контролю доступу; cybersecurity position description – опис штатної кібер-посади, computer network defense – захист комп'ютерної мережі; intrusion detection technologies – технології виявлення вторгнень.*

Модель **«Adj. + Adj. + N»** (21%). Використовується для створення точних характеристик: *advanced malware protection – розвинений захист від шкідливого ПЗ; cloud security posture – стан хмарної безпеки; zero day vulnerability – вразливість нульового дня.*

Чотирикомпонентні терміни використовуються для опису спеціалізованих концепцій: *cloud access security broker – безпечний доступ до хмарних сервісів; security orchestration automation response – оркестрація*

безпеки та автоматизація відповіді; zero trust network access – мережевий доступ з нульовою довірою; identity and access management – управління ідентифікацією та доступом.

Чотирикомпонентні терміни менш поширені і представлені моделями **N + Adj. + N + N**, як– от *cyber security human capital initiatives (ініціативи з розвитку людського капіталу в кібербезпеці),* **Adj. + Adj. + N + N** – national public awareness campaign (національна кампанія з інформування громадськості), а також **Adj. + N + PI + N** – *mature workforce planning capability (сформована здатність планування кадрової структури) і cyber workforce planning capability (можливість планування кадрового кібер-складу).*

Ці структурні моделі демонструють високий рівень системності термінології кібербезпеки. Кожна модель слугує для точного визначення специфічних аспектів кібербезпеки, від базових понять до складних технологічних рішень. Використання таких моделей забезпечує однозначність та точність професійної комунікації, що є особливо важливим у контексті швидкого розвитку технологій та постійного ускладнення кіберзагроз.

Як зазначають сучасні дослідники, абревіатури відіграють ключову роль у науковій комунікації, виконуючи маніфестуючу функцію [30, с. 83]. В термінології кібербезпеки це особливо актуально, оскільки вони дозволяють скорочувати складні багатокомпонентні терміни до компактних позначень, що значно полегшує професійну комунікацію. «Згорнуті» форми термінів не лише спрощують структуру наукових текстів, але й зберігають їх інформаційну щільність [50, с. 108].

Галузь кібербезпеки характеризується особливо високою щільністю використання абревіатур. Це пов'язано зі швидким розвитком технологій, необхідністю оперативної комунікації та наявністю великої кількості технічної документації, стандартів і протоколів. Абревіатури в кібербезпеці швидко набувають самостійного значення і починають функціонувати як

повноцінні лексичні одиниці: *VPN [Virtual Private Network] – віртуальна приватна мережа; IDS [Intrusion Detection System] – система виявлення вторгнень; IPS [Intrusion Prevention System] – система запобігання вторгненням; SIEM [Security Information and Event Management] – управління інформаційною безпекою та подіями; DDoS [Distributed Denial of Service] – розподілена атака типу «відмова в обслуговуванні».*

Абревіатури та акроніми займають важливе місце в терміносистемі кібербезпеки, оскільки виконують функцію економії мовних засобів та спрощують комунікацію серед фахівців, особливо при роботі з довгими багатокомпонентними термінами.

Прості абревіатури утворюються з перших літер слів у словосполученні: *VPN (Virtual Private Network – віртуальна приватна мережа) – технологія створення захищеного з'єднання через публічну мережу, IP (Internet Protocol – протокол Інтернету) – основний протокол передачі даних у мережі Інтернет, HTTP (HyperText Transfer Protocol – протокол передачі гіпертексту) – протокол для передачі веб-сторінок, DNS (Domain Name System – система доменних імен) – система перетворення доменних імен на IP-адреси.* Складні акроніми часто стають самостійними термінами, які вимовляються як окремі слова: *TLS (Transport Layer Security – протокол безпеки транспортного рівня) – криптографічний протокол для захисту даних при передачі, IDS/IPS (Intrusion Detection/Prevention System – система виявлення та запобігання вторгнень) – комплексне рішення для моніторингу та блокування підозрілої активності, SIEM (Security Information and Event Management – управління безпекою інформації та подій) – система збору, аналізу та управління інформацією про безпеку в реальному часі, APT (Advanced Persistent Threat – складна тривала загроза) – тип цілеспрямованої кібератаки, що характеризується тривалістю та складністю.*

Частка абревіатур у термінології кібербезпеки становить приблизно 8–10%, що значно вище, ніж у багатьох інших галузей. Це пояснюється динамічним характером розвитку галузі та постійною появою нових

технологій і концепцій, які потребують компактних позначень: *APT [Advanced Persistent Threat] – розвинена стійка загроза; MFA [Multi-Factor Authentication] – багатофакторна автентифікація; SOC [Security Operations Center] – центр моніторингу безпеки; CSIRT [Computer Security Incident Response Team] – група реагування на інциденти безпеки; PKI [Public Key Infrastructure] – інфраструктура відкритих ключів.*

Абревіатури в кібербезпеці забезпечують необхідну варіативність термінології, співвіщуючись з повними формами термінів і часто вживаючись паралельно з ними. Це дозволяє ефективно адаптувати мову до різних контекстів використання – від технічної документації до повсякденної професійної комунікації.

Варто звернути увагу на малу, але цікаву групу термінів-телескопізмів у кібербезпеці, які становлять приблизно 0,8% від загального обсягу термінології. Ці терміни утворюються шляхом поєднання частин різних слів, що дозволяє створювати компактні та зручні для використання форми: *Syslog* (від *system + logging*) – *система логування подій: The syslog server collects and stores security events from all network devices* [112]. – *Сервер системного логування збирає та зберігає події безпеки з усіх мережевих пристроїв* [103]. *Vishing* (від voice + phishing) – *голосовий фішинг: Vishing attacks use phone calls to trick victims into revealing sensitive information* [112]. – *Голосові фішингові атаки використовують телефонні дзвінки для обману жертв з метою отримання конфіденційної інформації* [105]. *Windump* (від Windows + dumping) – *утиліта для аналізу мережевого трафіку в Windows*: *Network analysts use windump to capture and examine packets on Windows systems* [112]. *Мережеві аналітики використовують Windump для захоплення та аналізу пакетів у системах Windows* [105]. *Smishing* (від SMS + phishing) – *фішинг через текстові повідомлення: Smishing campaigns often use urgent messages to prompt immediate action* [106]. – *Смішинг кампанії часто використовують екстрені повідомлення, щоб спонукати до негайних дій* [103]. *Cyborg* (від cybernetic + organism) – *концепція поєднання людського та машинного*

інтелекту: Cyborg security systems combine human intuition with AI capabilities [106]. – *Кібернетичні системи безпеки поєднують людську інтуїцію з можливостями штучного інтелекту* [103].

Ці телескопізми демонструють творчий підхід до термінотворення в кібербезпеці, де неологізми часто виникають у відповідь на нові виклики та технології. Незважаючи на свою нечисленність, вони відіграють важливу роль у професійній комунікації, забезпечуючи точність та ефективність передачі інформації.

Таким чином, за своїми структурними особливостями англомовні терміни кібербезпеки чітко розподіляються на терміни-прості слова, терміни-похідні слова, складні терміни, терміни-словосполучення та терміни-скорочення. Проведений аналіз демонструє, що прості терміни репрезентовані переважно іменниками та дієсловами, що відображає об'єктно-процесуальну природу понятттного апарату галузі.

Афіксація підтвердила свій статус одного з найпродуктивніших способів термінотворення, зокрема завдяки високій активності префіксів (anti-, cyber-, de-, mal-, re-), що дозволяють точно модифікувати семантику базових понять, та суфіксів (-er, -ing, -ity, -tion), що виражають агентивність, процесуальність та абстрактні характеристики. Словоскладання виявилося основним механізмом утворення складних термінів, що дозволяє створювати лаконічні та інформативно насичені одиниці для позначення комплексних явищ та технологій.

Найчисленнішою групою серед проаналізованих одиниць виявилися двокомпонентні терміни-словосполучення, переважно за моделлями N + N та Adj + N, що забезпечує структурну стійкість та семантичну прозорість термінів. Трикомпонентні та чотирикомпонентні словосполучення також є важливою складовою термінології, забезпечуючи точність при номінації складних концепцій. Окремої уваги заслуговує активне використання скорочень та акронімів, що є закономірною відповіддю на потребу в

оперативному та ефективному оперуванні технічними поняттями в умовах динамічного розвитку галузі.

У цілому, структурне різноманіття англомовної термінології кібербезпеки свідчить про її високий ступінь розвитку, системності та здатності адаптуватися до постійних змін у сфері інформаційної безпеки.

2.2. Семантичні особливості англомовних термінів кібербезпеки

Семантичний спосіб, що є одним з найдавніших механізмів формування термінології, відіграє важливу роль і в кібербезпеці. Він полягає у семантичній трансформації вже існуючих слів, які набувають спеціалізованих значень у контексті цифрової безпеки. Цей процес дозволяє швидко реагувати на потреби у нових термінах без необхідності створення абсолютно нових лексичних одиниць.

Процес формування термінології кібербезпеки є яскравим прикладом того, як мова динамічно реагує на виклики нового часу [17, с. 47]. Як було зазначено, він почався з адаптації загальновживаних слів, які набули спеціалізованих значень. Ця адаптація, однак, не була хаотичною; вона сформувала чітку семантичну структуру, де кожен термін існує у тісному зв'язку зі своїм загальномовним попередником і з іншими термінами в межах цієї сфери.

Зв'язок між загальномовним і спеціалізованим значенням є фундаментальним. Він ґрунтується на метафоричному переносі, що робить складні технічні поняття інтуїтивно зрозумілими. Наприклад, семантична зміна слова «*virus*», про яку йшлося в контексті технологічного прогресу, стала можливою саме через знаходження аналогії між біологічним збудником, що заражає організм, і шкідливим кодом, що заражає комп'ютерну систему. *The spread of misinformation online is like a digital* ***virus*** [103]. – *Поширення дезінформації в інтернеті схоже на цифровий* ***вірус*** **[107]**. *The analogy between a biological* ***virus*** *and a computer* ***virus*** *made the term*

easy to understand [106]. – *Аналогія між біологічним* ***вірусом*** *та комп'ютерним* ***вірусом*** *зробила цей термін легким для розуміння* [105]. Ця зв'язкова ланка – концепція «зараження та шкоди» – дозволяє терміну зберігати свою образність і легше засвоюватися, навіть коли його технічне значення суттєво ускладнилося.

Ця ж логіка поширюється і на еволюцію понять, таку як демонструє історія терміна «*hacker*». Його семантична трансформація від дослідника до злочинця та подальша диференціація на «етичного» та «чорного» хакера показує, що семантична структура не є статичною. Вона розгалужується, утворюючи гіпонімію (відношення «вид – рід»), де загальне поняття «хакер» набуває більш специфічних значень у залежності від контексту та мотивів діяльності. *The activities of a* ***black hat hacker*** *are illegal and motivated by personal gain or malice* [106]. – *Діяльність* ***хакера-злочинця («чорного капелюха»)*** *є незаконною та мотивована особистою вигодою або зловмисністю* [109]. *The company hired a* ***white hat hacker*** *to perform a penetration test and find vulnerabilities in their app* [106]. – *Компанія найняла* ***етичного хакера («білий капелюх»)****, щоб провести тестування на проникнення та знайти вразливості у своєму додатку* [109]. *A* ***grey hat hacker*** *found a critical flaw in the popular software and publicly disclosed it without the vendor's permission* [106]. – ***Хакер «сірий капелюх»*** *знайшов критичну ваду у популярному програмному забезпеченні та оприлюднив її без дозволу розробника* [109]. *The website was defaced by a* ***hacktivist*** *group protesting the new government policy* [106]. – *Веб-сайт був змінений (дефейсований) групою* ***хактивістів****, які протестували проти нової урядової політики* [109]. Таким чином, семантичні зміни, спричинені технологічним прогресом і еволюцією понять, безпосередньо формують ієрархічну та мережеву структуру термінології.

Отже, семантична структура термінів кібербезпеки може бути представлена як динамічна мережа. У її центрі знаходяться базові поняття, запозичені з загальної мови через метафору («*virus, wall, worm*). Від цього

центру відходять гілки більш спеціалізованих термінів, що уточнюють та диференціюють значення (*Trojan horse (or simply «Trojan*»**)** як окремий від вірусу тип загрози, *black hat hacker* як різновид хакера). *Unlike a virus, a* ***Trojan horse*** *cannot replicate itself; it relies on users downloading it thinking it is legitimate software* [106]. – *На відміну від вірусу, троянська програма не може самопоширюватися; вна покладається на користувачів, які завантажують її, вважаючи легітимним програмним забезпеченням* [109]. *A* ***black hat hacker*** *breached the company's database to steal customer credit card information* [106]. – ***Хакер-злочинець*** *(«чорний капелюх») зламав базу даних компанії, щоб викрасти інформацію про кредитні картки клієнтів* [109].

Кожен новий технологічний виклик або зміна в практиці породжують нові семантичні ланки в цій мережі, завжди зберігаючи, проте, зв'язок із вихідними поняттями, що забезпечує мовній системі як стабільність, так і гнучкість.

Попри прагнення термінології до однозначності, багато термінів у кібербезпеці мають складну семантичну структуру з кількома значеннями. Наприклад, термін «***Backdoor»*** *(«бекдор», «лазівка», «задні двері»)* може означати: 1. Програмно-реалізований механізм обходу автентифікації. 2. Уразливість у коді або конфігурації. 3. Законний інструмент для доступу. 4. Криптографічний механізм [102]. *The investigators found a* ***backdoor*** *in the server's operating system that allowed attackers to steal data unnoticed* [112]. – *Слідчі виявили* ***бекдор*** *(****лазівку****) в операційній системі сервера, який дозволяв нападникам непомітно викрадати дані* [104]. *The company claims the* ***backdoor*** *is only used for customer support, but security experts are concerned about its potential for abuse* [111]. – *Компанія стверджує, що ця* ***лазівка*** *використовується лише для підтримки клієнтів, але фахівці з безпеки стурбовані її потенційним зловживанням* [104]. *The government is pushing for a law that would require tech companies to install a* ***backdoor*** *in their encryption, a move criticized by privacy advocates* [111]. – *Уряд просує закон, який*

вимагатиме від технологічних компаній встановлювати ***бекдор*** *у своєму шифруванні, що критикується захисниками приватності* [104].

Цей приклад показує, що значення терміна визначається не лише технічною функцією, але й контекстом, намірами того, хто його створив чи використовує, та юридичним статусом.

У міру розвитку технологій семантичні зміни в кібербезпеці прискорюються. Термін ***«cloud»***, який спочатку позначав метеорологічне явище, тепер описує цілу галузь технологій хмарних обчислень. *Most companies now rely on the* ***cloud*** *for data storage and application hosting* [113]. – *Більшість компаній тепер покладаються на* ***хмару*** *для зберігання даних та хостингу додатків* [109]. Аналогічно, слово **«*blockchain*»** з концепції криптографічного ланцюжка перетворилося на термін, що охоплює цілий клас розподілених технологій. *The company uses* ***blockchain*** *to ensure transparency and security in its supply chain* [113]. – *Компанія використовує* ***блокчейн****, щоб забезпечити прозорість та безпеку у своєму ланцюжку поставок* [109].

Ця динаміка семантичних змін відображає швидкий розвиток галузі кібербезпеки та постійне збагачення її понятійного апарату. Семантичний спосіб термінотворення продовжує залишатися важливим інструментом адаптації мови до нових технологічних реалій.

Формування лексикона кібербезпеки є яскравим прикладом того, як мова адаптується до викликів нової, швидкозмінної реальности. Оскільки абстрактні цифрові явища потребували наочного опису, основним механізмом термінотворення стало метафоричне переосмислення слів із звичних для людини сфер досвіду. Ці метафори не тільки спрощують розуміння складних концепцій, але й формують певну ментальну модель цифрового світу. Метафоричні терміни в кібербезпеці можна чітко структурувати за групами, виходячи з джерела їх походження.

1. Антропоморфні метафори: цифровий організм та його захист.

Однією з найпотужніших моделей є проекція будови та функцій людського тіла на інформаційні системи. За її допомогою кіберпростір уявляється як складний організм, що потребує захисту.

- Імунна система: Центральне місце тут займає поняття **«*firewall*» (*брандмауер*)**. Ця «вогнестіна» функціонує як захисний бар'єр імунної системи, який фільтрує вхідний та вихідний мережевий трафік, блокуючи небезпечні «загрози». Так само, як організм відрізняє власні клітини від чужорідних, брандмауер розрізняє легітимний та шкідливий трафік. *The company's **firewall** blocked all unauthorized incoming traffic, just like the immune system fights off pathogens* [111]. – *Корпоративний **брандмауер** заблокував весь несанкційований вхідний трафік, так само як імунна система бореться з патогенами* [104].
- Приховані органи та шляхи: Термін **«*backdoor*» (*бекдор*)** – «*задні двері*» або «*лазівка*» – вказує на прихований механізм обходу стандартних процедур безпеки. Це аналог прихованого ходу в будівлі, який дозволяє зловмиснику уникнути «парадного входу» (системи автентифікації). *The attackers installed a **backdoor** on the server, allowing them to bypass security and steal data unnoticed* [106]. – *Нападники встановили **бекдор** на сервер, що дозволило їм обійти безпеку та викрадати дані непомітно* [108].
- Частини тіла: Інші терміни також використовують цю модель. «*head*» (*голова*) може позначати головний сервер у кластері (*head node*), а «*bone*» (*кістки*) – базову архітектуру мережі (*backbone* – *магістраль*). «*finger*» (*палець*) дав назву старому протоколу для отримання інформації про користувачів системи (*finger protocol*). *A DDoS attack targeted the network's **backbone**, causing widespread internet outages* [106]. – *DDoS-атака націлилася на мережеву **магістраль**, спричинивши масове відключення інтернету* [107].

2. Топографічні та архітектурні метафори: простір, шляхи та споруди

Ця група концептуалізує цифровий світ як фізичний ландшафт із конкретними об’єктами, шляхами сполучення та територіями.

- Атмосферні явища: Наймасштабнішою метафорою останніх років стало слово «*cloud*» (*хмара*). Воно ефективно описує модель обчислень, де ресурси (сховище, потужність) децентралізовані, динамічні та доступні з будь-якої точки, подібно до атмосферної хмари. *We migrated our entire infrastructure to the **cloud** to improve scalability and reduce costs* [106]. – *Ми перенесли всю нашу інфраструктуру в **хмару**, щоб покращити масштабованість і знизити витрати* [109].
- Інфраструктурні об'єкти: *«gateway» (шлюз*) виконує роль контрольно-пропускного пункту між різними мережами. «*port» (порт*) є логічним аналогом морського порту – специфічною адресою, куди «причалюють» пакети даних. «*tunnel*» (*тунель*) описує зашифроване з'єднання, яке створює захищений «коридор» всередині публічної мережі. *The secure **gateway** encrypts all data passing between the local network and the internet* [106]. – *Захищений **шлюз** шифрує всі дані, що передаються між локальною мережею та інтернетом* [109].
- Локації: Термін «*sandbox*» (*песочниця*) означає ізольоване середовище для безпечного виконання підозрілих програм, де вони, немов дитина в пісочниці, не можуть зашкодити основній системі. *The antivirus runs suspicious files in a secure **sandbox** to analyze their behavior without risking the main system* [106]. – *Антивірус запускає підозрілі файли в захищеній **пісочниці**, щоб проаналізувати їхню поведінку без ризику для основної системи* [109].

3. Зооморфні та біологічні метафори: віруси, черв'яки та трояни

Ця, мабуть, найвідоміша група термінів, запозичила образи з біологічного світу для опису цифрових загроз, що «живуть» і «розмножуються».

- Біологічні аналогії: Слово «*virus*» (*вірус*) зазнало глибокої семантичної трансформації. Як і його біологічний прототип, комп'ютерний вірус для розмноження потребує «клітини-господаря» (файлу або програми), здатний «заражати» системи та завдавати шкоди. «*worm*» (*черв'як*) є більш

автономним – він самопоширюється по мережах, не потребуючи файлу-носія, подібно до паразита. *The email attachment contained a **virus** that infected hundreds of computers within the organization* [106]. – *Вкладений у лист файл містив **вірус**, який заразив сотні комп'ютерів в організації* [109]. *The **worm** propagated rapidly through the network, exploiting a vulnerability in the operating system* [106]. – ***Черв'як** швидко поширився мережею, використовуючи вразливість в операційній системі* [109].

- Міфологічні та поведінкові аналоги**: «***Trojan horse***»** (*Троянський кінь*) – це досконала метафора для програми, що приховує зловмисний функціонал під виглядом корисного або цікавого вмісту, обманом спонукаючи користувача її встановити. «*Unicorn*» / «*Одноріг*» – у венчурному капіталі так називають стартап з оцінкою понад $1 млрд. У кібербезпеці цей термін іноді використовують для позначення рідкісного, дуже цінного та важкого для виявлення шкідливого програмного забезпечення або вразливості. *The cybersecurity team discovered a true **unicorn** – a piece of malware so sophisticated and targeted that it had been operating undetected for years* [106]. – *Команда кібербезпеки виявила справжнього **однорога** – шкідливе ПЗ настільки витончене та цілеспрямоване, що працювало непомічено протягом років* [109]. Ці приклади показують, що кібербезпека продовжує запозичувати потужні образи з міфології та опису поведінки, щоб надати абстрактним технічним поняттям більш яскравого та зрозумілого змісту.

- Фауна як джерело образів: «*spider*» (*павук*) або «*crawler*» (*краулер*) – це програма, яка «обповзає» веб-сайти для індексації їхнього вмісту. «*rabbit*» (*кролик*) може означати шкідливий процес, який швидко «розмножується», споживаючи всі обчислювальні ресурси системи. *Search engines use **web spiders** (or **crawlers**) to systematically browse and index the content of billions of websites, mapping the entire internet* [112]. – Пошукові системи використовують ***веб-павуків*** (або ***краулери**), щоб систематично переглядати та індексувати вміст мільярдів веб-сайтів, створюючи карту*

всього інтернету [108]. *A* ***rabbit*** *process is a type of malware that rapidly replicates itself, consuming all available system resources until the machine crashes or becomes unusable* [110]. *– Процес-**кролик** – це тип шкідливого ПЗ, який швидко самовідтворюється, споживаючи всі доступні системні ресурси, поки машина не аварійно завершить роботу або не стане непридатною до використання* [108].

4. Військові та транспортні метафори: поле битви в кіберпросторі

Оскільки кібербезпека часто є сферою конфлікту, військова лексика стала природним джерелом для термінів.

- Бойові дії: Поняття «*attack*» (*атака*), «*threat*» (*загроза*), «*intrusion*» (*вторгнення*) та «*defense*» (*захист*) безпосередньо запозичені з військової термінології. *The Security Operations Center detected an* ***intrusion*** *into the network at 3:00 AM and immediately launched the incident response protocol* [110]. *– Центр оперативної безпеки виявив **проникнення** в мережу о 3:00 ночі та негайно запустив протокол реагування на інцидент* [108]. *A strong* ***defense*** *in depth strategy employs multiple layers of security controls to protect sensitive data* [106]. *– Стратегія глибокого **захисту** передбачає використання багатьох шарів заходів безпеки для захисту конфіденційних даних* [109].
- Озброєння та тактика: «*payload*» (*корисне навантаження*) – це частина шкідливого коду, що безпосередньо виконує зловмисну дію (наприклад, шифрування файлів або викрадення даних), аналогічно боєголовці. «*zero-day attack*» (*атака нульового дня*) – це використання раніше невідомої вразливості, коли у захисників немає часу («нуль днів») на розробку патчу. *The hackers used a* ***zero-day attack*** *to breach the system before the vendor had a chance to release a patch* [106]. *– Хакери використали **атаку нульового дня**, щоб зламати систему до того, як розробник встиг випустити латку* [109].
- Транспорт: «*drive-by download*» (*завантаження на проїзді*) – це тип атаки, коли шкідливий код завантажується на пристрій користувача без

його відома під час простого відвідування веб-сторінки, подібно до нападу з автомобіля, що проїжджає повз. *The compromised website initiated a **drive-by download** that installed malware simply by visiting the page* [106]. – *Скомпрометований веб-сайт ініціював **завантаження на проїзді**, яке встановило шкідливе ПЗ просто під час відвідування сторінки* [109].

Таким чином, метафоричне термінотворення в кібербезпеці є системним процесом, що ґрунтується на потужних аналогіях із фізичного світу. Основними галузями-джерелами виступають біологія (організм, віруси), архітектура (стіни, шлюзи, хмара), зоологія (тварини, комахи) та військова справа (атаки, навантаження). Ці метафори не лише роблять складні технологічні концепції доступними для сприйняття, але й активно формують наше розуміння кіберпростору як середовища, де існують загрози, що «живуть» і «атакують», і де необхідно будувати «укріплення» для власного «цифрового організму».

Англійська термінологія кібербезпеки постійно еволюціонує та поповнюється новими поняттями, що безпосередньо відображає стрімкий розвиток цієї галузі. Формування нових термінів нерозривно пов'язане з семантичним процесом метонімії – явища, коли назва одного об'єкта переноситься на інший на основі реальної або уявної суміжності між ними.

Метонімія як мовний механізм ґрунтується на встановленні асоціативних зв'язків між різними об'єктами або явищами, що сприймаються як суміжні за просторовим, часовим або функціональним принципом. Результатом цього процесу є семантична трансформація слова, коли воно набуває нового спеціалізованого значення, зберігаючи при цьому зв'язок із вихідним поняттям. На відміну від метафори, яка ґрунтується на схожості, метонімія встановлює зв'язок за принципом сусідства або функціональної взаємодії. У кібербезпеці цей механізм виявився надзвичайно плідним, що дозволило створити цілу низку інтуїтивно зрозумілих і функціонально точних термінів.

1. Відношення «ціле-частина». Ця модель демонструє, як назва цілого об'єкта або його ключової характеристики поширюється на його структурний компонент у цифровому середовищі. Термін «*cache*» (*схованка*) є класичним прикладом. Спочатку це слово позначало приховане місце для зберігання цінностей. У контексті обчислювальної техніки воно набуло значення «*буферної пам'яті процесора*» – швидкої, але обмеженої за обсягом області, де тимчасово зберігаються найбільш затребувані дані. Таким чином, концепція «схованки» була метонімічно перенесена з фізичного світу на логічний компонент архітектури процесора.

Слово «*core*» (*серцевина, ядро*) історично використовувалося для позначення центральної, найважливішої частини чогось. У кібербезпеці та комп'ютерних науках воно стало позначати «*центральний процесор*» або «*основну частину операційної системи*». Це відображає розуміння процесора як «серця» комп'ютера, а ядра системи — як його фундаментальної основи.

Поняття «*kernel*» (*ядро*) пройшло аналогічний шлях. Як ядро горіха є його суттєвою, центральною частиною, так і «*ядро операційної системи*» є її основним компонентом, що відповідає за взаємодію апаратного забезпечення та програмного забезпечення. Тут ми спостерігаємо метонімічне перенесення з біологічного об'єкта на абстрактну програмну структуру.

2. Відношення «процес-результат». Ця модель ілюструє, як дія починає позначати як сам процес, так і його результат або інструмент. Слово «*scan*» (*оглядати, сканувати*) спочатку описувало уважний візуальний огляд. У кібербезпеці воно набуло значення «*процедури автоматичної перевірки системи*» на наявність загроз, вразливостей або певних даних. Таким чином, назва дії («сканувати») стала іменем для цілого технологічного процесу та його результату – звіту про сканування.

Термін «*patch*» (*латка*) вийшов з лексикона ремесел, де означав шматок матеріалу для закриття діри. У програмному забезпеченні він став означати «програмне виправлення» – невеликий фрагмент коду, призначений

для «залатання» знайденої вразливості. Назва об'єкта, що усуває дефект, була перенесена на сам інструмент усунення.

Поняття «*backup*» (*резерв, запас*) історично вказувало на щось, що зберігається на випадок потреби. Зараз це слово означає як «*процес резервного копіювання даних*», так і сам «*результат цього процесу*» – резервну копію. Тут ми бачимо, як стан («наявність резерву») трансформувався в назву дії та її продукту.

3. Перенесення за функціональною ознакою. Ця група термінів виникла через спільність функцій між об'єктами з різних сфер. Слово «*shield» (щит) з давніх-давен було символом захисту у фізичному бою. У кіберпросторі воно стало означати «програмний захист від кібератак»*. Функція щита – блокувати удари – була метонімічно перенесена на функцію програмного засобу, що блокує мережеві атаки, віруси та шкідливий трафік.

Термін *«gate»* (*ворота, хвіртка*) традиційно позначав точку входу та виходу. У мережевій інфраструктурі він набув значення «*мережевого шлюзу*» – пристрою або програми, що виконує аналогічну роль, маршрутизуючи трафік між різними мережами. Концепція контрольованого проходу була успадкована технологією.

Поняття «*filter*» (*фільтр*) прийшло з фізики та хімії, де означало пристрій для відділення одних речовин від інших. У контексті кібербезпеки воно трансформувалося в «*механізм відбору мережевого трафіку*» на основі заданих правил. Функція відсіювання непотрібного залишилася незмінною, але була застосована до цифрових даних.

Особливу категорію в лексиконі кібербезпеки становлять терміни, що виникли шляхом метонімічного перенесення власних назв – імен, прізвищ, назв компаній або географічних точок. Цей процес дозволяє створити виразні та економні поняття, які часто несуть у собі цілу історію про походження, функцію або автора певної технології, загрози чи методу.

1. Терміни, що походять від імені автора або компанії-розробника. Ця група є однією з найчисленніших. Назва технології або стандарту часто

успадковує ім'я того, хто її створив чи впровадив. «*Charlie-tagging*» (*Чарлі-мітка*): Цей термін походить від імені Чарлі Міллера (Charlie Miller), відомого дослідника безпеки. Він означає техніку «міткування» мережевих пакетів для відстеження їхнього шляху через складну мережеву інфраструктуру під час тестування на проникнення. Вираз *We used Charlie-tagging to map the internal network* [112]. – *Ми використали Чарлі-міткування, щоб змапити внутрішню мережу* означає застосування цієї конкретної методики, названої на честь її піонера [106].

«bcrypt» (хешування): алгоритм шифрування паролів *bcrypt* отримав свою назву від *Blowfish cipher* (*шифр Blowfish*) та адаптації для цілей хешування. Фраза **«***Passwords should be stored using bcrypt***»** [110]. – *«Паролі мають зберігатися за допомогою bcrypt*») [109] прямо вказує на використання цього конкретного, надійного алгоритму, назва якого стала стандартом у галузі.

2. Терміни, що походять від географічних назв або назв організацією Назви міст, регіонів або урядових установ часто стають на позначення кібератак, зловмисних груп або програм. *«WannaCry»:* назва глобальної атаки-вимагача 2017 року. Хоча це не власна назва в класичному розумінні, вона функціонує як ідентифікатор конкретної події. Речення *The WannaCry ransomware attack affected hundreds of thousands of computers worldwide* [111]. – *Атака вірусом-вимагачем WannaCry вразила сотні тисяч комп'ютерів по всьому світу* [109] однозначно ідентифікує цю конкретну кіберзпідію серед інших.

«APT29 (Cozy Bear)»: APT (Advanced Persistent Threat) – це загроза, а ідентифікація «*APT29*» або її псевдонім «*Cozy Bear*» («*Косолапий ведмідь*») – це власна назва, що позначає конкретну групу кібершпигунів, яку розвідслужби пов'язують з росією [104]. Фраза *The attack was attributed to APT29 – Атаку було приписано APT29* [107] відразу ж дає зрозуміти досвідченим фахівцям, хто ймовірно стоїть за атакою, які її методи та мотивація.

3. Терміни, що походять від назв продуктів або протоколів. Комерційні назви технологій часто стають загальновживаними термінами для опису певних класів продуктів або функцій. **«*Kerberos*»:** Цей мережевий протокол автентифікації отримав свою назву від імені ***Цербера*** **(*Kerberos*)** – триголового пса з грецької міфології, що охороняв вихід з підземного царства. Назва символізує надійний захист доступу. Речення *The corporate network uses Kerberos for single sign-on* [103]. – *Корпоративна мережа використовує Kerberos для єдиного* входу [110]» описує використання саме цього протоколу, назва якого стала синонімом безпечної автентифікації в мережах на базі Windows.

«Сервер Apache»: Веб-сервер Apache отримав свою назву не від індіанського племені, а від «a patchy server» («латкатий сервер»), оскільки спочатку був набором виправлень до іншого сервера. Однак зараз ця назва є власною для одного з найпопулярніших веб-серверів у світі. Фраза *The website is hosted on an Apache server* [106]. – *Веб-сайт розміщений на сервері Apache* [103]є стандартним способом вказати тип програмного забезпечення, що використовується.

Використання власних назв у термінології кібербезпеки – це не просто зручність, а потужний інструмент категоризації та комунікації. Вони дозволяють одним словом передати складний набір атрибутів: авторство, геополітичний контекст, технічні особливості або історичний прецедент. Такі терміни, як *WannaCry, APT29* чи *Kerberos,* стають міцними ланками в колективній пам'яті галузі, формуючи її унікальний, багатошаровий і постійно еволюціонуючий словник.

Отже, метонімія в кібербезпеці наочно демонструє глибокий взаємозв'язок між мовою, мисленням і технічним прогресом. Вона дозволяє переосмислити звичні поняття з фізичного світу та застосувати їх для опису складних цифрових явищ. Цей механізм не лише сприяє створенню функціонально точної термінології, але й робить її інтуїтивно зрозумілою як

для фахівців, так і для широкого загалу, формуючи міст між технологічною складнощі та людським сприйняттям.

Англійська термінологія кібербезпеки є яскравим прикладом динамічної лінгвістичної системи, що постійно еволюціонує під впливом технологічного прогресу. Як зазначає український лінгвіст І. Асмукович [2, с. 12], процес термінологізації передбачає семантичне перетворення загальновживаних слів у термінологічну систему через спеціалізацію або перенос значення. Це добре ілюструє трансформація слова «*worm*» (*черв'як*) – від біологічного поняття до технічного терміна «*самопоширювана шкідлива програма*». У реченні *The computer* ***worm*** *rapidly propagated through the network, exploiting vulnerabilities in the operating system* [112] цей термін уже не має нічого спільного з зоологією, а виконує чітку номінативну функцію у професійному контексті.

Процес детермінологізації, який академік Н. Бідненко визначає як перехід терміна зі спеціальної сфери у загальновживану, чітко простежується на прикладі слова «*phishing*» [6, с. 76]. Спочатку це був вузькоспеціалізований термін для позначення певного типу кібершахрайства, але сьогодні ми спостерігаємо його вживання у повсякденному мовленні: *My bank warned me about a new phishing attempt via email* [113]. Тут термін втрачає частину своєї технічної точності, але стає зрозумілим широкому загалу.

Як відзначають українські дослідники на кшталт С. Самійленко [58, с. 31] та Ю. А. Зацного [29], транстермінологізація (ретермінологізація) стала особливо продуктивним механізмом для кібербезпеки. Запозичення медичного терміна «*virus*» для позначення комп'ютерних загроз створило потужну образну аналогію. У реченні *The antivirus software detected a dangerous virus in the system memory* [113] ми бачимо повне переосмислення поняття, що дозволяє ефективно комунікувати складні технічні концепції.

Ці семантичні процеси відбуваються під впливом комплексу факторів. Згідно з концепцією О. Селіванової, інтеграція наук стала ключовим драйвером транстермінологізації [60, с. 217]. Військове поняття «*attack*» набуло нового життя в кіберпросторі, що добре видно у реченні T*he company suffered a DDoS* ***attack*** *that disrupted its online services* [111]. Тут термін зберігає свою агресивну конотацію, але набуває специфічного технологічного наповнення.

Лінгвістична економія, про яку пише Л. Білозерська [7. с. 42], проявляється в адаптації слова «*firewall*». Від первісного значення «*протипожежна стіна*» термін пройшов шлях до технічного поняття *The firewall blocked unauthorized access attempts to the corporate network* [112], а потім – до детермінологізованого вживання в маркетингових контекстах.

Таким чином, термінологія кібербезпеки уособлює динамічний характер сучасної наукової термінології, де постійно відбувається взаємодія між спеціалізованими та загальновживаними пластами лексики. Ця динаміка, як свідчать дослідження українських лінгвістів, не лише відображає технологічний прогрес, але й демонструє фундаментальні властивості мови як живої, адаптивної системи, здатної ефективно реагувати на виклики сучасного інформаційного суспільства.

Проведений аналіз демонструє чітку ієрархію семантичних процесів у формуванні термінологічного апарату кібербезпеки за критерієм їх частотності. Статистичні дані свідчать, що термінологізація (65%) є домінуючим механізмом, що обумовлено потребою швидкого номінування нових понять у стрімко розвиваючійся галузі. Цей процес дозволяє ефективно заповнювати лексичні лакуни шляхом адаптації звичних мовних одиниць, що значно прискорює комунікацію між фахівцями.

Детермінологізація (25%) посідає друге місце за частотою, відображаючи потужний вплив кібербезпеки на сучасну культуру та повсякденне життя. Цей показник свідчить про активне проникнення

спеціалізованих понять у масову свідомість, що є індикатором зростання обізнаності суспільства про кіберзагрози.

Найменш поширеною, але концептуально важливою є транстермінологізація (10%), яка забезпечує міждисциплінарність термінологічної системи. Цей процес підкреслює інтегративний характер кібербезпеки як науки, що розвивається на стику різних галузей знань. Це співвідношення вказує на динамічний баланс між професійною комунікацією, популяризацією знань та міжгалузевим синтезом. Така структура семантичних процесів забезпечує як точність професійної термінології, так і її доступність для широкого загалу, що є вирішальним чинником ефективної боротьби з кіберзагрозами в сучасному цифровому суспільстві.

Як було зазначено, механізми семантичного переосмислення, такі як метонімія, є основним джерелом наповнення словника кібербезпеки. Однак, щоб ця термінологія могла ефективно функціонувати, вона організовується в чітку систему. На основі проведеного аналізу англомовну терміносистему кібербезпеки можна структурувати навколо кількох основних тематичних груп, які відображають ключові аспекти цієї предметної галузі [85, с. 46]. Ці групи не існують ізольовано; вони тісно переплітаються, а їхні терміни часто походять від спільних семантичних моделей, розглянутих раніше.

Група 1: Загрози та шкідливе програмне забезпечення. Передусім виділяється тематична група, яка об'єднує терміни на позначення різноманітних видів кіберзагроз та атак. До цієї категорії належать: загальні категорії: *malicious software,cyber threat,network intrusion;* специфічні типи шкідливого ПЗ: *network worm, compromised computer, crypto-ransomware, cybercrime toolset;* методи проведення атак: *session hijacking, dictionary-based attack, packet fragmentation attack; m*ехніки соціальної інженерії: *credential harvesting, voice phishing, SMS-based fraud, physical reconnaissance*. Таким чином, ця група демонструє різноманітність та багатоаспектність сучасних кіберзагроз.

Група 2: Методи та засоби захисту. Ця категорія охоплює технології та механізми протидії загрозам: криптографічні методи: *data encryption, cryptographic protocol, block encryption cipher; c*истеми контролю доступу: *network security barrier, access management service, role-based permissions;* інструменти моніторингу: *behavioral analysis, traffic inspection, anomaly detection;* організаційні заходи: *system fortification, security updates, business resilience strategy.* Отже, ця група охоплює як технічні, так і організаційні аспекти забезпечення безпеки.

Група 3: Мережеві технології та компоненти інфраструктури. Терміни цієї групи описують базові компоненти мережевої архітектури: комунікаційні протоколи: *web transfer protocol, network management protocol, path selection protocol;* мережеві пристрої: *network gateway, secured host, packet forwarding device;* мережеві параметри: *data transfer capacity, network identifier,connection endpoint.* Таким чином, ця група забезпечує термінологічний апарат для опису технічної інфраструктури кіберпростору.

Група 4: Процеси забезпечення безпеки та управління. До цієї категорії належать терміни, пов'язані з операційною діяльністю: аналітичні процедури: *security assessment, vulnerability scanning, cryptographic analysis;* технічні процеси: *interface-based transmission, automated vulnerability discovery;* операційні процедури: *connection management, data stewardship, performance metric.* Отже, ця група відображає процесуальний аспект діяльності у сфері кібербезпеки.

Група 5: Властивості та характеристики систем безпеки. Ця група включає якісні характеристики систем захисту: фундаментальні принципи: *system accessibility, data protection, transaction integrity;* технічні атрибути: *biological identification, digital identity, cryptographic collision;* стани систем: *executable content, defensive security team, cryptographic credential.* Таким чином, ця група забезпечує термінологію для опису якісних параметрів систем безпеки.

Група 6: Структурні елементи та компоненти даних. Завершує класифікацію група термінів для опису базових структур даних: одиниці інформації: *binary digit, data unit, transmission frame;* структурні компоненти: *data header, system configuration database, network path segment;* організаційні поняття: *data segmentation, network layout, memory boundary violation.* Отже, ця група забезпечує базову термінологію для опису структури даних та систем.

Становлення термінологічного апарату кібербезпеки відбувалося переважно шляхом семантичної адаптації загальновживаної лексики, що було зумовлено необхідністю номінації нових технологічних концепцій. Основними механізмами цього процесу виступили семантичні трансформації, переосмислення та спеціалізація значень. Таким чином, семантичний спосіб термінотворення є основним механізмом формування лексикона галузі, що проявляється через метафоричне та метонімічне переосмислення загальновживаних слів. Це забезпечує швидке заповнення термінологічних лакун у умовах стрімкого технологічного прогресу. Структура термінології має ієрархічно-мережевий характер, де центральні поняття, запозичені з фізичного світу, утворюють ядро системи з гілками спеціалізованих значень. Ця структура поєднує стабільність з гнучкістю, дозволяючи адаптуватися до нових викликів.

Частотність семантичних процесів розподіляється як: термінологізація (65%), детермінологізація (25%) та транстермінологізація (10%), що відображає потреби у номінуванні, популяризації та міждисциплінарному синтезі. Метафоричні моделі систематизовані за джерелом походження на антропоморфні, топографічні, зооморфні та військові, формуючи ментальну модель кіберпростору. Метонімічні процеси реалізуються через відношення «ціле-частина», «процес-результат» та функціональну суміжність. Організація термінології в шість тематичних груп забезпечує системну класифікацію та демонструє комплексність галузі.

Таким чином, семантичні особливості термінології кібербезпеки відображають здатність мови адаптивно реагувати на виклики інформаційного суспільства та забезпечувати ефективну комунікацію в умовах технологічного розвитку.

РОЗДІЛ 3
ПЕРЕКЛАД АНГЛОМОВНОЇ ТЕРМІНОЛОГІЇ КІБЕРБЕЗПЕКИ

3.1. Переклад простих та складних англомовних термінів кібербезпеки

Значний масив англомовної термінології кібербезпеки представлений односкладовими та простими термінами, що дозволяє використовувати метод термінологічної еквівалентності як основний перекладацький підхід. Такі лексичні одиниці, які дослідники називають «базовими одиницями спеціалізованого перекладу» [49, с. 30], не становлять значних труднощів при трансляції українською мовою. До цієї категорії належать: *admin – адмін; format – формат; firewall – брандмауер; hacker – хакер; malware – шкідливе програмне забезпечення; password – пароль; backup – резервна копія; encryption – шифрування; phishing – фішинг.* Поняття адекватного відповідника слід розуміти не як спеціальний вид відповідності, а як оптимальний варіант передачі лексичної одиниці з урахуванням контекстуальних умов. Адекватними можуть вважатися як постійні еквівалентні аналоги, так і варіантні відповідники. Наприклад, прямими еквівалентами перекладаються терміни *firewall, encryption: The company installed a new* ***firewall*** *to protect its network* [112]. – *Компанія встановила новий* ***брандмауер*** *для захисту своєї мережі* [106]. *Data* ***encryption*** *ensures confidentiality of information* [111]. – *Шифрування даних забезпечує конфіденційність інформації* [108]. Варіантними відповідниками перекладаються терміни *security, access,* бо вони можуть мати кілька перекладів залежно від контексту: ***security*** – 1) безпека; 2) захист; 3) охорона; ***access*** – 1) доступ; 2) право доступу; 3) доступність; наприклад, у значенні загального стану безпеки – «*безпека*» [102]: *Information* ***security*** *is our priorit* [103]. – ***Безпека*** *інформації є нашим пріоритетом* [107]. У значенні заходів захисту – «*захист*»: *Network* ***security*** *measures were implemented* [103]. –

Впроваджені заходи ***захисту*** *мережі* [107]. Особливу групу становлять похідні терміни, утворені шляхом афіксації, переклад яких здійснюється через відповідні україномовні термінологічні еквіваленти: *scanning – сканування, encoding – кодування, brute-forcing – перебір. Regular vulnerability* ***scanning*** *helps identify threats* [112]. *– Регулярне* ***сканування*** *на вразливості допомагає виявляти загрози* [107]. *Data* ***encoding*** *prevents unauthorized access* [103]. *–* ***Кодування*** *даних запобігає несанкціонованому доступу* [107].

Еквівалентний переклад передбачає використання постійних, контекстно-незалежних відповідників між лексичними одиницями різних мов. Терміни, що мають стабільні еквіваленти в мові перекладу, виступають ключовими одиницями тексту, які дозволяють розкрити значення інших понять та визначити специфіку тексту.

Основне завдання перекладача полягає у пошуку та відборі відповідних лексичних одиниць, оптимальних мовних форм, здатних точно відтворити вихідні поняття з урахуванням загальноприйнятих термінологічних стандартів. Для цього необхідно не лише знайти відповідний еквівалент рідною мовою, але й коректно визначити межі його семантичного поля в конкретному професійному контексті. Наприклад, термін **«***patch***»** може перекладатися по-різному: у значенні «оновлення безпеки» – «*латка*»: *Install the latest security* ***patch*** [110]. *– Встановіть останню безпекову* ***латку*** [109]. У значенні процесу – *«виправлення»*: *Software* ***patching*** *is essential* [103]. *–* ***Виправлення*** *програмного забезпечення є необхідним* [109].

У сфері кібербезпеки перекладачі широко використовують метод транскодування, який за класифікацією В. Карабана [31, с. 125] включає чотири основні типи:

Транскрипція – передавання звукової форми терміна мовою перекладу: *phishing – фішинг, bitcoin – біткоїн, , hacker – хакер, cookie – кукі. The company reported a phishing attack on its employees* [106]. *– Компанія повідомила про фішингову атаку на своїх співробітників* [109]. *Bitcoin*

transactions require secure storage [106]. – *Транзакції біткоїна потребують безпечного зберігання* [109].

Транслітерація – відтворення літерного складу слова: *server – сервер, router – роутер; format – формат; plugin – пагін; driver –драйвер; token – токен; admin – адмін. The system* ***admin*** *quickly responded to the security incident* [110]. – *Системний* ***адмін*** *швидко відреагував на інцидент безпеки* [109]. *We need to restart the Wi-Fi* ***router*** *to fix the connection issue* [110]. – *Нам потрібно перезавантажити Wi-Fi* ***роутер****, щоб усунути проблему зі з'єднанням* [109]. *Please save the document in PDF* ***format*** [106]. – *Будь ласка, збережіть документ у PDF* ***форматі*** [109]. *This browser* ***plugin*** *blocks annoying advertisements* [110]. – *Цей браузер ний* ***пагін*** *блокує набридливу рекламу* [109].

Адаптивне транскодування – поєднання передавання інформації з адаптацією до фонетичних і граматичних норм мови перекладу: *encoding – кодування; scanning – сканування; cracking – крякінг; spoofing – спуфінг; hashing – хешування. Cracking software is illegal and poses a significant security risk* [106]. – ***Крякінг*** *програмного забезпечення є незаконним і становить значний ризик для безпеки* [105]. *The attacker used IP address* ***spoofing*** *to hide their real location* [106]. – *Зловмисник використав* ***спуфінг*** *IP-адреси, щоб приховати своє справжнє місцезнаходження* [105]. ***Hashing*** *passwords is a fundamental practice for protecting user data* [106]. – ***Хешування*** *паролів є фундаментальною практикою для захисту даних користувачів* [105].

Змішане транскодування – поєднання транскрипції з елементами транслітерації: *cryptocurrency – криптовалюта; cyberattack – кібератака; ransomware – рансомвер; backdoor – бекдор; honeypot – ханіпот. The company's website is currently under a massive* ***cyberattack*** [114]. – *Веб-сайт компанії зараз під масованою* ***кібератакою*** [109]. *The hospital's network was infected with* ***ransomware****, encrypting all patient files* [114]. – *Мережа лікарні була заражена* ***рансомвером****, який зашифрував усі файли пацієнтів* [104]. *Security experts set up a* ***honeypot*** *to study the tactics of cybercriminals* [113]. –

Фахівці з безпеки створили ***ханіпот****, щоб вивчати тактику кіберзлочинців* [107].

Важливо враховувати, що використання цього методу потребує попередньої перевірки наявності вже існуючих термінологічних аналогів у мові перекладу. Інакше може виникнути проблема дублювання термінів, що призводить до семантичної неоднозначності та порушення цілісності термінологічної системи кібербезпеки. Наприклад: *vulnerability – вразливість/уразливість; threat – загроза/ризик; breach – порушення/проникнення; access – доступ/право доступу.*

Це підтверджує необхідність стандартизації термінології та розробки єдиних підходів до перекладу професійної лексики у сфері кібербезпеки для забезпечення точної та однозначної комунікації між фахівцями.

Одним із ключових інструментів перекладу англомовних термінів кібербезпеки є описовий переклад. Цей метод полягає у передачі значення спеціалізованого поняття через розгорнуте пояснення його сутності. Наприклад: *zero-day – вразливість у програмному забезпеченні, про яку не відомо розробнику та для якої ще не існує заплатки; sandboxing – технологія ізоляції підозрілих програм у безпечному середовищі для аналізу їхньої поведінки*; *ransomware – шкідливе програма, що шифрує дані та вимагає викуп; spyware – програма, що таємно збирає інформацію про користувача. The hospital's computers were infected with* ***ransomware*** [111]. *– Комп'ютери лікарні були заражені* ***програмою-вимагачем*** [107]. *The* ***spyware*** *was secretly recording all keystrokes* [110]. *–* ***Шпигунська програма*** *таємно записувала всі натискання клавіш* [108].

При транскодуванні термінів описовий переклад часто використовується як додаткове пояснення у дужках: *phishing – фішинг* (*вид кібершахрайства, що полягає у виманюванні конфіденційних даних через підроблені веб-сторінки*); *botnet – ботнет* (*мережа заражених комп'ютерів, керована злочинцем для проведення кібератак*). Для термінів, що вже міцно

увійшли у вжиток, описовий переклад може не використовуватися: *firewall – брандмауер; malware – шкідливе програмне забезпечення.*

До описового перекладу висуваються певні вимоги: він має точно відтворювати суть поняття, бути лаконічним та мати просту синтаксичну структуру. Основною проблемою для перекладачів є необхідність глибокого розуміння предметної галузі для коректного розкриття змісту поняття через описову конструкцію.

Важливо враховувати, що багато термінів кібербезпеки мають контекстно-залежне значення [30, с. 178]. Наприклад, термін «*payload*» у загальному вживанні означає «*корисне навантаження*», але в контексті кібербезпеки він перекладається як «*шкідливий вміст*» – *частина зловмисного коду, що безпосередньо виконує цільову зловмисну дію.*

Важливим прийомом перекладу однокомпонентних термінів кібербезпеки є **смисловий розвиток (модуляція)** – метод контекстуальної заміни, при якому вихідне слово замінюється одиницею мови перекладу, значення якої є логічним розвитком значення оригіналу. *Analysts launched the malware in an* ***isolated environment,where it could not harm real systems*** [112]. *Security experts deployed a decoy* ***system, which mimicked a working server to study adversary tactics*** [106].

По-перше, такий підхід забезпечує точне розуміння технології, оскільки розкриває її функціональне призначення. Користувач одразу розуміє, що «*firewall* – захисний екран» служить для захисту, а не просто є технічним бар'єром. По-друге, він усуває непотрібні образні асоціації, які часто виникають при буквальному перекладі метафор. Наприклад, «*sandbox» «ізольоване середовище*» не викликає асоціацій з дитячою пісочницею, що дозволяє сприймати термін серйозно. По-третє, смисловий розвиток робить термін зрозумілим для широкого кола користувачів, включаючи неспеціалістів. Такі поняття як «*honeypot» – «система-приманка*» інтуїтивно зрозумілі навіть тим, хто не є експертом у кібербезпеці. Крім того, цей підхід сприяє кращій інтеграції термінів в україномовний технічний дискурс,

оскільки вони природно вписуються в професійну комунікацію без необхідності додаткових пояснень.

Таким чином, використання смислового розвитку особливо ефективне для термінів, заснованих на метафорах, оскільки дозволяє передати технічну суть поняття, а не лише його образне втілення в мові-джерелі, що значно підвищує точність і зрозумілість професійної комунікації.

Важливим інструментом перекладу в галузі кібербезпеки є **контекстуальна заміна** – прийом, коли оригінальний термін замінюється словом або словосполученням мови перекладу, яке не є прямим словниковим еквівалентом, але точніше передає зміст у конкретному контексті. Наприклад, термін *mousejacking* має значення «мишочне захоплення», але у реченні *Using a cheap radio dongle, the attacker performed* ***a mousejacking attack*** *to take control of the computer* [114]. *– За допомогою* ***перехоплення сигналу бездротової миші*** *зловмисник отримав контроль над комп'ютером* [109], переклад цього терміна не відповідає дійсності, тому найточнішим і найзрозумілішим способом передати це поняття в українському реченні буде відмовитися від терміна-кальки на користь контекстуальної заміни та описового перекладу, які розкриває суть. Таким чином, оригінальне речення набуває точного і зрозумілого вигляду українською. У цьому випадку контекстуальна заміна виявилася найефективнішою стратегією. Вона пояснює суть: читач одразу розуміє, який саме механізм було використано (перехоплення радіосигналу), а не лише кінцевий результат. Цей переклад зрозумілий як технічним спеціалістам, так і широкому загалу. Розглянемо ще речення, де краще застосувати контекстуальну заміну при перекладі*: After the online dispute, he became a victim of* ***doxing****, with his home address and phone number leaked online* [111] та *Police found a* ***skimming*** *device installed on the ATM* [113]. Прямий переклад *doxing* та *skimming* відбувається за допомогою транскрипції *доксінг* та *скімінг,* але ждя широкої аудиторії, яка не є технічно підкованою, слова «доксінг» та «*скімінг»* залишається порожнім звуком. Вони не розкривають суті дії. У новинній статті або матеріалі, розрахованому

на загальну публіку, важливо, щоб читач зрозумів зміст негайно, без необхідності пошуку значення незрозумілого терміну. Тому, замість транскрипції ми описуємо саму дію. *Doxing* – це *публічне розголошення чи публікація особистої та конфіденційної інформації про людину (такої як адреса, паспортні дані, листування тощо) без її згоди, з метою залякування чи шкідження,* а *skimming* – це *зчитування, копіювання або крадіжка даних з магнітної смуги платіжної картки за допомогою спеціального пристрою, який встановлюється на банкомат або платіжний термінал*. Таким чином, оригінальні речення набувають зрозумілого вигляду українською тільки за допомогою контекстуальної заміни, а саме *Після конфлікту в інтернеті він став жертвою* ***публікації конфіденційної інформації****, коли його домашня адреса та номер телефону з'явилися в мережі* [107]. *На банкоматі встановили* ***пристрій для зчитування даних платіжних карток*** [105]. В обох випадках контекстуальна заміна відкидає незрозумілий технічний жаргон на користь ясного опису загрози. Це робить інформацію доступною для всіх і безпосередньо виконує практичну функцію – попередження та інформування. Таким чином, використання контекстуальної заміни сприяє ефективнішій комунікації між фахівцями з кібербезпеки та кінцевими користувачами, підвищує обізнаність про кіберзагрози та сприяє кращому засвоєнню складних технічних понять українською мовою.

Як було зазначено, формування термінології кібербезпеки значною мірою відбувається шляхом термінологізації загальновживаних слів. У цьому процесі, коли між терміном і нетерміном існує постійна взаємодія, відбувається конкретизація значення слова, тобто звуження його семантичного поля. Відповідно до класифікації В. Карабана, **конкретизація** являє собою «заміну широкого значення одиниці вихідної мови більш конкретним значенням мови перекладу» [31, с. 300].

Ілюструючи це явище, можна звернутися до лексем *mouse* (*миша*) та *firewall* (*вогнестіна*). У загальновживаному контексті вони позначають, відповідно, гризуна та захисну стіну, що запобігає поширенню пожежі.

Однак у термінологічному полі кібербезпеки їх значення звужується і конкретизується: *mouse* стає *пристроєм введення*, а *firewall – програмним або апаратним бар'єром для мережевого трафіку*. *The IT department is investigating how a hacker gained control of the user's* ***mouse*** *and cursor* [106]. – *Відділ IT розслідує, як хакер отримав контроль над* ***пристроєм введення (мишею)*** *та курсором користувача* [109]. *Our network* ***firewall*** *blocked all unauthorized incoming traffic from that IP address* [106]. – *Мережевий* ***програмний або апаратний бар'єр для мережевого трафіку (фаєрвол)*** *заблокував весь несанкціонований вхідний трафік з цієї IP-адреси* [109]. Таким чином, у спеціалізованих текстах відбувається контекстна конкретизація значень цих лексем, що безпосередньо вказує на їхню належність до термінологічної системи кібербезпеки. Реалізація такої трансформації вимагає від перекладача не лише лінгвістичної компетенції, але й глибоких знань у предметній галузі.

Паралельно із термінологізацією відбувається й зворотний процес – детермінологізація. Він нейтралізує визначальну функцію терміна в загальному вживанні та відіграє ключову роль у популяризації знань, підвищуючи загальний рівень обізнаності суспільства у важливих технологічних сферах. Значення детермінологізованих одиниць, як правило, розширюється, що свідчить про **генералізацію** їхнього змісту. Під генералізацією розуміють «передавання значення широкого абстрактного поняття вихідної мови без його повного уточнення» [31, с. 129].

Яскравим прикладом генералізації може слугувати термін *phishing*. Спеціалістам відомо, що існують різноманітні його типи, такі як *spear-phishing* (*цілеспрямований фішинг*) чи *whaling* (*фішинг на керівників*). *The security team identified a* ***spear-phishing*** *campaign targeting our financial officers with emails mimicking the CEO* [113]. – *Команда безпеки виявила кампанію* ***цілеспрямованого фішингу****, націлену на наших фінансових директорів, з листами, що імітують гендиректора* [104]. Однак у ЗМІ або побутовій розмові це слово часто вживається в узагальненому значенні для

позначення будь-якої спроби виманити конфіденційні дані шляхом обману. *My grandmother received an email saying her bank account was locked, but it was just* ***phishing*** [106]. – *Моя бабуся отримала листа з інформацією про блокування банківського рахунку, але це був просто* ***фішинг*** [108]. Таким чином, технічно точний термін втрачає свою специфікацію і починає використовуватися як широке поняття, доступне для масової аудиторії. Наведемо ще приклади речень, де відбувається переклад за допомогою генералізації: *The* ***SQL injection*** *attack allowed the attacker to extract the entire user database* [110]. – *Атака* ***SQL-ін'єкцією*** *дозволила зловмиснику витягнути всю базу даних користувачів* [108]. *Someone* ***hacked*** *my social media account and posted strange messages* [110]. – *Хтось* ***зламав*** *мою сторінку в соцмережі і опублікував дивні повідомлення* [108].

Проаналізувавши вищенаведені приклади, можна дійти висновку, що основним засобом передачі англомовних термінів кібербезпеки, як простих, так і складних, є пошук адекватних термінологічних відповідників у мові перекладу (59% випадків). Крім того, переклад цих одиниць нерідко здійснюється шляхом різних видів транскодування – транскрипції та транслітерації (15%). Серед ключових перекладацьких прийомів вирізняються використання словникового еквівалента (14%) та описового перекладу (12%), які часто застосовуються в комплексі.

Передача подібних термінів у більшості випадків вимагає залучення лексико-семантичних трансформацій. На нашу думку, саме конкретизація виступає однією з найбільш продуктивних трансформацій під час перекладу англомовної термінології кібербезпеки. Це пов’язано з тим, що багато термінів цієї галузі утворені від слів загальної лексики, які в технічному контексті набувають значно звуженого та спеціалізованого значення. Вміння виокремити це конкретне значення та знайти його точний відповідник у мові перекладу є запорукою адекватного та зрозумілого перекладу.

3.2. Переклад англомовних термінів-словосполучень кібербезпеки

Сучасна англомовна термінологія кібербезпеки характеризується стрімким зростанням частки багатокомпонентних термінів-словосполучень. Ця тенденція обумовлена ускладненням термінологічного апарату галузі, що зумовлено постійним розвитком технологій, появою нових концепцій на стику з іншими науковими дисциплінами, а також складністю архітектури інформаційних систем і мережевих протоколів.

Переклад таких складноструктурних одиниць часто вимагає структурних трансформацій, що реалізуються через низку спеціальних перекладацьких прийомів. До них належать: калькування, описовий переклад, модуляція, граматичні заміни, контекстуальна заміна, цілісна перебудова речення, а також використання конструкцій з родовим відмінком або прийменниками [35, с. 420].

Як показує аналіз, домінуючою категорією в термінологічному масиві кібербезпеки є двокомпонентні терміни-словосполучення. Типовими прикладами виступають: *security policy – політика безпеки*; *firewall rules – правила фаєрволу*; *attack vector – вектор атаки*; *data breach – витік даних*; *malware analysis – аналіз шкідливого ПЗ*; *zero-day vulnerability – вразливість нульового дня*. У цих структурах перший компонент (*security, firewall, attack, data, malware, zero-day*) виконує функцію визначення по відношенню до головного компонента (*policy, rules, vector, breach, analysis, vulnerability*). Таким чином, переклад шляхом пошуку лексичного еквівалента залишається найпоширенішим підходом.

Значний масив двокомпонентних термінів, таких як *network traffic – мережевий трафік*; *application layer – аплікаційний рівень*; *computer virus – комп'ютерний вірус*; *cryptographic key – криптографічний ключ*; *access control – контроль доступу*, передається українською мовою шляхом **калькування**. Цей метод передбачає дослівне відтворення структури

вихідного терміна за допомогою відповідних лексичних одиниць мови перекладу [67, с. 284].

В галузі кібербезпеки значна частина багатокомпонентних термінів відсутня в спеціалізованих словниках, що зумовлено їхньою об'ємністю та практично необмеженими можливостями комбінування компонентів. Перекладач стикається з труднощами передачі значення таких словосполучень з кількох причин: по-перше, через кількість компонентів у терміні; по-друге, через специфічний зв'язок між цими компонентами; по-третє, через багатозначність окремих складових терміна. Тому вирішальне значення має визначення способів адекватної передачі значення таких словосполучень та критеріїв для їх перекладу.

Для успішного перекладу складного терміна кібербезпеки перекладачу необхідно послідовно виконати три етапи: ідентифікувати окремі компоненти терміна, знайти відповідний еквівалент для кожного з них з урахуванням галузевих особливостей та контексту, та грамотно об'єднати їх засобами рідної мови. Наприклад, багатокомпонентні словосполучення на кшталт *real-time malware behavior analysis – аналіз поведінки шкідливого ПЗ в реальному часі* можуть бути трансформовані у більш компактні структури шляхом виділення ключового терміна *malware behavior analysis* – аналіз поведінки шкідливого ПЗ.

Переклад подібних термінів найчастіше здійснюється методом калькування, коли «кожна значуща частина оригіналу перекладається буквально і займає в перекладі таке ж місце, як і в оригіналі» [32, с. 101]. Цей метод застосовується лише за умови структурної відповідності між вихідним терміном і перекладом, як у прикладах: *network security protocol – мережевий протокол безпеки*; *cloud access security broker – брокер безпеки доступу до хмари*; *intrusion detection system – система виявлення вторгнень*; *endpoint protection platform – платформа захисту кінцевих точок*; *zero-trust architecture – архітектура нульової довіри*.

Найчастішою перекладацькою трансформацією при роботі з багатокомпонентними термінами кібербезпеки є **зміна порядку слів** у словосполученні: *advanced threat protection – захист від розвинених загроз; cloud security posture management* – управління станом безпеки хмари; *zero trust network access* – мережевий доступ з нульовою довірою. Це пов'язано з фундаментальними відмінностями в синтаксичних структурах англійської та української мов. Англійська мова, будучи аналітичною, схильна до використання жорсткого порядку слів, тоді як українська, як синтетична мова, дозволяє більшу гнучкість у побудові фраз. Наприклад, термін «*data loss prevention*» перекладається як «*запобігання втраті даних*», де ми спостерігаємо не лише зміну порядку слів, але й трансформацію граматичних зв'язків між компонентами. ***Data loss prevention*** *technologies are essential for modern enterprises* [111]. – *Технології* ***запобігання втраті даних*** *є необхідними для сучасних підприємств* [109].

Аналогічно, «*cloud security posture management*» набуває форми «*управління станом безпеки хмари*», що демонструє необхідність адаптації терміна до української мовної картини світу. *Effective* ***cloud security posture management*** *is critical for maintaining compliance and preventing data breaches in cloud environments* [106]. – *Ефективне* ***управління станом безпеки хмари*** *є критично важливим для підтримання відповідності вимогам та запобігання витоку даних у хмарних середовищах* [108]. У цьому прикладі ми спостерігаємо одразу кілька перекладацьких трансформацій, а не тільки перестановку компонентів також і грамматичну заміну: слово *posture* (*становище, позиція, стан*) перекладається не дослівно, а за допомогою більш абстрактного і природнього для української мови поняття «*стан*». Це дозволяє уникнути незграбних кальок типу «*управління позицією безпеки*». Також можна спостерігати і структурну адаптацію, тому що вся конструкція перефразовується для того, щоб вона звучала природно і була зрозумілою для українського фахівця, точно передаючи суть процесу – саме *управління* поточним *станом* безпеки хмарної інфраструктури. Цей підхід підкреслює,

що переклад технічних термінів – це не механічна заміна слів, а творчий процес адаптації поняття до іншої мовної та професійної культури.

Компресія виявляється особливо ефективною для довгих складних термінів, де можна зберегти семантичне навантаження при зменшенні кількості компонентів. Ця трансформація демонструє зрілість української термінологічної системи, яка здатна створювати компактні та інформативні відповідники [84, с. 201]. Яскравим прикладом служить термін «*blockchain-based distributed ledger technology*», який українською звучить як «*технологія розподіленого реєстру*». *The company adopted* ***blockchain-based distributed ledger technology*** [110]. – *Компанія запровадила* ***технологію розподіленого реєстру*** **[109]**. Тут ми бачимо виключення компонента «*blockchain-based*», що не зменшує точності терміна, але робить його більш зручним для вживання. Подібним чином «*encrypted data transmission protocol*» трансформується в «*протокол шифрованого передавання*», де відбувається не лише скорочення, але й граматична адаптація.

Зворотний процес – **декомпресія** – стає необхідним, коли стислий англійський термін потребує додаткового пояснення для коректного розуміння українською. Це особливо характерно для нових концепцій, що ще не мають усталених коротких відповідників. Наприклад, термін «*sandboxing*» перекладається як «*ізоляція підозрілих процесів у безпечному середовищі*», що дозволяє точно передати суть технології: ***Sandboxing*** *helps analyze suspicious files safely* [112]. – ***Ізоляція підозрілих процесів у безпечному середовищі*** *допомагає аналізувати небезпечні файли* [109]. Аналогічно, «*tokenization*» потребує розгорнутого перекладу «заміна конфіденційних даних на унікальні ідентифікатори», оскільки пряма транскрипція «токенізація» була б недостатньо зрозумілою для широкої аудиторії. ***Tokenization*** *replaces sensitive data with unique identifiers* [106]. – ***Заміна конфіденційних даних на унікальні ідентифікатори*** *захищає інформацію* [108].

Морфологічні трансформації демонструють глибоку адаптацію термінів до української мовної системи. **Заміна частини мови** дозволяє

створити природно звучачі конструкції, що органічно вписуються в український мовний контекст. Термін «*threat hunting*» перекладається як «*полювання на загрози*», де дієприкметникова конструкція замінюється іменниковою, більш характерною для української термінології. «*Compliance reporting*» набуває форми «*звітність про відповідність*», що демонструє трансформацію іменникової конструкції в дієслівну, властиву українській мові. *Threat hunting requires specialized skills and tools* [106]. – *Полювання на загрози вимагає спеціалізованих навичок та інструментів* [108]. *Compliance reporting must be completed quarterly* [113]. – *Звітність про відповідність має подаватися щоквартально* [109].

Використання **прийменникових конструкцієй** відображає тенденцію до більш точного визначення взаємозв'язків між поняттями. Це дозволяє створити структурно складніші, але семантично більш точні терміни. «*Policy of least privilege*» перекладається як «*політика найменших привілеїв*», де прийменник «*of*» замінюється відповідним відмінком. «*Security by design*» стає «*безпека через проектування*», що точно передає причинно-наслідковий зв'язок між компонентами терміна: *Policy of least privilege minimizes potential damage* [106]. – *Політика найменших привілеїв мінімізує потенційну шкоду* [109]. *Security by design integrates protection into development process* [106]. – *Безпека через проектування інтегрує захист у процес розробки* [109].

Переклад акронімів та назв нових технологій вимагає особливого підходу, що поєднує **транскрипцію з описовими елементами**. «*Extended Detection and Response (XDR)*» отримує переклад «*розширене виявлення та реагування*», де зберігається оригінальний акронім, але додається його розшифровка. «*Secure Access Service Edge (SASE)*» трансформується в «*безпечний периферійний доступ як послуга*», що демонструє поєднання семантичного перекладу з пояснювальними елементами. *SASE architecture combines networking and security functions* [114]. – *Архітектура безпечного периферійного доступу як послуги (SASE) поєднує мережеві та захищені функції* [108].

Сучасна українська термінологія кібербезпеки знаходиться в стані активного формування, що проявляється в **паралельному використанні різних варіантів перекладу**. Це відображає пошук оптимального балансу між міжнародною стандартизацією та лінгвістичною автономією [30, с. 181]. Термін «zero trust» може перекладатися як «*нульова довіра*», «*відсутність довіри*» або зберігати оригінальну форму «*зеро-траст*» – кожен варіант має свої переваги та сфери вживання.

На практиці перекладачі часто поєднують кілька видів трансформацій одночасно. Наприклад, при перекладі «*Cloud-Native Application Protection Platform (CNAPP)*» використовується і компресія («*platform*» – «*платформа*»), і перестановка компонентів, і заміна частин мови. Такий комплексний підхід дозволяє створити термін, що відповідає вимогам точності, стислості та природності звучання. *CNAPP solutions integrate multiple security capabilities* [111]. – *Рішення платформи захисту рідних хмарних додатків (CNAPP) інтегрують численні функції безпеки* [109].

У ході аналізу також було виявлено приклади перекладу, що ґрунтуються на **методі лексичної заміни** українським словом-відповідником. Цей підхід дозволяє зробити термін інтуїтивно зрозумілим без втрати його суті [67, с. 286]. Серед таких прикладів: password *cracker* – «*взламувач паролів*»; *packet sniffer* – «*аналізатор мережевих пакетів*»; *computer worm* –«*комп'ютерний черв'як*». *The forensic team used a powerful* ***password cracker*** *to gain access to the encrypted files* [106]. – *Команда судових експертів використала потужний* ***засіб для взлому паролів****, щоб отримати доступ до зашифрованих файлів* [105]. *To diagnose the network issue, the administrator used a* ***packet sniffer*** *to analyze the data flow* [106]. – *Щоб діагностувати мережеву проблему, адміністратор використав* ***аналізатор мережевих пакетів*** *для перевірки потоку даних* [107].

Проаналізуємо практичні підходи до перекладу складних термінів-словосполучень у контексті кібербезпеки. Сучасна термінологічна система цієї галузі характеризується стрімким зростанням кількості

багатокомпонентних одиниць, що потребує застосування різноманітних перекладацьких стратегій.

При перекладі речення *The security team discovered a zero-day vulnerability in the widely used software library* [110]. – *Команда з безпеки виявила zero-day вразливість у широко вживаній бібліотеці програмного забезпечення* [109] було застосовано калькування та комбіновані методи перекладу. Термін *zero-day vulnerability* демонструє ефективність калькування у поєднанні з транслітерацією. Компонент *zero-day* передається як *zero-day* (т*ранслітерація*), а *vulnerability* перекладається як *вразливість*, утворюючи стабільний термін *zero-day вразливість*. *Many financial institutions are now implementing* ***blockchain technology*** *for secure transactions* [112]. – *Багато фінансових установ зараз впроваджують* ***блокчейн технологію*** *для безпечних транзакцій* [108]. Подібним чином *blockchain technology* перетворюється на *блокчейн технологія*, де перший компонент транслітерується, а другий – калькується.

Спостерігається значна кількість випадків заміни частин мови для адаптації до української граматики. Наприклад, у реченні *The* ***intrusion detection system*** *automatically blocked the malicious IP address* [106]. – ***Система виявлення вторгнень*** *автоматично заблокувала шкідливу IP-адресу* [105] «*intrusion detection system*» перекладається як *система виявлення вторгнень*, де відбувається трансформація іменникової конструкції у відмінкову форму. Термін «*data encryption standard*»набуває форми *стандарт шифрування даних*, що демонструє зміну синтаксичних зв'язків між компонентами. *All government agencies must comply with the new* ***data encryption standard*** [106]. – *Усі державні установи повинні дотримуватися нового* ***стандарту шифрування даних*** [105].

Структурні перетворення можна спостерігати у реченні *We are evaluating a* ***cloud access security broker*** *to enhance our cloud security posture* [113]. –*Ми оцінюємо* ***брокер безпеки доступу до хмари*** *для покращення нашого стану хмарної безпеки* [109].Для терміна *cloud access security broker*

застосовується комплексний підхід: перестановка компонентів (*cloud access – доступу до хмари*), морфологічна трансформація (*securityи – безпеки*) та додавання прийменникової конструкції, що у результаті дає *брокер безпеки доступу до хмари.*

Експлікація та описовий переклад спостерігаєть у реченні *Sandboxing is particularly effective for analyzing previously unknown malware samples* [106]. – *Ізоляція підозрілих процесів у безпечному середовищі є особливо ефективною для аналізу раніше невідомих зразків шкідливого ПЗ* [109]. У випадках, коли пряме калькування неможливе або створює незрозумілі конструкції, використовується описовий переклад. Наприклад, *sandboxing* перекладається як *ізоляція підозрілих процесів у безпечному середовищі*. Такий підхід особливо важливий для нових концепцій, що ще не мають усталених відповідників.

Отже, цей аналіз демонструє, що переклад термінології кібербезпеки є динамічним процесом, що поєднує традиційні перекладацькі методики з інноваційними підходами, адаптованими до специфіки галузі. Розвиток української термінологічної системи відбувається шляхом пошуку оптимального балансу між міжнародними стандартами та національною мовною традицією.

Специфіка термінології кібербезпеки полягає в її міждисциплінарному характері, поєднанні технічних понять з правовими, управлінськими та соціальними аспектами. Крім того, швидкість появи нових термінів часто випереджає процес їх стандартизації в українській мові. Це зумовлює необхідсть розробки чіткого алгоритму дій, який би забезпечував адекватну передачу значення термінів з урахуванням динаміки розвитку галузі.

Запропонований нижче алгоритм перекладу ґрунтується на аналізі сучасної практики перекладу термінології кібербезпеки та враховує особливості української мовної системи. Він спрямований на забезпечення точності, однозначності та природності звучання перекладу, а також на адаптацію міжнародних понять до українського термінологічного простору.

Алгоритм включає чотири послідовні етапи, кожен з яких є необхідним для досягнення якісного перекладацького рішення. Від уважного виконання цих кроків залежить не лише точність передачі терміна, але й його подальше сприйняття та вживання україномовною аудиторією.

1. Ідентифікація ключових компонентів. Перший етап передбачає структурний аналіз терміна для виявлення його основної логічної структури. Перекладач має визначити головне, найважливіше слово в терміні, яке виражає основне поняття, а також усі модифікатори, що уточнюють або звужують його значення. Цей аналіз можна порівняти з розбором речення, де ми визначаємо головні та другорядні члени.

2. Аналіз семантичних зв'язків. На цьому етапі необхідно з'ясувати логічні відношення між окремими компонентами терміна. Перекладач аналізує, як саме пов'язані між собою окремі частини терміна, який сенс вони створюють разом. Без такого аналізу переклад може бути механічним і не відображати справжньої суті поняття.

3. Вибір стратегії перекладу. Після повного розуміння структури та семантики терміна перекладач обирає оптимальне поєднання методів перекладу. Це може бути калькування, транскрипція, описовий переклад або їх комбінація. Вибір стратегії залежить від усталених норм, контексту та цільової аудиторії.

4. Адаптація до мовних норм. Фінальний етап передбачає приведення перекладу у відповідність до граматичних, синтаксичних і стилістичних норм української мови. Це включає правильне використання відмінків, прийменників, узгодження роду, числа та відмінків. На цьому етапі перекладач також враховує вже існуючі усталені відповідники та професійні стандарти.

Фінальний етап передбачає приведення перекладу у відповідність до граматичних, синтаксичних і стилістичних норм української мови, що включає правильне використання відмінків, прийменників, узгодження роду, числа та відмінків. На цьому етапі перекладач також враховує вже існуючі

усталені відповідники та професійні стандарти, що є особливо важливим через контекстуальну залежність перекладу. Важливо розуміти, що один і той самий термін може отримувати різні варіанти перекладу залежно від галузевої специфіки та цільової аудиторії, оскільки технічний переклад орієнтований на точність і відповідність професійним стандартам, тоді як переклад для менеджменту чи широкої аудиторії робить акцент на зрозумілості та функціональному призначенні технології.

3.3. Труднощі перекладу скорочень англомовної термінології кібернетики

Як уже зазначалося, англомовна термінологічна система кібербезпеки характеризується значною концентрацією різноманітних абревіатур. Це явище зумовлене складністю та громіздкістю багатокомпонентних термінів, потребою у мовній економії та прагненням до оперативності комунікації. На основі нових технологічних понять формуються скорочені одиниці, які завдяки своїй зручності активно вживаються та утворюють нові пласти спеціалізованої лексики [37, с. 65]. Однак саме при перекладі таких скорочень у текстах з кібербезпеки виникають значні труднощі.

Переклад термінів кібербезпеки становить особливу складність для фахівців, оскільки вимагає не лише високого рівня володіння мовою, але й глибоких спеціальних знань у галузі інформаційної безпеки. Особливу увагу слід приділяти перекладу скорочених одиниць, оскільки саме в них приховані значні перекладацькі виклики, що часто призводять до помилок. Механізми утворення абревіатур у кібербезпеці відрізняються гнучкістю та різноманіттям. Необмежена тенденція до створення нових термінів та відповідних абревіатур, їхнє активне дублювання та варіативність – все це значно ускладнює процес перекладу та може створювати труднощі навіть для досвідчених перекладачів.

У сучасній перекладацькій практиці використовують такі основні способи передачі абревіатур: описовий переклад із застосуванням транслітерації, транскрипції, коментаря, запозичення в оригінальній формі, використання абревіатур, що вже існують у мові перекладу, а також застосування повних термінів-відповідників [40, с. 32]. Важливо зазначити, що в реальній практиці часто поєднують кілька з цих методів одночасно. Таким чином, актуальним завданням є аналіз оптимальних шляхів передачі англомовних абревіатур галузі кібербезпеки українською мовою з урахуванням сучасних вимог до якості перекладу.

У процесі перекладу термінології кібербезпеки активно використовується метод прямого запозичення, який передбачає перенесення скорочень у оригінальній формі з подальшим поясненням українською мовою. Наприклад: *APT* (*Advanced Persistent Threat*) – *атака типу APT*, *EDR* (*Endpoint Detection and Response*) – *система EDR*. Цей підхід також застосовується для передачі назв компаній, продуктів і технологій: *CrowdStrike Falcon, McAfee MVISION, Palo Alto Networks*.

Найпоширенішими типами абревіатур у кібербезпеці є акроніми, що утворені з трикомпонентних словосполучень: *SIEM* (*Security Information and Event Management*) – *управління інформацією безпеки та подіями*, IAM (*Identity and Access Management*) – *управління ідентичністю та доступом*. Транслітерація як самостійний метод перекладу є малопродуктивною і зазвичай використовується лише для термінів, що не мають усталених відповідників. При першому вживанні транслітерованої абревіатури варто додавати розшифровку: *The* ***SIEM*** system provides centralized security monitoring [110]. – *Система* ***SIEM*** *(Security Information and Event Management) забезпечує централізований моніторинг безпеки* [108].

Для широкої аудиторії доцільно поєднувати транслітерацію з описовим перекладом: *The* ***NGFW*** *provides deep traffic inspection* [106]. – ***NGFW*** *(фаєрвол нового покоління) забезпечує глибинну перевірку трафіку* [104].

У технічній документації можна використовувати чисту транслітерацію: *For integration, use the **REST API*** [106]. – *Для інтеграції використовуйте **REST API*** [109]. Транслітерація залишається важливим інструментом у перекладі термінології кібербезпеки, особливо для термінів, що мають міжнародне визнання та стандартизоване вживання.

Часткове запозичення знаходить широке застосування при перекладі складних багатокомпонентних термінів: *NIST* (National Institute of Standards and Technology) – *NIST* (Національний інститут стандартів і технологій), *MITRE ATT&CK – матриця MITRE ATT&CK*. Цей спосіб дозволяє зберегти міжнародне впізнання терміна, одночасно надаючи українськомовному читачеві зрозуміле пояснення.

Транскрипція оригінальної форми використовується переважно для назв компаній, продуктів та технологій, що не мають аналогів в українській мові: *WannaCry – ВаннаКрай, Stuxnet – Стукснет*. Особливістю кібербезпеки є активне використання акронімів, що утворені за принципом словотвору: *CISA* (*Cybersecurity and Infrastructure Security Agency*) вимовляється як єдине слово, а не окремі літери.

Слід зазначити, що в українському термінологічному просторі кібербезпеки спостерігається тенденція до поєднання різних методів перекладу. Наприклад, абревіатура *XDR* (*Extended Detection and Response*) може передаватися як *XDR* (*розширене виявлення та реагування*), де поєднується пряме запозичення з описовим перекладом. Такий підхід дозволяє зберегти міжнародне стандартизоване позначення технології, одночасно роблячи її зрозумілою для української аудиторії.

Одним із найпоширеніших методів є передача абревіатури шляхом повного розшифрування та перекладу. Цей підхід застосовується, коли в українській мові відсутнє відповідне скорочення: *APT (Advanced Persistent Threat) – цілеспрямована тривала загроза; C&C (Command and Control) – сервер керування та контролю; DLP (Data Loss Prevention) – запобігання втраті даних; NAC (Network Access Control) – контроль доступу до мережі*.

За наявності в українській мові усталених скорочень, що побудовані за аналогічною моделлю, перекладачі віддають перевагу саме їм, тобто використовують українські абревіатури-відповідники: *IT (Information Technology) – IT (інформаційні технології); OS (Operating System) – ОС (операційна система), VPN (Virtual Private Network) – VPN (віртуальна приватна мережа).*

У випадках, коли в українській мові відсутній прямий еквівалент, застосовується описовий метод перекладу: *PII* (*Personally Identifiable Information*) *– особиста інформація, що ідентифікує користувача; SOC (Security Operations Center) – центр моніторингу та реагування на інциденти безпеки; IoCs (Indicators of Compromise) – індикатори компрометації системи.*

Коли в оригіналі абревіатура вживається неодноразово після повного розшифрування, перекладач може створити відповідне скорочення українською мовою: *CISA* (Cybersecurity and Infrastructure Security Agency) – *Агентство з кібербезпеки та захисту інфраструктури – АКЗІ; NIST (National Institute of Standards and Technology) – Національний інститут стандартів і технологій – НІСТ.*

У більшості випадків перекладачі відходять від дослівного перекладу, щоб врахувати норми української мови та повніше передати зміст поняття [30, с. 185]: *BYOD (Bring Your Own Device) – використання особистих пристроїв для роботи; ZTA (Zero Trust Architecture) – архітектура нульової довіри; MFA (Multi-Factor Authentication) – багатофакторна автентифікація.*

Важливо зазначити, що вибір методу перекладу абревіатур у кібербезпеці залежить від контексту, цільової аудиторії та ступеня усталеності терміна в українській мові. Для міжнародно стандартизованих термінів часто зберігають оригінальну абревіатуру з наступним розшифруванням українською мовою, що забезпечує баланс між міжнародним сприйняттям та зрозумілістю для україномовного читача.

При перекладі абревіатур у галузі кібербезпеки важливо враховувати явище розширеної омонімії. Характерною особливістю є те, що чим коротшою є абревіатура, тим вища ймовірність омонімії – коли різні поняття мають однакову літерну форму при повній відсутності мотивації між цими одиницями. Абревіатура *APT* може означати: ***Advanced Persistent Threat*** *– цілеспрямована тривала загроза (кібербезпека); Automated Penetration Testing – автоматизоване тестування на проникнення (тестування безпеки); Application Performance Testing – тестування продуктивності додатків (розробка ПЗ).* Абревіатура SOC має кілька значень: *Security Operations Center – центр моніторингу безпеки (кібербезпека); System on Chip – система на чіпі (апаратне забезпечення); Service Organization Control-контроль сервісних організацій (аудит).*

Внутрішньогалузева омонімія проявляється, коли в межах кібербезпеки одна абревіатура позначає різні поняття: *IOC – Indicators of Compromise (індикатори компрометації); IOC – Infrastructure Operations Center (центр операцій інфраструктури).*

Міжгалузева омонімія виникає, коли абревіатура з кібербезпеки має інші значення в суміжних галузях: *IDS –Intrusion Detection System (система виявлення вторгнень)* – кібербезпека; *IDS – Integrated Development System (інтегрована система розробки)* – програмування; *IDS – Intelligent Document Solution (рішення для роботи з документами)* – управління даними.

Єдиним ефективним інструментом для подолання цієї проблеми є контекст. Саме контекст дозволяє перекладачеві коректно визначити значення абревіатури та підібрати відповідний варіант перекладу. Для запобігання непорозумінням рекомендується при першому використанні абревіатури в тексті надавати її повне розшифрування та переклад.

Ця особливість термінології кібербезпеки вимагає від перекладача не лише мовної компетенції, але й глибокого розуміння предметної області та здатності аналізувати технічний контекст, в якому вживається абревіатура.

Для передачі ініціальних скорочень з англійської мови у випадках, коли відсутні усталені відповідники, застосовується метод створення нових українських абревіатур, що ґрунтується на закономірностях словотвору мови перекладу. Цей процес передбачає послідовне виконання двох ключових етапів, спрямованих на точну передачу термінологічного змісту.

На першому етапі перекладач проводить детальне розшифрування оригінальної абревіатури, що передбачає ретельне визначення вихідної групи англійських слів, які утворюють дану абревіатуру. Цей процес вимагає глибокого аналізу семантичної структури терміна та його функціонального призначення в контексті кібербезпеки.

Другий етап передбачає пошук семантичних корелятів – спеціалізованих мовних одиниць, що знаходяться у взаємозумовлених відносинах і здатні найбільш точно передати сутнісний зміст терміна засобами української мови. Під корелятами в цьому випадку розуміють члени мовних пар або цілих рядів, що перебувають у стійких співвідносних зв'язках і забезпечують адекватну передачу спеціалізованого значення.

Для реалізації описаного методу необхідно застосовувати чіткий алгоритм дій, який забезпечує системний підхід до розшифрування абревіатур. Цей алгоритм дозволяє стандартизувати процес перекладу та уникнути можливих семантичних помилок. Він формувався на основі аналізу практики перекладу спеціалізованих термінів у галузі кібербезпеки та враховує особливості роботи з абревіатурами, що відсутні в словниках.

Перший крок алгоритму передбачає комплексний аналіз контекстуального оточення абревіатури. Дослідження мікроконтексту, який охоплює основну ідею в межах окремого речення, та макроконтексту, що розкриває загальну тему абзацу, розділу або навіть всього тексту, дозволяє точно визначити спеціалізацію та галузеву приналежність абревіатури. Цей аналіз є фундаментальним для подальшого успішного перекладу.

На другому етапі здійснюється ретельний пошук корелятів у спеціалізованих галузевих джерелах. Перекладач звертається до професійних

словників скорочень, довідників з кібербезпеки, глосаріїв міжнародних організацій, таких як стандарти NIST, таксономія загроз MITRE ATT&CK, документація OWASP, що дозволяє знайти авторитетні відповідники та зрозуміти точне значення терміна.

Третій етап включає вивчення міжнародних стандартів та нормативних документів. Аналіз відповідних абревіатур у англомовних довідниках, міжнародних стандартах з кібербезпеки та технічній документації допомагає визначити точне значення терміна та його місце в загальній термінологічній системі.

Четвертий етап передбачає ітераційний пошук, який активізується у разі невдачі попередніх досліджень. Особливу увагу приділяють можливості скорочення з другої чи третьої літери оригінального терміна, оскільки цей метод часто дозволяє досягти бажаного результату. Практика показує, що саме остання ліва буква абревіатури часто пояснює терміни оригінальної групи, які могли бути відсутніми в словниках на момент їх публікації.

На п'ятому етапі проводиться дослідження тематично близьких матеріалів та аналіз вживання абревіатури в автентичних джерелах. Вивчення наукових статей, технічної документації, матеріалів конференцій з кібербезпеки дозволяє зрозуміти реальний контекст використання терміна.

Шостий, найскладніший етап, передбачає повну реконструкцію початкового набору термінів. Ця процедура вимагає обов'язкового залучення висококваліфікованих перекладачів та фахівців з кібербезпеки і не гарантує абсолютно достовірних результатів. До цього методу рекомендується вдаватися лише у випадку, коли всі попередні способи розшифрування виявилися неефективними.

Створення нової української абревіатури в галузі кібербезпеки вимагає обов'язкових консультацій з фахівцями та експертами з інформаційної безпеки. Цей процес має ґрунтуватися на професійному консенсусі та враховувати специфіку української термінологічної системи.

Впровадження нових скорочень має бути ретельно обґрунтоване об'єктивною необхідністю стандартизації термінології. Особливо це стосується термінів, що описують новітні технології захисту, такі як *ZTNA* (*Zero Trust Network Access – мережевий доступ з нульовою довірою*) або *CNAPP* (*Cloud-Native Application Protection Platform – Платформа Захисту Рідних Хмарних Додатків*).

Кожна нова абревіатура повинна відповідати загальним принципам українського термінотворення, бути інтуїтивно зрозумілою для професійної спільноти та органічно вписуватися в існуючу термінологічну систему. Не менш важливим є забезпечення схвалення нових термінів експертним співтовариством, що гарантує їх подальше широке використання та стандартизацію.

У сфері кібербезпеки особливу увагу при перекладі потребують усічені абревіатури, де разом із закінченням видаляється граматична інформація про слово. Такі скорочення практично неможливо адекватно перекласти без аналізу контексту їх вживання.

Найпоширенішим видом є апокопа, коли абревіатура формується з перших трьох-чотирьох літер слова. В українській мові такий спосіб словотворення не набув значного поширення, тому в перекладі зазвичай використовується повна форма розшифрованого терміна: *config (configuration) – конфігурація; admin (administrator) – адміністратор; auth (authentication) – автентифікація; crypt (cryptography) – криптографія; mal (malicious) – шкідливий.*

При визначенні вихідної форми англійського терміна важливо враховувати, що усічення може стосуватися не лише першого, а й останнього компонента словосполучення. Переклад таких абревіатур здійснюється шляхом повного перекладу вихідної форми: *ENCRYPT (encryption protocol) – протокол шифрування; VULN (vulnerability scan) – сканування вразливостей; BACKUP (backup system) – система резервного копіювання*.

Еліптичний спосіб, що передбачає пропуск окремих елементів слова, також є продуктивним у кібербезпеці. Такі терміни виникають шляхом випадіння голосних і приголосних*: PWD* [password] – *пароль; SRV* [server] – *сервер; PKI* [public key infrastructure] – *інфраструктура відкритих ключів; FW* [firewall] – *фаєрвол; DB* [database] – *база даних*. Цей вид скорочень становить значні труднощі при перекладі, оскільки важливі частини інформації опущені, і вони містять лише непрямі підказки для відновлення повного терміна. Усічення дає лише часткове уявлення про зашифроване слово, і без контексту неможливо точно визначити, яке саме слово чи частина мови використовується автором.

Додатковою складнощі є варіативність написання таких скорочень – вони можуть бути написані великими або малими літерами, з крапками чи без них, що ще більше ускладнює процес їх розпізнавання та перекладу. Наприклад, скорочення «*config*» може вживатися як «*config*», «*Config*» або «CONFIG», що не змінює його значення, але впливає на процес ідентифікації терміна.

Ефективний переклад таких абревіатур вимагає від перекладача не лише знання стандартних скорочень, але й здатності аналізувати технічний контекст та використовувати спеціалізовані ресурси для верифікації значення термінів.

Особливі труднощі при перекладі становлять абревіатури, що поєднують літерні скорочення з повними словами. Найпоширенішим підходом до перекладу таких конструкцій є відтворення повного вихідного словосполучення з подальшою адаптацією до української термінології: *X-drone – безпілотний літальний апарат з крос-платформовим програмним забезпеченням; Q-bot – шкідливий бот із квазі-розподіленою архітектурою; C-vector – вектор атаки з використанням хмарних технологій; S-breach – порушення безпеки з використанням соціальної інженерії; Z-exploit – експлойт, що використовує технології нульового дня.*

Скорочені термінологічні одиниці демонструють значну ефективність у професійній комунікації, оскільки зменшують обсяг тексту, дозволяють передавати значну інформацію в стислій формі та оперативно адаптуються до змін у термінологічному апараті галузі. Вони легко утворюються та швидко запозичуються мовною спільнотою.

Однак існують і суттєві складнощі, пов'язані з їх дешифруванням, зумовлені гнучкістю механізмів термінотворення, постійним зростанням кількості нових понять та явищем лексичного дублювання [46, с. 88]. Саме тому перекладу таких одиниць слід приділяти підвищену увагу, залучаючи контекстуальний аналіз та спеціалізовані джерела.

Для передачі скорочень та акронімів найефективнішими визнаються такі методи: відтворення повними відповідниками 35% (для більшості стандартних термінів), використання відповідних україномовних абревіатур 25% (для міжнародно визнаних термінів); застосування описового перекладу 20% (для нових або складних понять), транскрибування та транслітерація 20% (для назв технологій, продуктів та міжнародних стандартів).

Цей розподіл демонструє, що близько 60% усіх абревіатур перекладаються з використанням повних відповідників або українських абревіатур, що свідчить про достатній рівень стандартизації української термінології кібербезпеки. Решта 40% випадків потребують більш гнучких підходів, таких як описовий переклад або транскрибування, що відображає динамічний характер розвитку галузі та постійне з'явлення нових понять.

Контекст відіграє вирішальну роль при перекладі стягнень та усічень, оскільки саме він дозволяє точно ідентифікувати значення скорочення та підібрати адекватний відповідник. Особливо це стосується новітніх термінів, таких як *AI-worm* (*шкідливий програмний код із штучним інтелектом*) або *QL-injection* (*ін'єкція з використанням квантових алгоритмів*), де без аналізу контексту неможливо визначити точну семантику скорочення.

Сучасна практика перекладу термінології кібербезпеки вимагає поєднання традиційних методів з інноваційними підходами, що враховують

швидкі темпи розвитку галузі та міждисциплінарний характер багатьох понять.

Отже, переклад абревіатур у галузі кібербезпеки є комплексним процесом, що поєднує лінгвістичні знання з глибоким розумінням предметної області. Основними викликами залишаються омонімія, швидке оновлення термінології та відсутність усталених відповідників. Ефективний переклад вимагає використання різноманітних методів – від прямого запозичення до творення нових українських абревіатур, з обов'язковим врахуванням контексту та цільової аудиторії. Ключовим фактором успіху є поєднання мовної компетенції з експертними знаннями з кібербезпеки, що забезпечує точність, однозначність та відповідність термінології сучасним вимогам. Стандартизація українських абревіатур має ґрунтуватися на професійному консенсусі та враховувати міжнародний досвід, що сприятиме розвитку вітчизняної термінологічної системи.

ВИСНОВКИ

Сучасна термінологія кібербезпеки являє собою живий організм, що перебуває у стані постійної трансформації. Вона характеризується безперервними внутрішніми модифікаціями, перегрупуванням значень, структурно-семантичними змінами та адаптацією до нових технологічних реалій. Ця динаміка обумовлена стрімким розвитком галузі, де щорічно з'являються нові загрози, технології та концепції захисту.

Термін кібербезпеки можна визначити як слово або словосполучення, що співвідноситься з відповідним поняттям галузі інформаційної безпеки, вступає в системні відносини з іншими термінологічними одиницями та утворює разом з ними цілісну термінологічну систему.

Лексичний фонд кібербезпеки демонструє переважно англо-латинське походження, що характерно для технічних дисциплін. Його відмінними рисами є інтенсивне неологізування, висока частка абревіатур та акронімів, а також переважання інтернаціоналізмів. Ці характеристики забезпечують ефективну міжнародну комунікацію та сприяють глобальному поширенню знань.

Сучасна термінологічна система кібербезпеки продемонструвала здатність до швидкої еволюції в умовах реальних загроз. Вона продовжує динамічно розвиватися, формуючи основу для професійної комунікації та створюючи передумови для подальшого вдосконалення термінологічного апарату галузі. Ця адаптивність забезпечує ефективне функціонування термінології в умовах постійних технологічних змін і нових викликів безпеці.

Термінологічна система пройшла складний шлях еволюції – від вузькоспеціалізованого технічного лексикону до комплексної, багаторівневої структури. Кожен етап розвитку характеризувався специфічними рисами, обумовленими технологічним прогресом, появою нових загроз та розширенням сфери застосування.

Сучасна термінологія кібербезпеки демонструє здатність до швидкої адаптації в умовах реальних загроз та технологічних змін. Вона продовжує динамічно розвиватися, формуючи основу для професійної комунікації та створюючи передумови для подальшого вдосконалення термінологічного апарату. Прагнення до глобальної стандартизації відображає інтернаціональний характер кіберзагроз та необхідність узгоджених підходів до захисту.

Термінологічний апарат кібербезпеки демонструє чітку стратифікацію за складністю структури. Переважають багатокомпонентні терміни (68%), тоді як однокомпонентні становлять лише 32%. Серед багатокомпонентних одиниць найпоширенішими є двокомпонентні (35%) та трикомпонентні (25%) терміни, що відображає потребу у точній номінації складних понять технічної галузі.

За частинами мови спостерігається значне домінування іменників (82%), що свідчить про об'єктно-орієнтований характер термінології. Дієслова (11%) та прикметники (6%) займають менші частки, відображаючи процесуальні та атрибутивні аспекти кібербезпеки. Прислівники представлені мінімально (1%), що характерно для технічних термінологій.

Серед простих термінів переважають афіксальні утворення (41%), тоді як кореневі (27%) та складні терміни (32%) мають приблизно рівну представленість. Це свідчить про високу продуктивність морфологічного словотворення в галузі кібербезпеки.

Афіксація підтвердила свій статус одного з найпродуктивніших способів термінотворення. Особливої продуктивності набули префікси cyber-, anti-, mal-, re- та суфікси -er, -ing, -tion, -ity. Словоскладання є основним механізмом утворення складних термінів, що забезпечує створення лаконічних та інформативно насичених одиниць.

Серед двокомпонентних термінів найпродуктивнішими є моделі Adj + N (65%) та N + N (45%), що забезпечує структурну стійкість та семантичну

прозорість. Моделі Ved + N (12%) та Ving + N (5%) демонструють активне використання дієприкметників для вираження якісних характеристик.

Трикомпонентні терміни представлені переважно моделями N + N + N (45%), Adj + Adj + N (21%) та Ved + N + N (15%). Чотирикомпонентні терміни менш поширені, що свідчить про прагнення до лаконічності при збереженні точності термінів.

Частка абревіатур становить 8-10%, що значно вище за багато інших галузей. Також виявлено незначну, але цікаву групу телескопізмів (0,8%), що свідчить про інноваційний характер термінотворення.

Структурне різноманіття термінології безпосередньо пов'язане з функціональними потребами галузі, де необхідно точно номінувати агенти, процеси та ключові атрибути цифрової безпеки. Висока частка багатокомпонентних термінів відображає складність та міждисциплінарний характер сучасної кібербезпеки.

Отже, структурні особливості англомовної термінології кібербезпеки демонструють її високий ступінь розвитку, системності та здатності адаптуватися до постійних змін у сфері інформаційної безпеки, що робить її ефективним інструментом професійної комунікації у глобальному масштабі.

Семантична трансформація існуючих лексичних одиниць є основним механізмом формування термінологічного апарату кібербезпеки. Цей процес забезпечує швидке реагування на потреби у нових термінах без необхідності створення абсолютно нових лексичних одиниць, що особливо важливо в умовах стрімкого технологічного прогресу.

Дослідження виявило чітку ієрархію семантичних процесів за критерієм їх частотності: Термінологізація (65%) – домінуючий механізм, що відображає потребу швидкого номінування нових понять; Детермінологізація (25%) – свідчить про вплив кібербезпеки на сучасну культуру та масову свідомість; Транстермінологізація (10%) – забезпечує міждисциплінарність термінологічної системи.

Метафоричні моделі систематизовані за джерелом походження на чотири основні категорії: антропоморфні метафори; топографічні метафори; зооморфні метафори; військові метафори. Метонімічні процеси реалізуються через три основні типи відношень: «ціле – частина»; «процес – результат»; функціональна суміжність.

Терміносистема структурована навколо шести основних тематичних груп, що відображають ключові аспекти галузі: загрози та шкідливе програмне забезпечення; методи та засоби захисту; мережеві технології та інфраструктура; процеси забезпечення безпеки та управління; властивості та характеристики систем безпеки; структурні елементи та компоненти даних.

Структура термінології має ієрархічно-мережевий характер, де центральні поняття, запозичені з фізичного світу, утворюють ядро системи з гілками спеціалізованих значень. Ця структура поєднує стабільність з гнучкістю, дозволяючи адаптуватися до нових викликів.

Семантичні особливості термінології кібербезпеки демонструють здатність мови адаптивно реагувати на виклики інформаційного суспільства. Динамічний баланс між професійною комунікацією, популяризацією знань та міжгалузевим синтезом забезпечує як точність термінології, так і її доступність для широкого загалу.

Отже, семантичні процеси в термінології кібербезпеки відображають фундаментальні властивості мови як живої, адаптивної системи, здатної ефективно реагувати на виклики сучасного інформаційного суспільства та забезпечувати ефективну комунікацію в умовах технологічного розвитку.

Проведене дослідження довело, що основним засобом передачі англомовних термінів кібербезпеки є пошук адекватних термінологічних відповідників (59% випадків). Переклад термінології є динамічним процесом, що поєднує традиційні методики з інноваційними підходами, адаптованими до специфіки галузі. Розвиток української термінологічної системи відбувається шляхом пошуку оптимального балансу між міжнародними стандартами та національною мовною традицією.

Для простих термінів найефективнішими виявилися методи термінологічної відповідності та конкретизації. Остання є особливо продуктивною, оскільки багато термінів утворені від слів загальної лексики, які в технічному контексті набувають спеціалізованого значення. Вміння виокремити це конкретне значення є запорукою адекватного перекладу.

Складні терміни та словосполучення вимагають застосування чотириетапного алгоритму перекладу: ідентифікація ключових компонентів; аналіз семантичних зв'язків; вибір стратегії перекладу; адаптація до мовних норм. Цей алгоритм забезпечує точність, однозначність та природність звучання перекладу.

Для абревіатур характерне таке статистичне розподілення методів перекладу: відтворення повними відповідниками (35%); використання україномовних абревіатур (25%); описовий переклад (20%); транскрибування та транслітерація (20%). Близько 60% усіх абревіатур перекладаються з використанням повних відповідників або українських абревіатур, що свідчить про достатній рівень стандартизації української термінології.

Контекст відіграє вирішальну роль при перекладі, особливо для новітніх термінів та абревіатур. Один і той самий термін може отримувати різні варіанти перекладу залежно від галузевої специфіки та цільової аудиторії. Технічний переклад орієнтований на точність, тоді як переклад для менеджменту робить акцент на зрозумілості.

Основними викликами залишаються омонімія, швидке оновлення термінології та відсутність усталених відповідників. Ефективний переклад вимагає поєднання мовної компетенції з експертними знаннями з кібербезпеки.

Проведене дослідження довело, що переклад англомовних скорочень у сфері кібербезпеки реалізується через декілька ключових підходів. Найпоширенішими методами для ініціальних скорочень та акронімів є використання відповідних українських абревіатур, застосування описового перекладу та різні види транскодування. Особливу увагу при перекладі

усічень та стягнень потребує контекстуальний аналіз, оскільки саме контекст дозволяє точно ідентифікувати значення таких скорочених форм.

Специфічні труднощі виникають при необхідності створення нових скорочень засобами української абревіації, коли відповідного аналога в мові перекладу не існує. У таких випадках процес перекладу здійснюється за двоетапною методикою, що включає дешифрування вихідної одиниці з подальшим передаванням семантичних корелятів українською мовою.

Перспективним напрямом подальших наукових пошуків вбачається аналіз комунікативно-прагматичних аспектів вживання англомовних термінів кібербезпеки у фахових текстах, що дозволить поглибити розуміння функціонування термінології в професійній комунікації та вдосконалити методику її перекладу.

Отже, сучасна практика перекладу термінології кібербезпеки вимагає комплексного підходу, що враховує структурні, семантичні та функціональні особливості термінів, а також динамічний характер розвитку галузі.

SUMMARY

The theme of the master degree paper is English Professional Vocabulary of Cybersecurity: Structure, Semantics, Translation.

The topicality of the research lies in the necessity for a comprehensive study of English cybersecurity terminology. This need arises from the insufficient scholarly exploration of this issue, coupled with the rapid growth of the industry term base. The relevance is further underscored by the prospective nature of research into the peculiarities of translating English cybersecurity terms, particularly within the context of the constant renewal in the terminological fund.

The requirement for further linguistic analysis is driven by both the practical needs of professional communication and the scientific task of systematizing the national terminology in line with modern global trends. It is equally crucial to study cybersecurity terminology as a vehicle of scientific knowledge, to define its structure, derivation methods, specific features and composition. A significant practical impetus for this work is the notable absence of specialized Ukrainian-English dictionaries in this field.

The objective of the paper is to study and describe English cybersecurity terms, their structural and semantic features, as well as the methods of their translation into Ukrainian.

The objective set foresees the fulfilling of the following **tasks:** to to clarify the meaning of the core concepts «term», «terminology», and «terminological system» and to characterize their structure and semantic features; to trace the main stages of the formation and development of English cybersecurity terminology in historical and technological aspects and to provide a systematic description of the terminological composition in cybersecurity vocabulary, identifying its structural components and functional characteristics; to outline the criteria for defining English cybersecurity terminology and to conduct a structural-semantic analysis of the specified terms; to investigate the methods of translating cybersecurity terms and to provide recommendations for their translation.

The object of the research is English-language cybersecurity terms.

The subject of the research is the structural and semantic peculiarities of English-language cybersecurity terms and the methods of their translation into Ukrainian.

The following methods were used in the research: *the descriptive method* – for providing a general characterization of the concepts «term», «terminology», «terminological system» and for describing the lexical units of the English-language cybersecurity terminological system; *the thesaurus method* – for disclosing the meaning of new lexical units through dictionary definitions; *the word-formation method* – for determining the structural types, paths, ways, and mechanisms of formation of English-language cybersecurity terms; *the contextual method* – for clarifying the semantics of cybersecurity terms within specific speech environments; *the componential method* – for identifying the constituents of the sememic structure of cybersecurity terms; *translation analysis* – for aiming at identifying methods for translating English-language cybersecurity terms in context and the translation transformations involved in this process. Auxiliary methods include *etymological analysis* and *quantitative analysis* of the factual material used.

The novelty of the research lies in the fact that, for the first time, a comprehensive historical and linguistic analysis of modern English cybersecurity terminology has been undertaken within a single study. This paper identifies its structural and semantic features systematically, describes the most productive ways and models of term formation, and establishes primary approaches to translating these terms into Ukrainian. The research contributes to the systematization of the national terminological system in the field of cybersecurity significantly.

The practical significance of the obtained results lies in their potential to enhance the language training of specialists in information security and related IT fields. The systematized models of term formation and translation of English cybersecurity terms provide a foundation for developing educational and methodological materials, specialized modules for professional English language

courses, and training programs for technical translators. The research findings can be applied in formulating recommendations for the standardization and unification of Ukrainian equivalents of cybersecurity terminology, as well as in the practice of specialized translation within governmental structures, the business sector, and educational-scientific institutions. These developments can facilitate the creation of modern glossaries, industry-specific dictionaries, and reference resources, thereby improving the accuracy and standardization of professional communication in the field of cybersecurity.

The MP consists of an introduction, which briefly summarizes the topicality, novelty, object, subject matter, research material, objective and tasks, as well as the practical significance of the study.

The first chapter of the qualification paper outlines the theoretical foundations of terminology studies, specifically defining the essence of the concepts «term», «terminology», and «terminological system». It traces the stages of formation and development of the English-language cybersecurity terminological system, shaped by technological progress and global challenges. Methodological approaches to researching this specialized terminology are also considered.

The second chapter is dedicated to investigating the structural and semantic peculiarities of English-language cybersecurity terms. It identifies the main word-formation models, mechanisms, and means of creating these terms. Their part-of-speech structure is analyzed. Particular attention is paid to key semantic processes within this terminological sphere: terminologization of common vocabulary, determinologization, and reterminologization.

The third chapter conducts a detailed analysis of the methods for translating English-language cybersecurity terms, taking into account their structural and semantic features. It examines the lexical-semantic and grammatical transformations applied when translating sentences containing these units and discusses the difficulties in translating English cybersecurity terminology.

The main conclusions outline the key theoretical and practical results of the presented work, as well as its potential future research directions. **The Appendices** contain a Glossary of English-language cybersecurity terms and examples of these terms in context.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алієва О. Н. Семантичний інваріант як компонент терміноутворення // Вісник Львівського університету. Серія Іноземні мови. Львів: Львівський нац. ун-т ім. І. Франка, 2010. Вип. 17. С. 88–93.

2. Асмукович І. Сучасна термінологія: теорія та практика: навчальний посібник. Київ : Вид-во Київського університету, 2019. 312 с.

3. Баловнєва О. Особливості перекладу англійської науковотехнічної термінології // Вісник Житомирського державного університету ім. І. Франка. 2004. № 17. С. 79–81. URL : http://www.nbuv.gov.ua/articles/2004/04boontt.zip (дата звернення 04.09.2025).

4. Баранова О. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. 2014. № 2 (42). С. 54–62. URL: http://ippi.org.ua/sites/default/files/ 14boavpk.pdf (дата звернення 04.09.2025).

5.Басова А. Забезпечення громадської безпеки: поняття та зміст // Адміністративне право і процес. 2012. № 2 (2). URL : http://applaw.knu.ua/index.php/arkhiv-nomeriv/2-2-2012/item/52-zabezpechennya-hromadskoyi-bezpekyponyattya-ta-zmist-basov-a-v1(дата звернення 14.09.2025).

6. Бідненко Н. Науково-технічний переклад з англійської мови. Дніпропетровськ : Дніпропетровський університет Альфреда Нобеля, 2014. 243 с.

7. Білозерська Л., Возненко Н., Радецька С. Термінологія та переклад : навчальний посібник. Вінниця : Нова Книга, 2010. 232 с.

8. Бойченко Л. Структурно-семантичні типи абревіатур і діапазон їх деривaційної активності в сучасній українській мові // Мовознавство. 1982. № 5. С. 75–80.

9. Борщ І. Особливості перекладу сучасних термінів комп’ютерної сфери з англійської українською мовою // Нова філологія. Запоріжжя : Запорізький національний університет. 2011. № 45. С. 175–177.

10. Ботвин Т. Щодо англомовної термінологічної системи сектору кібербезпеки України в умовах воєнного стану: аналіз дефініцій // Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика. Т. 33 (72). № 6. Ч. 1. 2022. С. 90–94.

11. Васковець О. Українська термінологія: історія і сучасність. Київ : ВЦ «Академія», 2013. 400 с.

12. Васковець О. Термінологія як об'єкт стандартизації. Київ : Наукова думка, 2015. 458 с.

13. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення // Комп'ютерні науки та кібербезпека, 2019, (1), 18–30. URL : https://doi. org/10.26565/2519-2310-2019-1-02 (дата звернення 14.09.2025).

14. Гаврилова О. Місце комп'ютерної термінології в українській мові // Лінгвістичні дослідження: збірник. наук. праць ХНПУ ім. Г. С. Сковороди. Харків. 2017. Вип. 45. С. 189–193.

15. Гільченко Р. Переклад англійських суфіксальних термінів фахової мови авіації // Вісник Національного університету «Львівська політехніка». Сер. : «Проблеми української термінології». 2006. № 559. С. 109–112.

16. Горпинич В. Сучасна українська літературна мова. Морфеміка. Словотвір. Морфонологія. Київ : Вища школа, 1999. 326 с.

17. Даник Ю. До питання про визначення поняття «кібербезпека» // Актуальні проблеми філології та перекладознавства. 2018. Вип. 13. С. 45–49.

18. Даник Ю. Семантична структура терміна «кібербезпека» в англійській та українській мовах // Лінгвістика XXI століття: нові дослідження і перспективи. 2019. С. 112–116.

19. Даник Ю. Термінологічна стандартизація в галузі кібербезпеки: український та міжнародний контекст // Мова: науковий журнал. 2020. № 33. С. 87–93.

20. Д’яков А., Кияк Т., Куделько З. Основи термінотворення: семантичний та соціолінгвістичний аспект. Київ : Видавничий дім «КМ Academia», 2000. 218 с.

21. Дячук Т. Авіаційна термінологія української мови: тематична класифікація та генетична характеристика // Матеріали наук.-практ. конф. Київ : Наука, 2009. С. 45–52.

22. Єнчева Г. Лінгвокогнітивне моделювання процесу перекладу авіаційних термінів (на матеріалі англо-українських версій нормативно-технічної документації ІСАО) : автореф. дис. … канд. филол. наук : [спец.] 10.02.16 «Перекладознавство» / Південно-український національний педагогічний університет ім. К. Д. Ушинського. Одеса, 2011. 24 с.

23. Єнікеєва С. Англомовна термінологія інформаційної безпеки: структурно-семантичний аспект // Наукові записки Національного університету «Острозька академія». Серія «Філологія». 2015. Вип. 52. С. 84–87.

24. Єнікеєва С. Лексико-семантичні особливості англомовної термінології інформаційної безпеки // Мовні і концептуальні картини світу. Київ, 2014. Вип. 49. С. 267–271.

25. Єнікеєва С. Особливості побудови термінографічного порталу (на матеріалі англомовної термінології інформаційної безпеки) // Мовні і концептуальні картини світу : збірник наукових праць / Київський національний університет імені Тараса Шевченка. Київ, 2016. Випуск 52, Том 1. С. 208–214.

26. Єнікеєва С. М. Структурно-семантичні особливості англомовної термінології інформаційної безпеки // Актуальні проблеми германістики, романистики та україністики: тези доповідей міжнародної наукової конференції. Чернівці: Чернівецький нац. ун-т, 2014. С. 85–86.

27. Животченко О., Кузнєцова І. Метафорічні терміни англомовної терміносистеми кібербезпеки // Тези доповідей І Міжнародній науково-практичній конференції «Актуальні проблеми дискурсології,

перекладознавства та методики викладання», Запоріжжя, 21 листопада 2025 року. Запоріжжя: НУ «Запорізька політехніка», 2025. С. 118–121.

28. Животченко О., Кузнєцова І. Щодо етімології слова «кібербезпека» // Тиждень науки-2025. Гуманітарний факультет. Тези доповідей науково-практичної конференції, Запоріжжя, 14–18 квітня 2025 р. [Електронний ресурс] / Редкол.: Вадим ШАЛОМЄЄВ (відпов. ред.) Електрон. дані. Запоріжжя: НУ «Запорізька політехніка», 2025. С. 94–96. 1 електрон. опт. диск (DVD-ROM); 12 см. Назва з тит. екрана.

29. Зацний Ю., Пахомова Т. Мова і суспільство: збагачення словникового складу сучасної англійської мови. Запоріжжя : ЗДУ, 2001. 243 с.

30. Кальник О., Воробйова О., Симоненко А., Олешко О. Термінологічні проблеми перекладу наукових текстів в сфері ІТ-технологій // Молодий вчений. 2019. № 5.1 (69.1). С. 178–190.

31. Карабан В. Переклад англійської наукової і технічної літератури. Граматичні труднощі, лексичні, термінологічні та жанрово-стилістичні проблеми. Вінниця : Нова книга, 2004. 564 с.

32. Карабан В. Посібник-довідник з перекладу англійської наукової і технічної літератури на українську мову. Київ : Політична думка, 1997. 438 с.

33. Квитко І. Термін у науковому документі. Львів. : Вища школа, 1976. 128 с.

34. Кияк Т. Проблема лінгвістичного упорядкування термінології // Українська термінологія і сучасність : зб. наук. пр. Київ, 2005. Вип. VI. С. 13–17.

35. Кікец І. До питання про деякі труднощі при перекладі термінів ішляхи їх подолання // Вісник державного університету «Львівська політехніка». Львів : Львівська політехніка, 2000. № 402. С. 420.

36. Ковалик І., Самійленко С. Загальне мовознавство: Історія лінгвістичної думки : навчальний посібник. Київ : Вища шк., 1985. 215 с.

37. Коваленко А. Я. Загальний курс наукового перекладу. Київ : Інкос, 2001. 346 с.

38. Ковальчук О. Структурно-семантичні особливості сучасної англомовної комп'ютерної термінології // Наукові записки Національного університету «Острозька академія». Серія «Філологічна». Острог, 2015. Вип. 55. С. 49–52.

39. Ковальчук О. Термінологічні неологізми в англомовній комп'ютерній лексиці // Молодий вчений. 2016. № 3. С. 47–50.

40. Коптілов В. В. Теорія і практика перекладу. Київ, 2003. 185 с.

41. Коробова І. О. Лексико-семантичне освоєння новітніх англізмів у сучасній українській мові // Вісник Київського національного лінгвістичного університу. Серія : Філологія. 2019. № 22. Т. 1. С. 109–122.

42. Крижанівська А., Симоненко Л. Актуальні проблеми упорядкування наукової термінології. Київ : Вища школа, 1987. 163 с.

43. Кротевич Є. Словотвір термінів // Мовознавство. 1968. № 2. С. 3–9.

44. Лук'янчук Р. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції // Вісник НАДУ: зб. наук. праць. 2015. Вип. 3. С. 110–116.

45. Ментинська І. Основи термінознавства: навч. посіб. Київ : Центр навчальної літератури, 2008. 224 с.

46. Мирошниченко В., Шишкова І. Англійські лексичні новоутворення у сфері комп'ютерних технологій та особливості їх перекладу українською мовою // Вісник Національного технічного університету «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства, № 1. Харків. 2019. С. 87–92.

47. Михайлова Т. Семантичні відношення в українській науково-технічній термінології : дис. … канд. філол. наук. [спец.]: 10.02.01 «Українська мова» / Харківський національний педагогічний університет імені Г. С. Сковороди. Харків, 2002. 218 с.

48. Мороховський О. М. Деякі питання теорії запозичень // Мовознавство. 1984. № 1. С. 19–25.

49. Мосієвич Л. Труднощі перекладу англомовних багатокомпонентних термінів з машинобудування українською мовою // Вчені записки Таврійського національного університету імені В. Вернадського, серія «Філологія. Журналістика». 2022. Т. 33 (72). № 5. С. 29–35.

50. Мостовий М. Лексикологія англійської мови. Харків : Основа, 1993. 256 с.

51. Основи термінотворення: Семантичний та соціолінгвістичний аспекти / Д'яков А.С., Кияк Т., Куделько З. Київ. КМ Academia. 2000. Випуск 34. Том 1. 218 с.

52. Панько Т. Українське термінознавство : підручник для студ. вищ. навч. закл. Львів : Світ, 1994. 216 с.

53. Полюга Л. Про антоніми та їх використання // Словник антонімів української мови / ред. Л. С. Паламарчук. 2-е вид., доп. і випр. Київ : Довіра, 2001. С. 5–22.

54. Перебийніс В. Термінологічна лексика. Київ : Наукова думка, 1979. 175 с.

55. Пономарева Л. Семантические ограничения в образовании девербативных производных со значеним субъекта действия // Вісник ДНУ. Сер. : Мовознавство. Днепропетровск, 2014. Т. 22. № 11. С. 127 –133.

56. Радецька С. Засоби вираження експресії в науково-популярній літературі // Наукові записки Ніжинського державного університету ім. Миколи Гоголя. Сер. : Філологічні науки. 2014. Кн. 2. С. 191–195.

57. Ракшанова Г. Семантичні особливості науково-технічного терміна // Українська термінологія і сучасність : зб. наук. праць. / ред. Л. Симоненко. Київ, 2005. Вип. VI. С. 198–201.

58. Романенко А. Термінологія в системі мови. Київ : Наукова думка, 1986. 160 с.

59. Самійленко С. Термінографічна практика в Україні: традиції та новації // Мовознавство. 2001. № 4. С. 23–29.

60. Селіванова О. Сучасна лінгвістика: напрями та проблеми. Полтава : Довкілля. Київ : Довіра, 2008. 712 с.

61. Семантична деривація лексики в аспекті міжмовних досліджень : колективна монографія / кол. авт.; голов. ред. О. Деменчук. Рівне : РДГУ, 2019. 150 с.

62. Сергєєва Г. Термінологічна лексикографія: український досвід // Мовознавство. 2012. № 4. С. 45–52.

63. Симоненко Л. Українська термінографія: стан і перспективи // Мовознавство. 2014. № 4. С. 28–35.

64. Скороходько Є. Термінологічні системи: структура та функціонування. Київ : Наукова думка, 1998. 215 с.

65. Тарасова Л. Термінологічні поля: структура та семантика // Мовні і концептуальні картини світу. 2014. Вип. 48. С. 134–140.

66. Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення // Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.практ. конф. (м. Київ, 4 квіт. 2019 р.). Київ : Нац. акад. СБУ, 2019. С. 365–368.

67. Фурт Д. Способи перекладу термінів українською мовою з англійської // Філологічні студії. Науковий вісник Криворізького державного пед. університету. Кривий Ріг : ФОП Маринченко С., 2018. Вип. 17. С. 284–292.

68. Халіновська Л. Українська авіаційна термінологія у лексикографічному опрацюванні // Українська мова, 2014. № 3. С. 86–110.

69. Черновол В. Кібербезпека як різновид публічної безпеки // Актуальні проблеми адміністративно-правового забезпечення діяльності Національної поліції. Харків, 2017. С. 72–74.

70. Шванова О. Особливості перекладу термінів з кібербезпеки // Науковий вісник Міжнародного гуманітарного університету. Сер.: Філологія. Одеса. 2023. № 59. Том 3. С. 180–183.

71. Шелова С. Термінологічні системи та їх класифікація // Вопросы языкознания. 1972. № 5. С. 34–45.

72. Янковець О. Сучасна термінологія: теорія, методологія, практика. Київ : Вид-во КНУ імені Тараса Шевченка, 2018. 320 с.

73. Alimemaj (Metaj) Zamira. Web-language and Word-formation Processes on Slang Words // Lingua Mobilis. 2012. No. 5 (38). P. 119–125.

74. Atul G., Rezawana I., Tonoy C. Evolution of Aircraft Flight Control System and Fly-By-Light Flight Control System // International Journal of Emerging Technology and Advanced Engineering. 2013. Vol. 3. Iss. 12. P. 568–600.

75. Bauer L. Compounds and Multi-word Expressions in English // Complex Lexical Units: Compounds and Multi-Word Expressions / ed. by Barbara Schlücker. London : GmbH, 2019. P. 53–65.

76. Bidnenko N.The Language Peculiarities Of Modern English Scientific And Technical Literature Style // Вісник Дніпропетровського університету імені Альфреда Нобеля. Сер. : Філологічні науки. 2014. № 2 (8): URL : http://phil.duan.edu.ua/images/stories/Files/2014/2014_222/27.pdf (дата звернення 30.09.2025).

77. Cabré M. T. Theories of Terminology: Their Description, Prescription and Explanation // Terminology. 2003. № 2. P. 163–199.

78. Griffiths Ch. The Latest 2024 Cyber Crime Statistics. AAG IT Support. URL : aag-it.com (дата звернення 30.09.2025).

79. Johansen A.G. What is Cyber Security? What you Need to Know? NORTON.LifeLock. 28.04.2022. URL: https://us.norton.com/ blog/ malware/what-is-cybersecurity-what-you-need-toknow# (дата звернення 30.09.2025).

80. Friginal E. English in Global Aviation: Context and Pedagogy. London : Bloomsbury Academic, 2019. 304 p.

81. Jochansen A. Terminology in the Digital Age: Theories and Practices. Copenhagen : Nordic Academic Press, 2019. 245 p.

82. Hughes J., Aycock S., Caines A. Detecting Trending Terms in Cybersecurity Forum Discussions // Proceedings of the Sixth Workshop on Noisy User-generated Text (W-NUT 2020). Online: Association for Computational Linguistics, 2020. P. 107–115. URL: https://aclanthology.org/2020.wnut-1.16/14. (дата звернення 30.09.2023).

83. 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-badmetaphoric-branding-cyberspace (дата звернення: 24.09.2025).

84. Li Y., Cheng J., Huang C., Chen Z., & Niu W. NEDetector: Automatically Extracting Cybersecurity Neologisms from Hacker Forums // Journal of Information Security and Applications. 2021. № 58. P. 65–76.

85. Mosiyevych L. The Formation of a Modern Translation Competence in Translator Training // At the Crossroads: Challenges of Foreign Language Learning. 2017. P. 189–202.

86. Munday J. Introducing Translation Studies: Theories and Applications // Routledge. 2005. P. 45–54.

87. Rezawana I., & Stubelius S. Terminology Extraction and Management in Digital Humanities: A Corpus-Based Approach // Proceedings of the 12th International Conference on Language Resources and Evaluation (LREC). 2020. P. 456–462.

88. Savory T. The Art of Translation. London : Routledge, 1957. 286 p.

89. Schatz D., Bashroush R., Wall J. Towards a More Representative Definition of Cyber Security // Journal of Digital Forensics, Security and Law. 2017, 12 (2). P. 87–92.

90. Stubelius S. The Dynamics of Legal Terminology in a Multilingual Context: A Case Study of EU Documents // Terminology. 2018. 24(2). P. 189–215.

91. Tonoy C., Das A., & Zhang W.A Survey on Neural Terminology Extraction: Methods, Applications and Challenges // ACM Computing Surveys. 2021. 54(8). P. 1–36.

92. Trong L. Strategies to Translate Information Technology (IT) Terms // Theory and Practice in Language Studie. Vol. 1. No. 1. January 2011. P. 1–7.

93. Wüster E. Einführung in die Allgemeine Terminologielehre und Terminologische Lexikographie. Wien / New York: Springer, 1979. 2., um ein Vorwort erweiterte Auflage. 138 S.

СПИСОК ЛЕКСИКОГРАФІЧНИХ ДЖЕРЕЛ

94. Академічний тлумачний словник української мови (1970–1980). URL : http://sum.in.ua/ (дата звернення 13.11.2023).

95. Англо-український словник термінів з інформаційних технологій та кібербезпеки / уклад. А. Гладун та ін.; за ред. А. Гладуна. Київ : Наукова думка, 2021. 648 с.

96. Великий тлумачний словник сучасної української мови / уклад. та голов. ред. В. Т. Бусел. Київ : Ірпінь : Перун, 2001. 1440 с.

97. Гладун А., Пучков О., Субач І., Хала К. Англо-український словник термінів з інформаційних технологій та кібербезпеки. URL : https://ela.kpi.ua/handle/123456789/45895 (дата звернення 13.11.2023).

98. Загнітко А. Сучасний лінгвістичний словник. Вінниця : ТВОРИ, 2020. 920 с.

99. Кротевич Є., Родзевич Н. Словник лінгвістичних термінів. Київ : Вид-во АН УРСР, 1957. 236 с.

100. Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/cybersecurity (дата звернення 13.11.2023).

101. Gadsby A.. Longman Dictionary of Contemporary English. Barcelona : Longman dictionaries, 1995. 1668 p.

102. Glossary of Cyber Security Terms. URL : https://csrc.nist.gov/glossary/term/cybersecurity (дата звернення 13.11.2023).

ДЖЕРЕЛА ІЛЮСТРАТИВНОГО МАТЕРІАЛУ

103. Відділ «Безпека» // Інтернет-видання DO (depo.ua) : веб-сайт. URL : https://dt.ua/TECHNOLOGIES/security/ (дата звернення: 12.11.2025).

104. Державна установа «Комп'ютерна група екстренного реагування України (CERT-UA)» : офіційний веб-сайт. URL : https://cert.gov.ua/ (дата звернення: 12.11.2025).

105. Кіберполіція Національної поліції України : офіційний веб-сайт. URL : https://cyberpolice.gov.ua/ (дата звернення: 12.11.2025).

106. Кребс Б. Krebs on Security : особистий блог про кібербезпеку та кіберзлочинність / Brian Krebs. URL : https://krebsonsecurity.com/ (дата звернення: 12.11.2025).

107. Офіційний канал Кіберполіції України // Telegram : месенджер. URL : https://t.me/cyberpolice_ua (дата звернення: 12.11.2025).

108. Розділ за тегом «Security» // AIN.UA : українське онлайн-видання про технології. URL : https://ain.ua/tag/security/ (дата звернення: 22.11.2025).

109. Рубрика «Безпека» // Тексти.org.ua : український журнал про технології та суспільство. URL : https://texty.org.ua/tag/security/ (дата звернення: 22.11.2025).

110. BleepingComputer : новинний сайт та форум з питань кібербезпеки та інформаційних технологій. URL : https://www.bleepingcomputer.com/ (дата звернення: 12.10.2025).

111. CSO Online : інформаційний ресурс для керівників з інформаційної безпеки (CISO). URL : https://www.csoonline.com/ (дата звернення: 22.11.2025).

112. Dark Reading : інформаційно-аналітичний портал з поглибленими матеріалами з кібербезпеки. URL : https://www.darkreading.com/ (дата звернення: 22.11.2025).

113. National Institute of Standards and Technology Glossary. NIST Computer Security Resource Center. URL : 120 https://csrc.nist.gov/glossary?sortBy-lg=relevance&ipp-lg=100 (дата звернення: 24.09.2025).

114. The Hacker News : міжнародне новинне видання про кібербезпеку. URL : https://thehackernews.com/ (дата звернення: 22.11.2025).

ДОДАТКИ

Додаток А

Глосарій англомовних термінів кібербезпеки

- 2FA (Two-Factor Authentication) – двофакторна автентифікація (2FA)
- 3FA (Three-Factor Authentication) – трифакторна автентифікація (3FA)
- 5G Application Protection – захист додатків 5G
- 5G Network Security – безпека мережі 5G

A

- Abuse – зловживання
- Access – доступ
- Access Blocking – блокування доступу
- Access Control – контроль доступу
- Access Control List (ACL) – список контролю доступу (СКД)
- Access Control Rules – правила контролю доступу
- Access Point (AP) – точка доступу
- Access Rights – права доступу
- Access Rights-Based Web Attack Handling Strategies – стратегії обробки веб-атак на основі прав доступу
- Account – обліковий запис
- Account Hijacking – захоплення облікового запису
- Account Recovery – відновлення облікового запису
- Accreditation – акредитація
- Acquisition – отримання, захоплення (даних)
- Active Attack – активна атака
- Active Directory (AD) – служба каталогів Active Directory
- Adblocker – блокувальник реклами

- Advanced Attack Analysis Strategies – стратегії аналізу розширених атак
- Advanced Cyber Attacks – розширені кібератаки
- Advanced Encryption Standard (AES) – розширений стандарт шифрування (AES)
- Advanced Exploit Attack Handling Strategies – стратегії обробки розширених атак з використанням вразливостей
- Advanced Hacking Attack Handling Strategies – стратегії обробки розширених хакерських атак
- Advanced Malware Analysis – розширений аналіз шкідливого ПЗ
- Advanced Network Analysis Strategies – стратегії розширеного аналізу мережі
- Advanced Network Attacks Analysis – аналіз розширених мережевих атак
- Advanced Persistent Threat (APT) – розширена постійна загроза (APT/РПЗ)
- Advanced Persistent Threat (APT) Detection – виявлення розширених постійних загроз (APT)
- Advanced Persistent Threats (APTs) – розширені постійні загрози (APTs)
- Advanced Security Analysis – розширений аналіз безпеки
- Advanced Security Threats – розширені загрози безпеки
- Advanced Threat – розширена загроза
- Advanced Threat Analysis – аналіз розширених загроз
- Advanced Threat Detection – виявлення розширених загроз
- Advanced Threat Detection Systems – системи виявлення розширених загроз
- Adversary – противник, супротивник
- Adware – рекламне ПЗ, адвер

- Aggressive Penetration Attack Analysis – аналіз агресивних атак на проникнення
- AI-based Device Protection Strategies – стратегії захисту пристроїв на основі ШІ
- Aircraft Computer System Protection – захист комп'ютерних систем літаків
- Air Safety System Breach Attack Handling Strategies – стратегії обробки атак на порушення авіаційних систем безпеки
- Alert – сповіщення, тривога
- Algorithm – алгоритм
- Allowlist – дозволений список (білий список)
- Amplification Attack – атака посилення
- Analytics – аналітика
- Anomaly – аномалія
- Anomaly Behavior Analysis – аналіз аномальної поведінки
- Anomaly Behavior Predictive Analysis – прогнозний аналіз аномальної поведінки
- Anomaly Detection – виявлення аномалій
- Anomaly Monitoring – моніторинг аномалій
- Animal Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання тварин
- Anti-Malware – антивірус, захист від шкідливого ПЗ
- Anti-Malware Protection – захист від шкідливого ПЗ
- Anti-Malware Software – антивірусне програмне забезпечення (ПЗ)
- Anti-Spam – захист від спаму (антиспам)
- Anti-Spyware – захист від шпигунського ПЗ
- Anti-Tampering Techniques – методи захисту від несанкціонованого втручання
- Antivirus / Antivirus Protection – антивірус / антивірусний захист

- Antivirus software – антивірусне програмне забезпечення (антивірус)
- API Security – безпека API
- Appliance – апаратне рішення, пристрій безпеки
- Application – додаток, застосунок
- Application Layer – рівень застосунків
- Application Misuse Attack Analysis – аналіз атак з використанням неправильного вжитку додатків
- Application Security – безпека додатків
- Application Security Testing – тестування безпеки додатків
- Application Testing – тестування додатків
- Arbitrary Code Execution (ACE) – виконання довільного коду
- Arbitrary Security Threats – довільні загрози безпеки
- Architecture – архітектура
- Archive – архів
- Artificial Intelligence (AI) – штучний інтелект (ШІ)
- Artificial Intelligence Data Protection – захист даних штучного інтелекту
- Artificial Intelligence Privacy Breach Attack Analysis – аналіз атак на порушення приватності штучного інтелекту
- Artificial Intelligence System Breach Attack Analysis – аналіз атак на порушення систем штучного інтелекту
- Artificial Intelligence-Based Device Protection – захист пристроїв на основі штучного інтелекту
- Artificial Intelligence-Based Intelligence Systems Protection – захист інтелектуальних систем на основі штучного інтелекту
- Artificial Intelligence-Based Systems Protection – захист систем на основі штучного інтелекту
- Asset – актив
- Asset Management – управління активами

- Assurance – гарантія, забезпечення
- Assurance and Trust Analysis – аналіз гарантій та довіри
- Association and Organization Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління асоціаціями та організаціями
- Asymmetric Cryptography – асиметрична криптографія
- ATM Technology System Protection – захист систем банкоматної (ATM) технології
- Attack – атака, напад
- Attack Alerting – сповіщення про атаки
- Attack Attribution – атрибуція атаки (визначення джерела)
- Attack Chain – ланцюжок атаки
- Attack Mitigation – пом'якшення атаки
- Attack Surface – поверхня атаки
- Attack Targeting – цілеспрямованість атаки / вибір цілі для атаки
- Attack Vector – вектор атаки
- Attacker – атакуючий, зловмисник
- Audit – аудит, перевірка
- Audit Log (Audit Trail) – журнал аудиту (слід аудиту)
- Augmented Reality Device Breach Attack Handling Strategies – стратегії обробки атак на порушення пристроїв доповненої реальності
- Augmented Reality Privacy Breach Attack Analysis – аналіз атак на порушення приватності в доповненій реальності
- Authentication – автентифікація
- Authentication Bypass – обхід автентифікації
- Authentication Bypass Attack Analysis – аналіз атак на обхід автентифікації
- Authentication Management Strategies – стратегії управління автентифікацією
- Authenticity – справжність, автентичність

- Authorization – авторизація
- Automated Attack Detection Strategies – стратегії автоматичного виявлення атак
- Automatic Patching – автоматичне виправлення вразливостей
- Automatic Patching Attack Analysis – аналіз атак на автоматичне виправлення вразливостей
- Autonomous Vehicle Protection – захист автономних транспортних засобів
- Autonomous Vehicle Technology System Protection – захист систем технології автономних транспортних засобів
- Availability – доступність
- Aviation and Air Traffic Control Security System Protection – захист систем безпеки авіації та управління повітряним рухом
- Award-winning Device Protection – нагороджений захист пристроїв (преміальний захист)
- Awareness – обізнаність, поінформованість

B

- Backdoor – задні хвіртка, бекдор
- Backup – резервне копіювання, бекап
- Backup Data Recovery – відновлення даних з резервної копії
- Banking Application Privacy Breach Attack Analysis – аналіз атак на порушення приватності банківських додатків
- Banking Fraud Attack Analysis – аналіз атак банківського шахрайства
- Banking Fraud Attack Handling Strategies – стратегії обробки атак банківського шахрайства
- Banking Network Protection – захист банківської мережі
- Banking System Breach Attack Handling Strategies – стратегії обробки атак на порушення банківських систем

- Bare-Metal Computing Privacy Breach Attack Analysis – аналіз атак на порушення приватності при роботі на апаратному залізі (bare-metal)
- Behavioral Analysis – аналіз поведінки
- Behavioral Security Analysis – аналіз поведінкової безпеки
- Big Data Analytics System Breach Attack Analysis – аналіз атак на порушення систем аналітики великих даних
- Big Data Security – безпека великих даних
- Big Data Security Strategies – стратегії безпеки великих даних
- Binary Authentication – бінарна автентифікація
- Biological Hacking Protection Techniques – методи захисту від біологічного хакерства
- Biometric Access Protection – біометричний захист доступу
- Biometric Data Security – безпека біометричних даних
- Biometric Device Protection – захист біометричних пристроїв
- Biometric Sensor Privacy Breach Attack Analysis – аналіз атак на порушення приватності біометричних сенсорів
- Biometrics – біометрика
- Biotechnology and Pharmaceuticals Technology System Protection – захист систем технології біотехнологій та фармацевтики
- Biotechnology Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління біотехнологіями
- Black hat hacker – чорний капелюх хакер (злочинний хакер)
- Blacklisting – чорний список / внесення до чорного списку
- Blackout Attack Handling Strategies – стратегії обробки атак на відключення енергії (блэкаут)
- Blockchain System Breach Attack Handling Strategies – стратегії обробки атак на порушення блокчейн-систем
- Blockchain-Based System Protection – захист систем на основі блокчейну

- Blockchain-based Virtual Network Protection – захист віртуальної мережі на основі блокчейну
- Bluetooth Privacy Breach Attack Analysis – аналіз атак на порушення приватності Bluetooth
- Botnet – ботмережа (зомбі-мережа)
- Brain-Computer Interface Device Breach Attack Handling Strategies – стратегії обробки атак на порушення пристроїв інтерфейсу "мозок-комп'ютер"
- Brute-force attack – атака грубої сили (перебір)
- Buffer Overflow Attack Analysis – аналіз атак на переповнення буфера
- Buffer Overflow Protection – захист від переповнення буфера
- Bug – вада (баг)
- Building Control System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем контролю будівель
- Business and Enterprise Technology System Protection – захист систем бізнес- та корпоративних технологій
- Bypass Attack Handling Strategies – стратегії обробки атак на обхід захисту
- Bypassing Security – обхід заходів безпеки

C

Cache Poisoning – отруєння кешу

Caching Server Protection – захист серверів кешування

Call Tracking Attack Analysis – аналіз атак на відстеження дзвінків

Camera Breach Attack Handling Strategies – стратегії обробки атак на порушення захисту камер

Capability – здатність, можливість (у безпеці)

Card Cloning Attack Analysis – аналіз атак клонування карток

Carding – кардинг (шахрайство з платіжними картками)

Certificate – сертифікат

Certificate Authority (CA) – центр сертифікації (ЦС)

Chain of Custody – ланцюжок збереження доказів

Challenge-Response – виклик-відповідь

Character Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання символів

Checksum – контрольна сума

Child Protection from Cyber Threats – захист дітей від кіберзагроз

Cipher – шифр

Ciphertext – шифротекст

Click Fraud Protection Strategies – стратегії захисту від клікового шахрайства

Clickjacking – клікджекинг (підміна кліків)

Client – клієнт

Climate Control and HVAC System Protection – захист систем контролю клімату та вентиляції (HVAC)

Cloning Attack Handling Strategies – стратегії обробки атак клонування

Cloud Application Protection – захист хмарних додатків

Cloud Application Security Enhancement – підвищення безпеки хмарних додатків

Cloud Computing Privacy Breach Attack Analysis – аналіз атак на порушення приватності хмарних обчислень

Cloud Data Protection – захист хмарних даних

Cloud Data Security – безпека даних у хмарі

Cloud Hacking Attack Handling Strategies – стратегії обробки хакерських атак на хмарні системи

Cloud Infrastructure Protection – захист хмарної інфраструктури

Cloud Malware Attack Handling Strategies – стратегії обробки хмарних атак шкідливого ПЗ

Cloud Security – хмарна безпека

Cloud Services Privacy Breach Attack Analysis – аналіз атак на порушення приватності хмарних сервісів

Cloud Services Protection – захист хмарних сервісів

Cloud Storage Security – безпека хмарного сховища

Cloud System Protection – захист хмарних систем

Cloud-based Network Protection – захист мережі на основі хмари

Cloud-based Security System Building – побудова хмарної системи безпеки

Cloud-based Software Protection – захист програмного забезпечення на основі хмари

Cloud-connected Device Protection – захист пристроїв, під'єднаних до хмари

Cluster – кластер

Code Execution Attack Handling Strategies – стратегії обробки атак на виконання коду

Code Signing – підписання коду

Cold Storage – холодне сховище (для ключів)

Collision – колізія

Combined arms – застосування різнорідних сил (об'єднання родів військ)

Command and Control (C&C, C2) – командування та управління (сервер)

Communication Network Security – безпека мереж зв'язку

Communication Protection – захист зв'язку (комунікацій)

Community Health Protection – захист здоров'я спільноти (в кіберконтексті)

Compartmentalization – компартменталізація (розділення)

Compliance – відповідність вимогам (комплаєнс)

Compliance Enforcement – забезпечення дотримання вимог (комплаєнс)

Comprehensive Security Management – комплексне управління безпекою

Compromised User Accounts – скомпрометовані облікові записи

Computer Emergency Response Team (CERT) – група реагування на комп'ютерні надзвичайні події (CERT)

Computer Forensics – комп'ютерна криміналістика

Computer Hardening – загартування (підвищення стійкості) комп'ютерних систем

Computer virus – комп'ютерний вірус

Confidentiality – конфіденційність

Configuration Management – управління конфігурацією

Connected Car Cybersecurity Protection – кібербезпека підключених автомобілів

Consent – згода

Construction and Infrastructure Sustainability Technology System Protection – захист систем технології сталості будівництва та інфраструктури

Container Security – безпека контейнерів

Containment – стримування (інциденту)

Continuous Monitoring – постійний моніторинг

Contract Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління контрактами

Control – контроль, керування

Cookie – кукі (файл cookie)

Core System Protection – захист ядра системи

Counter-battery fire – контрбатарейна боротьба

Countermeasure – контрзасіб

Credential – облікові дані

Credential Harvesting – збір облікових даних

Credential Stuffing – підбір облікових даних (credential stuffing)

Crimeware – кримінальне ПЗ

Critical Infrastructure Protection (CIP) – захист критичної інфраструктури

Critical Infrastructure Threat Analysis – аналіз загроз критичній інфраструктурі

Critical Systems Protection – захист критичних систем

Cross-Site Request Forgery (CSRF) – міжсайтова підробка запиту

Cross-Site Scripting (XSS) – міжсайтовий скриптинг

Cryptanalysis – криптоаналіз

Cryptoasset – криптоактив

Cryptography – криптографія

Cryptojacking – криптоджекинг (несанкціонований майнінг)

Cryptomining – криптомайнінг

Cryptovirus – криповірус

Custom Software Protection – захист спеціалізованого програмного забезпечення

Customer Knowledge Protection – захист знань про клієнтів

Customer Relationship Management (CRM) Privacy Breach Attack Handling Strategies – стратегії обробки атак на порушення приватності в системах управління взаємовідносинами з клієнтами (CRM)

Customer Relationship Management (CRM) System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління взаємовідносинами з клієнтами (CRM)

Cyber attack – кібератака

Cyber Crimes – кіберзлочини

Cyber Defense Strategies – стратегії кібероборони

Cyber espionage – кібершпигунство

Cyber Fraud Management Strategies – стратегії управління кібершахрайством

Cyber Fraud Protection Strategies – стратегії захисту від кібершахрайства

Cyber Hijacking Attack Handling Strategies – стратегії обробки кібератак на захоплення контролю

Cyber hygiene – кібергігієна

Cyber Incident Response Strategies – стратегії реагування на кіберинциденти

Cyber Proactive Strategies – проактивні кіберстратегії

Cyber Risk Assessment – оцінка кіберризиків

Cyber Risk Management – управління кіберризиками

Cyber Stalking Attack Handling Strategies – стратегії обробки кіберпереслідування

Cybercrime – кіберзлочинність

Cybersecurity Big Data Analytics – аналіз великих даних у кібербезпеці

Cybersecurity Monitoring – моніторинг кібербезпеки

Cybersecurity Solutions for Endpoints – рішення з кібербезпеки для кінцевих точок

Cybersecurity Solutions for Small and Medium Enterprises – рішення з кібербезпеки для малого та середнього бізнесу

Cybersecurity Threats – загрози кібербезпеки

D

- Damage Mitigation – пом'якшення наслідків пошкоджень
- Darknet Attack Handling Strategies – стратегії обробки атак через темну мережу (даркнет)
- Data – дані
- Data Backups – резервні копії даних
- Data Breach – витік даних, порушення захисту даних
- Data Breach Handling Strategies – стратегії обробки витоків даних
- Data Cloning Attack Handling Strategies – стратегії обробки атак клонування даних
- Data Encryption – шифрування даних
- Data Exfiltration – вивіз даних
- Data Exfiltration Attack Analysis – аналіз атак на вивіз даних
- Data Injection Attack Analysis – аналіз атак на ін'єкцію даних
- Data Integrity – цілісність даних
- Data Lake – озеро даних
- Data Leakage – витік даних

- Data Leakage Analysis – аналіз витоку даних
- Data Leakage Attack Handling Strategies – стратегії обробки атак на витік даних
- Data Leakage Prevention (DLP) – запобігання витоку даних (DLP)
- Data Loss Prevention (DLP) – запобігання втраті даних
- Data Masking – маскування даних
- Data Mining – видобування даних
- Data Privacy – приватність даних
- Data Recovery – відновлення даних
- Data Security – безпека даних
- Database – база даних
- Database Attack Analysis – аналіз атак на бази даних
- Database Encryption – шифрування бази даних
- Database Protection – захист баз даних
- Database Security – безпека баз даних
- Dating Application Privacy Breach Attack Analysis – аналіз атак на порушення приватності додатків для знайомств
- DDoS Attack (Distributed Denial of Service Attack) – розподілена атака типу "відмова в обслуговуванні" (DDoS-атака)
- DDoS Mitigation – пом'якшення DDoS-атак
- DDOS Attack Analysis – аналіз DDoS-атак
- Decryption – дешифрування
- Defense and Security System Protection – захист оборонних та безпекових систем
- Defense in Depth – захист в глибину
- Demilitarized Zone (DMZ) – демілітаризована зона (DMZ)
- Denial of Service (DoS) Attack – атака типу "відмова в обслуговуванні"
- Denial of Service (DoS) Attacks – атаки типу "відмова в обслуговуванні"

- Denial of Service Attack Analysis – аналіз атак типу "відмова в обслуговуванні"
- Denial of Service Attack Handling Strategies – стратегії обробки атак типу "відмова в обслуговуванні"
- Depth Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання глибини
- Deserialization Attack – атака десеріалізації
- Detection – виявлення
- Device – пристрій
- Device Control System Breach Attack Analysis – аналіз атак на порушення систем контролю пристроїв
- Device Hardening – загартування пристрою
- Device Hardening Attack Handling Strategies – стратегії обробки атак на загартування пристроїв
- Digital Asset – цифровий актив
- Digital Asset Management Software Protection – захист ПЗ для управління цифровими активами
- Digital Asset Protection – захист цифрових активів
- Digital Assistant Security – безпека цифрових помічників
- Digital Banking Breach Attack Handling Strategies – стратегії обробки атак на порушення цифрових банківських систем
- Digital Certificate – цифровий сертифікат
- Digital Certificate Management – управління цифровими сертифікатами
- Digital Certificate Management Strategies – стратегії управління цифровими сертифікатами
- Digital Certificate Preservation – збереження цифрових сертифікатів
- Digital Cloning Attack Handling Strategies – стратегії обробки атак цифрового клонування

- Digital Document Protection – захист цифрових документів
- Digital Education System Protection – захист цифрових освітніх систем
- Digital Employee Rights – цифрові права працівників
- Digital Financial System Protection – захист цифрових фінансових систем
- Digital Forensics – цифрова криміналістика
- Digital Healthcare System Protection – захист цифрових систем охорони здоров'я
- Digital Identity – цифрова ідентичність
- Digital Identity Protection – захист цифрової ідентичності
- Digital Identity Theft Attack Analysis – аналіз атак на крадіжку цифрової ідентичності
- Digital Ransom Attack Analysis – аналіз цифрових атак з вимаганням викупу
- Digital Ransomware Attack Handling Strategies – стратегії обробки цифрових атак шантажного ПЗ
- Digital Signature – цифровий підпис
- Digital Theft Attack Analysis – аналіз атак цифрової крадіжки
- Digital Transformation Protection – захист цифрової трансформації
- Digital Wallet Application Privacy Breach Attack Analysis – аналіз атак на порушення приватності додатків цифрового гаманця
- Digital Wallet Security – безпека цифрового гаманця
- Direct Penetration Attack Analysis – аналіз атак прямого проникнення
- Disaster Data Recovery – відновлення даних після катастрофи
- Disaster Recovery – відновлення після катастрофи, аварійне відновлення
- Disaster Recovery Strategies – стратегії аварійного відновлення
- Disaster System Recovery – відновлення системи після катастрофи

- Disclosure – розкриття (інформації)
- Distributed Network Protection – захист розподіленої мережі
- DNS (Domain Name System) – система доменних імен
- DNS Amplification – DNS-посилення (атака)
- DNS Hijacking – викрадення DNS
- DNS Spoofing – підробка DNS
- Document Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління документами
- Domain – домен
- Domain Generation Algorithm (DGA) – алгоритм генерації доменів (DGA)
- Domain Hijacking – захоплення домену
- DoS Attack (Denial of Service Attack) – атака типу "відмова в обслуговуванні" (DoS-атака)
- Doxing – доксінг (розголошення особистої інформації)
- Drive-by Download – завантаження при відвідуванні сайту
- Dropbox Security – безпека Dropbox
- Due Diligence – належне розслідування (у безпеці)
- Dump – дамп (даних, пам'яті)
- Dumpster Diving – пошук у смітті (в контексті інформації)
- Dynamic Analysis – динамічний аналіз
- Dynamic Threat Analysis Strategies – стратегії динамічного аналізу загроз

E

- Early Attack Detection Strategies – стратегії раннього виявлення атак
- Early Intrusion Detection – раннє виявлення вторгнень
- Eavesdropping – підслуховування
- Eavesdropping Attack Handling Strategies – стратегії обробки атак підслуховування

- E-commerce – електронна комерція
- E-commerce Application Privacy Breach Attack Analysis – аналіз атак на порушення приватності додатків електронної комерції
- E-commerce Breach Attack Handling Strategies – стратегії обробки атак на порушення систем електронної комерції
- E-commerce Payment Security – безпека електронних платежів
- E-commerce Platform Protection – захист платформ електронної комерції
- E-commerce Privacy Breach Attack Handling Strategies – стратегії обробки атак на порушення приватності в електронній комерції
- E-commerce Protection – захист електронної комерції
- Edge Computing Security – безпека периферійних обчислень (edge computing)
- Effective Response Strategies to Attacks – ефективні стратегії реагування на атаки
- E-Fraud Attack Handling Strategies – стратегії обробки атак електронного шахрайства
- Egress Filtering – фільтрація вихідного трафіку
- E-health Privacy Breach Attack Handling Strategies – стратегії обробки атак на порушення приватності в електронній охороні здоров'я
- E-Learning System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем електронного навчання
- Electronic Banking Fraud Attack Analysis – аналіз атак електронного банківського шахрайства
- Electronic Fraud Attack Analysis – аналіз атак електронного шахрайства
- Electronic Fraud Attack Handling Strategies – стратегії обробки атак електронного шахрайства
- Electronic Gaming Application Privacy Breach Attack Analysis – аналіз атак на порушення приватності додатків електронних ігор

- Electronic Health Data System Protection – захист систем електронних медичних даних
- Electronic Payment System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем електронних платежів
- Electronic Payments Security – безпека електронних платежів
- Elevator Control Device Breach Attack Handling Strategies – стратегії обробки атак на порушення пристроїв контролю ліфтів
- Email – електронна пошта
- Email Breach Attack Analysis – аналіз атак на порушення безпеки електронної пошти
- Email Exploitation Attack Handling Strategies – стратегії обробки атак з використанням електронної пошти
- Email Penetration Attack Analysis – аналіз атак на проникнення через електронну пошту
- Email Protection – захист електронної пошти
- Email Security – безпека електронної пошти
- Email Spam Filtering – фільтрація спаму в електронній пошті
- Embedded OS Breach Attack Analysis – аналіз атак на порушення вбудованих операційних систем
- Embedded Operating System Breach Attack Analysis – аналіз атак на порушення вбудованих операційних систем
- Embedded Software Protection – захист вбудованого програмного забезпечення
- Embedded System Breach Attack Analysis – аналіз атак на порушення вбудованих систем
- Embedded Systems Protection – захист вбудованих систем
- Emergency Response Plan – план дій у надзвичайних ситуаціях
- Emerging Cyber Piracy Attack Handling Strategies – стратегії обробки нових кіберпіратських атак

- Emerging Hacking Attack Handling Strategies – стратегії обробки нових хакерських атак
- Emerging Technology Trends – новітні технологічні тенденції
- Emerging Threats Handling Strategies – стратегії реагування на новітні загрози
- Employee Data Protection – захист даних співробітників
- Encrypted Communication – зашифрований зв'язок
- Encrypted Communications Protection – захист зашифрованого зв'язку
- Encrypted Data Storage – зашифроване зберігання даних
- Encryption – шифрування
- Encryption Attack Analysis – аналіз атак на шифрування
- Encryption Security – безпека шифрування
- Encryption System – система шифрування
- Endpoint – кінцева точка
- Endpoint Detection and Response (EDR) – виявлення та реагування на кінцевих точках (EDR)
- Endpoint Protection – захист кінцевих точок
- Endpoint Security Policy Rules – правила політики безпеки кінцевих точок
- Energy and Power Control System Protection – захист систем контролю енергії та електропостачання
- Energy and Renewable Energy Technology System Protection – захист систем технології енергетики та відновлюваної енергетики
- Energy Ecosystem Security – безпека енергетичної екосистеми
- Energy System Protection – захист енергетичних систем
- Enigma – Енігма (історичний шифр)
- Enterprise – підприємство
- Enterprise Core System Protection – захист ключових систем підприємств

- Enterprise Infrastructure Protection – захист інфраструктур підприємств
- Enterprise Network Breach Attack Analysis – аналіз атак на порушення корпоративних мереж
- Enterprise Network Protection – захист корпоративної мережі
- Entertainment System Protection – захист розважальних систем
- Environment and Intelligent Transportation Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління навколишнім середовищем та розумним транспортом
- Environmental System Protection – захист екологічних систем
- Ergonomics – ергономіка (у безпеці інтерфейсу)
- Escalation – ескалація (привілеїв, інциденту)
- Espionage – шпигунство
- Espionage Attack Analysis – аналіз атак шпигунства
- Ethical Hacking – етичний хакінг
- Ethical Hacking Attack Analysis – аналіз атак етичного хакінгу
- Evasion – ухилення
- Evasion and Obfuscation Attack Analysis – аналіз атак на ухилення та обфускацію
- Event – подія
- Event Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління подіями
- Evidence – доказ
- Exfiltration – вивіз (даних)
- Exploit – експлойт, засоби використання вразливості
- Exploit Attack Handling Strategies – стратегії обробки атак з використанням вразливостей
- Exploit Attack Patterns – шаблони атак з використанням вразливостей
- Exploit Template Analysis – аналіз шаблонів експлойтів

- Exploitation – експлуатація (вразливостей)
- Exposure – експозиція, вплив, розкриття
- Extended Detection and Response (XDR) – розширене виявлення та реагування (XDR)
- External Network Security – безпека зовнішніх мереж
- Extortion – вимагання

F

- Face Cloning Attack Handling Strategies – стратегії обробки атак клонування обличчя
- Facial Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання обличчя
- Facility Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління об'єктами
- Failover – перемикання на резерв
- Fail-Safe – відмовостійкість
- Fail-Secure – забезпечення безпеки при відмові
- False Positive – хибнопозитивний результат
- False Threats – хибні загрози
- Farm Security – безпека ферм (серверних, IoT)
- Fast Response Strategies to Threats – стратегії швидкого реагування на загрози
- Fault Tolerance – відмовостійкість
- Federated Identity – федеративна ідентичність
- File Integrity Monitoring (FIM) – моніторинг цілісності файлів
- File Protection – захист файлів
- File Sharing Protection – захист спільного доступу до файлів
- File Transfer Attack Handling Strategies – стратегії обробки атак на передачу файлів
- File Transfer Protocol (FTP) Security – безпека FTP

- Financial Fraud Attack Handling Strategies – стратегії обробки атак фінансового шахрайства
- Financial Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення фінансових систем управління
- Financial Revenue Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління фінансовими надходженнями
- Fingerprint Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання відбитків пальців
- Firewall – міжмережевий екран, брандмауер
- Firewall Protection – захист брандмауера (межового екрана)
- Firewall Rules – правила брандмауера
- Firmware – прошивка, мікропрограмне забезпечення
- Firmware Security – безпека прошивок
- Firmware Update – оновлення прошивки
- Fitness Tracker Breach Attack Handling Strategies – стратегії обробки атак на порушення фітнес-трекерів
- Flaming Attack Analysis – аналіз атак "полум'я" (флеймінгу)
- Flooding Attack – атака затоплення (трафіком)
- Fog Computing Security – безпека туманних обчислень (Fog Computing)
- Food Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління харчуванням
- Footprinting – знімок (інформації про систему)
- Forensic Analysis – криміналістичний аналіз
- Forensic Tools – інструменти для криміналістики
- Forgery – підробка
- Fraud – шахрайство
- Fraud Detection – виявлення шахрайства
- Fraud Prevention – запобігання шахрайству

- Fuel System Protection – захист паливних систем
- Full Disk Encryption (FDE) – повне шифрування диска
- Fuzz Testing – фазз-тестування (тестування на спотворення)

G

- Gait Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання ходи
- Gaming Console Breach Attack Analysis – аналіз атак на порушення ігрових консолей
- Gaming Infrastructure Protection – захист ігрової інфраструктури
- Gateway – шлюз
- GDPR (General Data Protection Regulation) – Загальний регламент захисту даних (GDPR)
- Geolocation Tracking Privacy Breach Attack Analysis – аналіз атак на порушення приватності через відстеження геолокації
- Geofencing – геозонування
- Global Security Analysis – глобальний аналіз безпеки
- Governance Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем корпоративного управління
- Government System Breach Attack Handling Strategies – стратегії обробки атак на порушення урядових систем
- Graphical Password – графічний пароль
- Gray Hat Hacker – сірий капелюх хакер
- Greyware – сіре ПЗ (grayware)
- Guard – захисний засіб, варта
- Guideline – керівний принцип, рекомендація

H

- Hacking – хакерство, несанкціонований доступ

- Hacking Attacks – хакерські атаки
- Handwriting Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання почерку
- Hardening – загартовування, підвищення стійкості
- Hardware – апаратне забезпечення
- Hardware Protection – захист апаратного забезпечення
- Hardware Security Module (HSM) – апаратний модуль безпеки (HSM)
- Hash – геш, хеш-сума
- Hashing – хешування
- Header – заголовок
- Health Insurance Portability and Accountability Act (HIPAA) – Закон про переносимість та підзвітність медичного страхування (HIPAA)
- Heuristic Analysis – евристичний аналіз
- HIDS (Host-based Intrusion Detection System) – система виявлення вторгнень на основі хоста
- HIPS (Host-based Intrusion Prevention System) – система запобігання вторгненням на основі хоста
- Honeypot – пастка (honeypot)
- Home Automation Control System Protection – захист систем контролю домашньої автоматизації
- Home Automation System Breach Attack Analysis – аналіз атак на порушення систем домашньої автоматизації
- Home Electrical System Protection – захист систем домашнього електропостачання
- Home Network Device Breach Attack Handling Strategies – стратегії обробки атак на порушення пристроїв домашньої мережі
- Home System Protection – захист домашніх систем
- Hopper – хопер (для email-спаму)

- Hospital and Healthcare System Protection – захист лікарняних та медичних систем
- Host – хост, вузол
- Hotel Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління готелями
- Human Firewall – людський брандмауер (обізнаність співробітників)
- Human Resources Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління людськими ресурсами (HR)
- Hybrid Application Protection – захист гібридних додатків
- Hybrid Attack Prevention Strategies – стратегії запобігання гібридним атакам
- Hybrid Attack Protection Strategies – стратегії захисту від гібридних атак
- Hybrid Cloud Security – безпека гібридної хмари
- Hybrid Cloning Attack Handling Strategies – стратегії обробки гібридних атак клонування
- Hybrid Threat – гібридна загроза
- Hypervisor – гіпервізор
- Hypervisor Security – безпека гіпервізора

I

Identity and Access Management (IAM) – управління ідентичністю та доступом (IAM)

Identity and Access Management (IAM) управління ідентичністю та доступом (IAM)

Identity Assurance Technology Privacy Breach Attack Analysis – аналіз атак на порушення приватності технологій підтвердження особи

Identity Assurance Technology Privacy Breach Attack Analysis аналіз атак на порушення приватності технологій підтвердження особи

Identity Fraud Attack Handling Strategies – стратегії обробки атак на шахрайство з ідентичністю

Identity Fraud Attack Handling Strategies стратегії обробки атак на шахрайство з ідентичністю

Identity Protection – захист ідентичності

Identity Protection захист ідентичності

Identity Protection захист ідентичності

Identity Theft – крадіжка ідентичності

Identity Theft Attack Analysis – аналіз атак на крадіжку ідентичності

Identity Theft Attack Analysis аналіз атак на крадіжку ідентичності

Identity Theft Attack Handling Strategies – стратегії обробки атак на крадіжку ідентичності

Identity Theft Attack Handling Strategies стратегії обробки атак на крадіжку ідентичності

Identity Theft крадіжка ідентичності

Identity Theft крадіжка ідентичності

Identity Verification – верифікація особи (підтвердження особистості)

Identity Verification верифікація особи (підтвердження особистості)

Identity Verification верифікація особи (підтвердження особистості)

Identity Verification верифікація особи (підтвердження особистості)

Image Cloning Attack Handling Strategies – стратегії обробки атак клонування зображень

Image Cloning Attack Handling Strategies стратегії обробки атак клонування зображень

Image Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання зображень

Image Recognition Privacy Breach Attack Analysis аналіз атак на порушення приватності через розпізнавання зображень

Imaging and Camera Technology System Protection – захист систем технології візуалізації та камер

Imaging and Camera Technology System Protection захист систем технології візуалізації та камер

Incident Analysis – аналіз інцидентів

Incident Analysis аналіз інцидентів

Incident Analysis аналіз інцидентів

Incident Monitoring and Security Investigations – моніторинг інцидентів та розслідування в безпеці

Incident Monitoring and Security Investigations моніторинг інцидентів та розслідування в безпеці

Incident Response – реагування на інциденти

Incident Response реагування на інциденти

Incident Response реагування на інциденти

Incident Response реагування на інциденти

Industrial Automation System Protection – захист систем промислової автоматизації

Industrial Automation System Protection захист систем промислової автоматизації

Industrial Control System Breach Attack Analysis – аналіз атак на порушення систем промислового контролю

Industrial Control System Breach Attack Analysis аналіз атак на порушення систем промислового контролю

Industrial Control Systems Protection – захист систем промислового контролю

Industrial Control Systems Protection захист систем промислового контролю

Industrial Control Systems Security – безпека систем промислового контролю

Industrial Control Systems Security безпека систем промислового контролю

Industrial Cybersecurity Technology System Protection – захист систем технології промислової кібербезпеки

Industrial Cybersecurity Technology System Protection захист систем технології промислової кібербезпеки

Industrial IoT Infrastructure Protection – захист інфраструктури промислового Інтернету речей

Industrial IoT Infrastructure Protection захист інфраструктури промислового Інтернету речей

Industrial Network Protection – захист промислових мереж

Industrial Network Protection захист промислових мереж

Industrial Network Protection захист промислових мереж

Industrial Process System Protection – захист систем промислових процесів

Industrial Process System Protection захист систем промислових процесів

Industrial Systems Protection – захист промислових систем

Industrial Systems Protection захист промислових систем

Information Leakage Attack Handling Strategies – стратегії обробки аток на витік інформації

Information Leakage Attack Handling Strategies стратегії обробки аток на витік інформації

Information Phishing Attack Analysis – аналіз атак фішингу інформації

Information Phishing Attack Analysis аналіз атак фішингу інформації

Information Retrieval – пошук / отримання інформації

Information Retrieval пошук / отримання інформації

Information Retrieval пошук / отримання інформації

Information Retrieval пошук інформації / отримання інформації

Information Technology in Cybersecurity – інформаційні технології в кібербезпеці

Information Technology in Cybersecurity інформаційні технології в кібербезпеці

Information Technology Infrastructure Protection – захист інфраструктури інформаційних технологій

Information Technology Infrastructure Protection захист інфраструктури інформаційних технологій

Infrastructure Attacker Analysis – аналіз атакуючого інфраструктури

Infrastructure Attacker Analysis аналіз атакуючого інфраструктури

Insider Threat Protection – захист від внутрішніх загроз

Insider Threat Protection захист від внутрішніх загроз

Instant Messaging Application Privacy Breach Attack Analysis

Instant Messaging Application Privacy Breach Attack Analysis аналіз атак на порушення приватності додатків миттєвих повідомлень

Instant Messaging Application Privacy Breach Attack Analysis аналіз атак на порушення приватності додатків миттєвих повідомлень

Insurance System Breach Attack Handling Strategies стратегії обробки атак на порушення страхових систем

Interactive Screen Security безпека інтерактивних екранів

Interface Hijacking Attack Handling Strategies стратегії обробки атак на захоплення інтерфейсів

Internal Device Protection захист внутрішніх пристроїв

Internal Intrusion Handling Strategies стратегії обробки внутрішніх вторгнень

Internal Threat Attack Analysis аналіз атак внутрішніх загроз

Internal Threat внутрішня загроза

Internal Threat внутрішня загроза

Internal Threat внутрішня загроза

International Organization Cyber Attacks Protection захист міжнародних організацій від кібератак

Internet Connection Security безпека інтернет-з'єднання

Internet Connection Security безпека інтернет-з'єднання

Internet Hijacking Attack Analysis аналіз атак на захоплення інтернет-трафіку

Internet of Things (IoT) Device Network Breach Attack Analysis аналіз атак на порушення мережі пристроїв Інтернету речей

Internet of Things (IoT) Device System Protectionзахист систем пристроїв Інтернету речей

Internet of Things (IoT) Security безпека Інтернету речей (IoT)

Internet of Things Network Security безпека мережі Інтернету речей

Internet of Things Security безпека інтернету речей

Intrusion Attack Handling Strategies стратегії обробки атак на вторгнення

Intrusion Detection and Prevention (IDPS) виявлення та запобігання вторгненням (IDPS)

Intrusion Detection Privacy Breach Attack Analysis аналіз атак на порушення приватності при виявленні вторгнень

Intrusion Detection Strategies стратегії виявлення вторгнень

Intrusion Detection виявлення вторгнень

Intrusion Detection виявлення вторгнень

Intrusion Detection виявлення вторгнень

Intrusion Prevention запобігання вторгненням

Intrusion Prevention запобігання вторгненням

Intrusion Risk Management Strategies стратегії управління ризиками вторгнень

Inventory Management System Breach Attack Handling Strategies стратегії обробки атак на порушення систем управління запасами

IoT Device Security безпека пристроїв Інтернету речей (IoT)

IoT Infrastructure Protection захист інфраструктури Інтернету речей

IoT Network Protection захист мережі Інтернету речей

IoT Network Protection захист мережі Інтернету речей (IoT)

IoT Network Security безпека мережі Інтернету речей

IPTV Privacy Breach Attack Analysis аналіз атак на порушення приватності IPTV

Iris Recognition Privacy Breach Attack Analysis аналіз атак на порушення приватності через розпізнавання райдужної оболонки

Iris Recognition Privacy Breach Attack Analysis аналіз атак на порушення приватності через розпізнавання райдужної оболонки

J

- Jailbreak (джейлбрейк, злом захисту ОС)

Jamming Attack Analysis аналіз атак на радіозаглушення (джаммінг)

- JavaScript injection (ін'єкція JavaScript)
- Job scheduler attack (атака через планувальник завдань)
- Joint cyber operation (спільна кібероперація)
- Journaling (журналювання, ведення журналу подій)
- JPA (Java Persistence API, можлива точка атаки)
- JRE (Java Runtime Environment, середовище виконання Java)
- JTRIG (Joint Threat Research Intelligence Group)
- Judgmental forecasting (експертне прогнозування загроз)
- Junction (точка з'єднання, можлива вразливість)
- Just-in-Time Compilation (JIT-компіляція, вектор атаки)
- Just-in-Time Exploitation (експлуатація в момент завантаження)
- Juvenile hacker (неповнолітній хакер)

K

- K-anonymity – k-анонімність

- Kerberos – протокол Kerberos
- Kernel – ядро (операційної системи)
- Kernel Exploit – експлойт ядра
- Kernel-level Rootkit – руткіт рівня ядра
- Key – ключ
- Key Clustering – кластеризація ключів
- Key Derivation Function (KDF) – функція виведення ключа
- Key Escrow – депонування ключів
- Key Exchange – обмін ключами
- Key Fingerprint – відбиток ключа
- Key Generation – генерація ключів
- Key Logger / Keylogger – кейлогер
- Key Management – управління ключами
- Key Pair – пара ключів
- Key Recovery – відновлення ключа
- Key Schedule – розклад ключів
- Key Stretching – розширення ключа
- Key Verification – перевірка ключа
- Keystroke Dynamics – динаміка набору на клавіатурі
- Kill Chain – ланцюг кілерів (модель атаки)
- Kill Disk – знищення диска
- Kill Switch – аварійний вимикач
- Knowledge-based Authentication – аутентифікація на основі знань
- Knowledge Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління знаннями

L

- L2TP (Layer 2 Tunneling Protocol) – протокол тунелювання другого рівня

- Ladder Logic – мова релейної логіки (вразливості SCADA)
- Lambda Function Attack – атака на лямбда-функцію
- LAN (Local Area Network) – локальна мережа
- LAN Penetration Attack Analysis – аналіз атак на проникнення в локальну мережу (LAN)
- Land Attack – атака типу Land
- Language Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання мови
- Laptop Device Breach Attack Analysis – аналіз атак на порушення захисту ноутбуків
- Laptop Hacking Attack Handling Strategies – стратегії обробки хакерських атак на ноутбуки
- Large Enterprise Network Breach Attack Handling Strategies – стратегії обробки атак на порушення мереж великих підприємств
- Lateral Movement – пересування в бок (латеральний рух)
- Layer 2 Attack – атака на другому рівні OSI
- Layer 7 Firewall – файрвол рівня застосунків
- Layered Defense – багаторівнева оборона
- Layered Security – багаторівнева безпека
- Layered Security Analysis – багаторівневий аналіз безпеки
- LDAP (Lightweight Directory Access Protocol) – легкий протокол доступу до каталогів
- LDAP Injection – ін'єкція LDAP
- Leak – витік
- Least Privilege – принцип найменших привілеїв
- Legacy Protocol – застарілий протокол
- Legacy System – успадкована система
- Legal Affairs Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління юридичними справами

- Legal Intercept – легальний перехоплення
- Legal Violation Attack Handling Strategies – стратегії обробки атак, що порушують законодавство
- Let's Encrypt – центр сертифікації Let's Encrypt
- Level of Assurance – рівень гарантії
- Liability in Cybersecurity – відповідальність у кібербезпеці
- Library Hijacking – перехоплення бібліотеки
- Library Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління бібліотеками
- Lifecycle Management – управління життєвим циклом
- Li-Fi Security – безпека Li-Fi
- Lighting Control System Privacy Breach Attack Analysis – аналіз атак на порушення приватності систем контролю освітлення
- Lightweight Cryptography – легка криптографія
- Link – посилання, зв'язок
- Link Layer Security – безпека на рівні ланки
- Live Data Protection – захист живих (активних) даних
- Live Forensic Analysis – живий форензичний аналіз
- Living Technology Breach Attack Handling Strategies – стратегії обробки атак на порушення технологій "розумного" життя
- Loader – завантажувач (компонент шкідливого ПЗ)
- Local Area Network (LAN) Security – безпека локальної мережі
- Local File Inclusion (LFI) – включення локального файлу
- Local Privilege Escalation (LPE) – підвищення привілеїв локально
- Local Wireless Network Protection – захист локальної бездротової мережі
- Lock – блокування, замок

- Lockout Policy – політика блокування облікового запису
- Log – журнал (подій), лог
- Log Analysis – аналіз журналів подій
- Log Forging – підробка журналів
- Log Management – управління журналами
- Logic Bomb – логічна бомба
- Logic Flaw – логічна вразливість
- Logic Gate Manipulation – маніпуляція логічними вентилями
- Login – вхід в систему
- Logistics Systems Protection – захист логістичних систем
- Logistics Transportation System Breach Attack Handling Strategies – стратегії обробки атак на порушення логістичних транспортних систем
- Longitudinal Study – лонгітюдне дослідження загроз
- LoRaWAN Security – безпека LoRaWAN
- Low and Slow Attack – повільна атака
- Low-Power Device Infrastructure Protection – захист інфраструктури малопотужних пристроїв
- Lure – приманка (у соціальній інженерії)

M

- MAC Address Spoofing – спуфінг MAC-адреси
- MAC Flooding – затоплення MAC-таблиці
- Machine Learning in Cybersecurity – машинне навчання в кібербезпеці
- Macro Virus – макровірус
- Mail Server Security – безпека поштового сервера
- Main-in-the-Middle Attack (MitM) – атака "людина посередині"
- Maintenance Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління технічним обслуговуванням

- Malicious Activity – шкідлива активність
- Malicious Agent – шкідливий агент
- Malicious Apps Handling Strategies – стратегії обробки шкідливих додатків
- Malicious Download – шкідливе завантаження
- Malicious Email Attack Handling Strategies – стратегії обробки атак зі шкідливою електронною поштою
- Malicious Email Protection Strategies – стратегії захисту від шкідливої електронної пошти
- Malicious Exploit Attack Analysis – аналіз атак з використанням шкідливих експлойтів
- Malicious Link Analysis – аналіз шкідливих посилань
- Malvertising – малвертайзинг, шкідлива реклама
- Malvertising Attack Analysis – аналіз атак зі шкідливою рекламою
- Malware – шкідливе програмне забезпечення
- Malware Analysis – аналіз шкідливого ПЗ
- Malware-as-a-Service (MaaS) – шкідливе ПЗ як послуга
- Malware Attack Analysis – аналіз атак шкідливого ПЗ
- Malware Attack Handling Strategies – стратегії обробки атак шкідливого ПЗ
- Malware Attack Handling Strategies on Smart Devices – стратегії обробки атак шкідливого ПЗ на розумних пристроях
- Malware Detection – виявлення шкідливого ПЗ
- Malware Removal Strategies – стратегії видалення шкідливого ПЗ
- Malware Scanning – сканування на наявність шкідливого ПЗ
- Malware Threat Cloning – клонування загроз шкідливого ПЗ
- Managed Security Service Provider (MSSP) – провайдер керованих послуг безпеки
- Mandatory Access Control (MAC) – обов'язкове управління доступом

- Manually Triggered Backdoor – бекдор з ручним запуском
- Manufacturing System Protection – захист виробничих систем
- MapReduce Security – безпека MapReduce
- Maritime Cybersecurity – морська кібербезпека
- Maritime Transportation System Protection – захист морських транспортних систем
- Markov Chain Model – модель ланцюга Маркова (для загроз)
- Masking – маскування
- Mass Surveillance – масове спостереження
- Master Boot Record (MBR) Infection – інфекція MBR
- Match-on-Card Technology – технологія перевірки на карті
- Medical and Healthcare Devices System Protection – захист систем медичних пристроїв та пристроїв охорони здоров'я
- Medical Biometric Data Protection – захист медичних біометричних даних
- Medical Device Breach Attack Handling Strategies – стратегії обробки атак на порушення захисту медичних пристроїв
- Medical Information Technology Security – безпека медичних інформаційних технологій
- Memory Corruption – пошкодження пам'яті
- Memory Dump – дамп пам'яті
- Memory Forensics – форензика пам'яті
- Memory Scraping – скрейпінг пам'яті
- Memory-safe Language – мова з безпечною пам'яттю
- Mental Pattern Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання психічних шаблонів
- Merkle Tree – дерево Меркла
- Mesh Network Security – безпека mesh-мереж
- Message Authentication Code (MAC) – код автентифікації повідомлення

- Metadata Leakage – витік метаданих
- Metering System Protection – захист систем обліку (лічильників)
- Microarchitectural Attack – мікроархітектурна атака
- Microsegmentation – мікросегментація
- Mimikatz – інструмент Mimikatz
- Mining System Protection – захист гірничодобувних систем
- Misconfiguration – неправильна конфігурація
- Mismatched Protocol – несумісний протокол
- Mobile App Privacy Breach Attack Analysis – аналіз атак на порушення приватності мобільних додатків
- Mobile Communication Device Breach Attack Analysis – аналіз атак на порушення пристроїв мобільного зв'язку
- Mobile Device / Mobile Phone / Smartphone Protection – захист мобільних пристроїв / телефонів / смартфонів
- Mobile Device / Mobile Phone Security – безпека мобільних пристроїв / телефонів
- Mobile Device Management (MDM) – управління мобільними пристроями
- Mobile Device Security – безпека мобільних пристроїв
- Mobile Devices and Wearable Technology System Protection – захист систем мобільних пристроїв та носимих технологій
- Mobile Malware Attack Analysis – аналіз атак мобільного шкідливого ПЗ
- Mobile Network Protection – захист мобільної мережі
- Mobile OS Privacy Breach Attack Analysis – аналіз атак на порушення приватності мобільних операційних систем
- Mobile Payment Application Breach Attack Handling Strategies – стратегії обробки атак на порушення додатків мобільних платежів
- Mobile Phishing Protection – захист від мобільного фішингу

- Mobile Phone Phishing Attack Analysis – аналіз атак мобільного фішингу
- Mobile Phone Privacy Breach Attack Analysis – аналіз атак на порушення приватності мобільних телефонів
- Mobile Threat Defense (MTD) – захист від мобільних загроз
- Mobile Tracking Device Privacy Breach Attack Analysis – аналіз атак на порушення приватності пристроїв мобільного відстеження
- Mobile-based Attack Analysis – аналіз атак на основі мобільних пристроїв
- Modbus Protocol Attack – атака на протокол Modbus
- Model Inversion Attack – атака інверсії моделі
- Monetization of Attacks – монетизація атак
- Monitoring as a Service – моніторинг як послуга
- Motion Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання руху
- Multi-cloud Security – безпека мультихмарного середовища
- Multi-Device Protection – захист на декількох пристроях
- Multi-factor Authentication (MFA) – багатофакторна аутентифікація
- Multilayer Encryption – багаторівневе шифрування
- Multi-layer Network Security – багаторівнева безпека мережі
- Multi-vector Attack – багатовекторна атака

N

- NAC (Network Access Control) – контроль доступу до мережі
- Namespace Attack – атака на простір імен
- National Cyber Strategy – національна кіберстратегія
- Native Code Exploit – експлойт нативного коду
- Natural Language Processing in SIEM – NLP в SIEM
- Near Field Communication (NFC) Attack – атака через NFC

- Nested Virtualization Attack – атака на вкладну віртуалізацію
- Netflow Analysis – аналіз Netflow
- Network Access Quarantine – карантин мережевого доступу
- Network Address Translation (NAT) Traversal – обхід NAT
- Network Analysis – аналіз мережі
- Network and Communication Security System Protection – захист систем безпеки мереж та зв'язку
- Network Behavior Analysis (NBA) – аналіз поведінки мережі
- Network Breach Attack Analysis – аналіз атак на проникнення в мережу
- Network Breach Attack Handling Strategies – стратегії обробки атак на порушення мереж
- Network Deception – мережева децепція
- Network Detection and Response (NDR) – виявлення та реагування в мережі
- Network Evasion and Evasion Attack Analysis – аналіз атак на ухилення та обхід в мережах
- Network Forensics – мережева форензика
- Network Function Virtualization (NFV) Security – безпека NFV
- Network Infrastructure Protection – захист мережевої інфраструктури
- Network Intrusion – проникнення в мережу
- Network Intrusion Prevention System (NIPS) – система запобігання вторгненням у мережу
- Network Log Analysis – аналіз мережевих журналів подій
- Network Mapping – картування мережі
- Network Monitoring – моніторинг мережі
- Network Perimeter – мережевий периметр

- Network Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання мереж
- Network Security – безпека мережі
- Network Security Policy – політика мережевої безпеки
- Network Segmentation – сегментація мережі
- Network Sensor – мережевий сенсор
- Network Server Protection – захист мережевих серверів
- Network Traffic Analysis (NTA) – аналіз мережевого трафіку
- Network Users Behavior Analysis – аналіз поведінки мережевих користувачів
- Network-Based Malware Attack Handling Strategies – стратегії обробки мережевих атак шкідливого ПЗ
- Neural Network for Malware Detection – нейронна мережа для виявлення шкідливого ПЗ
- Neural Networks and Machine Intelligence System Protection – захист систем нейронних мереж та машинного інтелекту
- Never-before-seen Malware – ніколи не бачений зразок шкідливого ПЗ
- New Phishing Management Strategies – стратегії управління новими видами фішингу
- Next-generation Firewall (NGFW) – файрвол нового покоління
- NIST Cybersecurity Framework – кібербезпековий фреймворк NIST
- Node.js Security – безпека Node.js
- No-execute (NX) Bit – біт NX (заборона виконання)
- Nonce – одноразове число
- Non-disclosure Agreement (NDA) in Infosec – угода про нерозголошення в інфобезпеці
- Non-repudiation – неспростовність

- North-south Traffic – трафік "північ-південь"
- NoSQL Injection – ін'єкція NoSQL
- Notes and Tasks Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління нотатками та завданнями
- Notification of Data Breach – сповіщення про витік даних

O

- OAuth Token Hijacking – перехоплення токена OAuth
- Obfuscated Code – обфусцированний код
- Obfuscation – обфускація
- Obfuscator – обфускатор
- Object – об'єкт
- Object Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання об'єктів
- Object-level Security – безпека на рівні об'єктів
- Oblivious RAM (ORAM) – ORAM (схема приховування шаблонів доступу до пам'яті)
- Observability – спостережність
- Observer – спостерігач
- Occupational Safety and Health Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління охороною праці та безпекою
- Occlusion – оклюзія, перешкода
- Off-chain Security – безпека офчейн
- Offense – наступ, напад
- Offensive Security – офенсивна безпека
- Offline – офлайн
- Olfactory Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання запахів
- Omission – упущення, пропуск

- One-time Password (OTP) – одноразовий пароль
- Onion Routing – цибулева маршрутизація
- Online – онлайн
- Online Banking Protection – захист інтернет-банкінгу
- Online Malware Attack Analysis – аналіз онлайн-атак шкідливого ПЗ
- On-path Attacker – атакуючий на шляху
- On-premises Security – безпека локальної інфраструктури
- Opaque – непрозорий
- Opcode – код операції
- Open Port – відкритий порт
- Open Source Encryption Methods – методи шифрування з відкритим кодом
- Open Source Intelligence (OSINT) – розвідка на основі відкритих джерел
- Open Web Application Security Project (OWASP) – проект безпеки веб-додатків
- OpenPGP – стандарт шифрування OpenPGP
- Operand – операнд
- Operating System Fingerprinting – визначення ОС
- Operating System Protection – захист операційної системи
- Operating System Security – безпека операційної системи
- Operator – оператор
- Operator Error – помилка оператора
- Opportunistic – опортуністичний
- Optical Covert Channel – оптичний прихований канал
- Optical Network Infrastructure Security – безпека інфраструктури оптичних мереж
- Opt-out – відмова (від отримання)
- Oracle – оракул (в криптографії)

- Orange Team – оранжева команда
- Orchestration of Attacks – оркестрування атак
- Order – порядок, команда
- Organizational Resilience – організаційна стійкість
- Organized Attack Analysis – аналіз організованих атак
- Organized Attack Threats – загрози організованих атак
- Origin – джерело, походження
- Oscillator – генератор
- OS Command Injection – ін'єкція OS-команд
- OS Hardening – загартовування ОС
- Out-of-band (OOB) Attack – поза-смугова атака
- Out-of-band Authentication – поза-смугова аутентифікація
- Outage – перерва в роботі
- Outbound – вихідний
- Outlier – викид, аномальне значення
- Output Encoding – кодування виводу
- Overflow – переповнення
- Overhead – додаткові витрати
- Overload – перевантаження
- Overprivileged Application – застосунок з надмірними привілеями
- Overrun – перевищення
- Oversight – нагляд
- Over-the-air (OTA) Update Security – безпека OTA-оновлень
- Over-the-shoulder Attack – атака "через плече"
- Override – перевизначення
- Overwrite – перезапис

P

- P2P Botnet – P2P-ботнет
- Package Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання пакетів

- Pack – пакувати, пакунок
- Packet Craft – створення пакетів
- Packet Sniffing – перехоплення пакетів
- Padding – доповнення (padding)
- Padding Oracle Attack – атака Padding Oracle
- Page – сторінка
- Pair – пара
- Pairing Protocol Attack – атака на протокол парування
- Palette – палітра
- Pan-tilt-zoom (PTZ) Camera Hacking – злом PTZ-камер
- Panic – паніка, аварійний режим
- Paradigm – парадигма
- Parallel – паралельний
- Parameter – параметр
- Parasite – паразит
- Parent – батьківський
- Parity – парність
- Parser – парсер
- Partition – розділ, розбиття
- Passive Attack – пасивна атака
- Passive Fingerprinting – пасивне визначення ОС
- Passphrase – пасфраза
- Passport – паспорт (цифровий)
- Password – пароль
- Password Attack – атака на пароль
- Password Cracking – зламування паролів
- Password Entropy – ентропія пароля
- Password Hashing – хешування паролів
- Password Policy – політика паролів
- Password Protection – захист паролів

- Password Salting – соління паролів
- Paste – вставка, паста
- Patch – виправлення, патч
- Patch Exploitation Attack Handling Strategies – стратегії обробки атак з використанням виправлень
- Patch Management – управління патчами
- Patch Tuesday – вівторок патчів
- Path – шлях
- Pattern Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання шаблонів
- Payload – корисне навантаження
- Payment Card Fraud Attack Handling Strategies – стратегії обробки атак шахрайства з платіжними картками
- Payment Card Industry Data Security Standard (PCI DSS) – стандарт безпеки даних індустрії платіжних карток
- Peer – одноранговий вузол, пір
- Pen Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання ручки
- Penalty – штраф, покарання
- Penetration Testing – тестування на проникнення (пентест)
- Perfect Forward Secrecy (PFS) – ідеальна пряма секретність
- Perimeterless Security – безпека без периметра
- Peripheral Device Protection – захист периферійних пристроїв
- Permission & Access Management – управління дозволами та доступом
- Permission Creep – поступове розширення дозволів
- Persistence – персистентність
- Persistence Mechanism – механізм персистентності
- Personal Cloud Computing Privacy Breach Attack Analysis – аналіз атак на порушення приватності персональних хмарних обчислень

- Personal Data Breach – витік персональних даних
- Personal Data Protection – захист персональних даних
- Personal Network Protection – захист персональної мережі
- Personal Network Security – безпека персональної мережі
- Personal Security System Breach Attack Analysis – аналіз атак на порушення персональних систем безпеки
- Personality Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання особистості
- Personally Identifiable Information (PII) – особисто ідентифікована інформація
- Phantom – фантом, привид
- Pharming – фармінг
- Phase – фаза
- Phish – фішити
- Phishing – фішинг
- Phishing Attack Analysis – аналіз фішингових атак
- Phishing Attack Handling Strategies – стратегії обробки фішингових атак
- Phishing Attack Protection Strategies – стратегії захисту від фішингових атак
- Phishing Kit – набір для фішингу
- Phishing Protection Strategies – стратегії захисту від фішингу
- Phishing Threats – загрози фішингу
- Phreaking – фрікінг
- Physical Cyber Attack – фізична кібератака
- Physical Network Protection Strategies – стратегії захисту фізичної мережі
- Physical Ransom Attack Analysis – аналіз атак фізичного вимагання викупу
- Physical Security – фізична безпека

- Pilfering – дрібна крадіжка
- Pin – пін-код, шпилька
- Pipeline – конвеєр
- Pivot – точка опори, півотинг
- Pivoting – півотинг (поворот)
- Plain – простий, відкритий
- Plaintext – відкритий текст
- Planner – планувальник
- Plate Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання номерних знаків
- Platform Security – безпека платформи
- Plugin – плагін
- Pluggable Authentication Module (PAM) – модуль аутентифікації
- Point-of-sale (POS) Malware – шкідливе ПЗ для POS-терміналів
- Poison – отрута
- Poll – опитування
- Polymorphic Engine – поліморфний рушій
- Pool – пул, об'єднання
- Port – порт
- Port Attack Protection Strategies – стратегії захисту від атак через порти
- Port Knocking – стукання по портах
- Portable Drive Security – безпека портативних накопичувачів
- Portal – портал
- Post-Attack Recovery – відновлення після атаки
- Post-exploitation – пост-експлуатація
- Posture – стан, позиція (безпеки)
- Potential Attacks – потенційні атаки
- Power Analysis Attack – атака аналізом споживання
- PowerShell Attack – атака через PowerShell

- Pre-shared Key (PSK) – заздалегідь узгоджений ключ
- Precision – точність
- Predator – хижак
- Prefix – префікс
- Pretexting – претекстинг
- Preset – попередній набір
- Prevent Unauthorized Access – запобігання несанкціонованому доступу
- Prey – жертва
- Primitive – примітив
- Principal – принципал, основний
- Printer – принтер
- Privacy – приватність
- Privacy Breach Attack Handling Strategies – стратегії обробки атак на порушення приватності
- Privacy by Design – приватність на етапі проектування
- Privacy Protection – захист приватності
- Privacy-enhancing Technology (PET) – технологія посилення приватності
- Private Cloud Network Protection – захист мережі приватної хмари
- Private Key – закритий ключ
- Privilege Abuse – зловживання привілеями
- Privilege Escalation – підвищення привілеїв
- Privilege Escalation Attack Handling Strategies – стратегії обробки атак на підвищення привілеїв
- Proactive Cybersecurity – проактивна кібербезпека
- Proactive Defense – проактивний захист
- Probe – зонд, зондування
- Probabilistic Risk Assessment – ймовірнісна оцінка ризику
- Procedure – процедура

- Process – процес
- Process Hollowing – порожнення процесу
- Procurement Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління закупівлями
- Professional Protection Strategies – професійні стратегії захисту
- Profile – профіль
- Profiling – профілювання
- Project Estimation Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління оцінкою проектів
- Project Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління проектами
- Proof of Concept (PoC) – доказ концепції
- Proof of Work (PoW) – доказ виконаної роботи (у безпеці)
- Propagation – розповсюдження
- Property-based Testing in Security – тестування на основі властивостей у безпеці
- Protection against Hacking Attacks – захист від хакерських атак
- Protocol – протокол
- Protocol Anomaly – аномалія протоколу
- Provisioning – провайденінг
- Proximity Card Cloning – клонування проксіміті-карт
- Proxy – проксі
- Proxy Server Attack – атака через проксі-сервер
- Pseudonym – псевдонім
- Pseudonymization – псевдомінізація
- Public Key – відкритий ключ
- Public Key Infrastructure (PKI) – інфраструктура відкритих ключів

- Public Relations Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління зв'язками з громадськістю
- Public Security and Surveillance Technology System Protection – захист систем технології суспільної безпеки та спостереження
- Public Transportation Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління громадським транспортом
- Public Transportation Smart System Protection – захист розумних систем громадського транспорту
- Pulse – імпульс
- Pump – накачування (наприклад, даних)
- Purple Team – фіолетова команда
- Python for Offensive Security – Python для офенсивної безпеки

Q

- QoS Abuse – зловживання QoS
- QRadar – платформа SIEM (QRadar)
- Quad9 – рекурсивний DNS-резолвер Quad9
- Qualitative Risk Analysis – якісний аналіз ризиків
- Quality Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління якістю
- Quantitative Risk Analysis – кількісний аналіз ризиків
- Quantum Cryptography – квантова криптографія
- Quantum Key Distribution (QKD) – квантовий розподіл ключів
- Quantum-Level Breach Handling Strategies – стратегії обробки порушень на квантовому рівні
- Quantum-safe Algorithm – квантостійкий алгоритм
- Quarantine – карантин
- Quarantine Network – карантинна мережа
- Query – запит

- Query String Manipulation – маніпуляція рядком запиту
- Queue – черга
- Quest for Indicators of Compromise (IoC) – пошук індикаторів компрометації
- Quirk – особливість, хиба
- Quota – квота
- Quote – цитата, котирування

R

- Race Condition – гонка умов
- RACI Matrix in Security – матриця RACI у безпеці
- Radio Frequency Jamming – радіочастотне заглушення
- Raid – рейд (на дисках), атака
- Rainbow Table – райдужна таблиця
- Ransom – викуп
- Ransomcloud – рансомхмара
- Ransomware – шантажне ПЗ (ransomware)
- Ransomware Attack Handling Strategies – стратегії обробки атак шантажного ПЗ
- Ransomware Attack Protection Strategies – стратегії захисту від атак шантажного ПЗ
- Ransomware-as-a-Service (RaaS) – шантажне ПЗ як послуга
- Rapid7 – компанія з кібербезпеки Rapid7
- Raspberry Pi Pentesting – пент-тестування на Raspberry Pi
- RAT (Remote Access Trojan) – троянська програма віддаленого доступу
- Rate Limiting – обмеження частоти запитів
- Rationalization – раціоналізація (у соціальній інженерії)
- RBAC (Role-Based Access Control) – контроль доступу на основі ролей
- RCE (Remote Code Execution) – виконання віддаленого коду

- Reachability – досяжність
- Reaction – реакція
- Read – читання
- Reading Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання читання
- Real Estate Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління нерухомістю
- Real Estate System Protection – захист систем нерухомості
- Real-Time Governance – управління в реальному часі
- Real-time Joint Attack Analysis – аналіз спільних атак у реальному часі
- Real-time Monitoring – моніторинг у реальному часі
- Reassembly Attack – атака при повторній збірці
- Reconnaissance – розвідка
- Reconnaissance Phase – фаза розвідки
- Recovery Point Objective (RPO) – цільова точка відновлення
- Recovery Time Objective (RTO) – цільовий час відновлення
- Red Team – червона команда
- Red Team Exercise – вправа червоної команди
- Redundancy for Security – надмірність для безпеки
- Reference Monitor – еталонний монітор
- Reflected Attack – відображена атака
- Reflection – відображення
- Registry Attack – атака через реєстр
- Regression Testing in Security – регресійне тестування у безпеці
- Regulatory Compliance – нормативна відповідність
- Remote Code Execution (RCE) – виконання віддаленого коду

- Remote Desktop Protocol (RDP) Attack – атака на протокол віддаленого робочого столу
- Remote File Inclusion (RFI) – включення віддаленого файлу
- Remote Managed System Protection – захист системи, якою керують віддалено
- Remote Work System Security – безпека систем дистанційної роботи
- Renewable Energy System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем відновлюваної енергетики
- Renewable Energy System Protection – захист систем відновлюваної енергетики
- Replay Attack – атака повторенням
- Repudiation Attack – атака на неспростовність
- Reputation – репутація
- Reputation-based Filtering – фільтрація на основі репутації
- Request Forgery – підробка запиту
- Residual Risk – залишковий ризик
- Resilience – стійкість
- Resource – ресурс
- Resource Exhaustion – виснаження ресурсів
- Response – відповідь, реагування
- Retention – збереження, утримання
- Return-oriented Programming (ROP) – програмування, орієнтоване на повернення
- Reverse Engineering – зворотна розробка
- Reverse Proxy Security – безпека зворотного проксі
- Reverse Shell – зворотна оболонка
- Review – огляд
- Revocation – відкликання
- Risk – ризик

- Risk Appetite – схильність до ризику
- Risk Assessment Methodology – методологія оцінки ризиків
- Risk Management – управління ризиками
- Risk Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління ризиками
- Risk Mitigation Strategy – стратегія зменшення ризиків
- Risk Transfer – передача ризику
- Robot Exclusion Standard – стандарт виключення роботів
- Robot System Breach Attack Analysis – аналіз атак на порушення роботизованих систем
- Robotics and Industrial Automation System Protection – захист систем робототехніки та промислової автоматизації
- RockYou Attack – атака на основі паролів з бази RockYou
- Rogue Access Point – нелегітимна точка доступу
- Rogue Software – шахрайське ПЗ
- Role-Based Access Control (RBAC) – контроль доступу на основі ролей
- Rolling Code Attack – атака на код, що змінюється
- Root – рут, кореневий доступ
- Root Cause Analysis (RCA) – аналіз первопричин
- Root Certificate Authority – кореневий центр сертифікації
- Rootkit – руткіт
- Rootkit Detection – виявлення руткітів
- Router Attack – атака на маршрутизатор
- Router Control Attack Analysis – аналіз атак на контроль маршрутизаторів
- Rowhammer Attack – атака Rowhammer
- RSA Algorithm – алгоритм RSA
- RSI (Reputational System for IoT) – репутаційна система для IoT
- Rule – правило

- Rule-based Detection – виявлення на основі правил
- Runtime – час виконання
- Runtime Application Self-Protection (RASP) – самозахист додатків під час виконання

S

- S/MIME (Secure/Multipurpose Internet Mail Extensions) – розширення безпечної електронної пошти
- SaaS Security – безпека SaaS
- Safe Internet Usage – безпечне використання інтернету
- Safe Mode Bypass – обхід безпечного режиму
- Sales Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління продажами
- Salting – соління
- Sampling – вибірка
- Sandbox – сандбокс (пісочниця)
- Sandbox Evasion – ухилення від сандбоксу
- Satellite Identity Theft Attack Analysis – аналіз атак на крадіжку ідентичності через супутники
- SCADA Security – безпека SCADA
- Scanner – сканер
- Scareware – скірвер
- Scent Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання запахів
- Schema Poisoning – отруєння схеми
- Scraping Attack – атака скрейпінгу
- Script Kiddie – скрипт-кіді
- Sea Turtle Attack – атака "морська черепаха", DNS hijacking
- Second-order Injection – ін'єкція другого порядку
- Secret – секрет
- Secret Sharing – розділення секрету

- Secure Boot – безпечне завантаження
- Secure Cloud Computing – безпечні хмарні обчислення
- Secure Coding Practice – практики безпечного програмування
- Secure Communication Protocols – безпечні протоколи зв'язку
- Secure Communications with Data Encryption – безпечний зв'язок із шифруванням даних
- Secure Development Lifecycle (SDLC) – життєвий цикл безпечної розробки
- Secure Element – безпечний елемент
- Secure Erase – безпечне стирання
- Secure Handling Attack Handling Strategies – стратегії обробки атак на безпечну обробку
- Secure Hash Algorithm (SHA) – безпечний алгоритм хешування
- Secure Real-time Transport Protocol (SRTP) – безпечний протокол транспорту в реальному часі
- Secure Shell (SSH) Tunneling – тунелювання SSH
- Secure Sockets Layer (SSL) Stripping – знесення SSL
- Secure Software Development – безпечна розробка програмного забезпечення
- Secure Voice and Video Communications – безпечний голосовий та відеозв'язок
- Securing Distributed Geographical Networks – забезпечення безпеки розподілених географічних мереж
- Securing Internet-connected Robots – забезпечення безпеки інтернет-під'єднаних роботів
- Securing Online Business Transactions – забезпечення безпеки онлайн-бізнес-транзакцій
- Security Analysis – аналіз безпеки
- Security Assertion Markup Language (SAML) – мова розмітки тверджень безпеки

- Security Assessment – оцінка безпеки
- Security Assurance Analysis – аналіз забезпечення безпеки
- Security Audit – аудит безпеки
- Security Audit Log – журнал аудиту безпеки
- Security Awareness – обізнаність з безпеки
- Security Awareness Training – навчання обізнаності в безпеці
- Security Classification – класифікація безпеки
- Security Content Automation Protocol (SCAP) – протокол автоматизації контенту безпеки
- Security Deception Attack Handling Strategies – стратегії обробки атак на обман в безпеці
- Security Incident and Event Management (SIEM) – управління інцидентами та подіями безпеки
- Security Incident Recovery – відновлення після інциденту безпеки
- Security Incident Response – реагування на інциденти безпеки
- Security Information Management (SIM) – управління інформацією безпеки
- Security Management – управління безпекою
- Security Monitoring – моніторинг безпеки
- Security Orchestration, Automation and Response (SOAR) – оркестрування, автоматизація та реагування в безпеці
- Security Policy – політика безпеки
- Security Policy Enforcement – забезпечення дотримання політики безпеки
- Security Posture – стан безпеки
- Security Quality Assurance – забезпечення якості безпеки
- Security Risk Analysis – аналіз ризиків безпеки
- Security Risk Management Strategies – стратегії управління ризиками безпеки

- Security Scanning Attack Analysis – аналіз атак на сканування безпеки
- Security Strategies – стратегії безпеки
- Security System Protection – захист систем безпеки
- Security Threat Assessment – оцінка загроз безпеки
- Security Threat Detection Strategies – стратегії виявлення загроз безпеки
- Security Threat Management – управління загрозами безпеки
- Security through Obscurity – безпека через неясність
- Security Token – токен безпеки
- Security Training – навчання з безпеки
- Security Updates – оновлення безпеки
- Security Verification – верифікація безпеки
- Security Vulnerabilities – вразливості (діри) безпеки
- Segmentation – сегментація
- Segregation of Duties (SoD) – розділення обов'язків
- Self-decrypting Malware – саморозшифровуване шкідливе ПЗ
- Self-propagating Worm – саморозповсюджуваний черв'як
- Semantic Attack – семантична атака
- Sensitive Data Encryption – шифрування конфіденційних даних
- Sensitive Data Exposure – викриття чутливих даних
- Sensitive Data Protection – захист конфіденційних даних
- Sensitive Data Security in Communications – безпека конфіденційних даних у зв'язку
- Sensitive Data Security in Hybrid Cloud – безпека конфіденційних даних у гібридній хмарі
- Sensitive Information Protection – захист конфіденційної інформації
- Sensor and Wearable Device Protection – захист сенсорів та носимих пристроїв

- Server-side Request Forgery (SSRF) – підробка запиту на стороні сервера
- Service-level Agreement (SLA) for Security – угода про рівень обслуговування (SLA) для безпеки
- Service-oriented Architecture (SOA) Security – безпека сервіс-орієнтованої архітектури
- Session – сесія
- Session Fixation – фіксація сесії
- Session Hijacking – перехоплення сесії
- Shadow API – тіньовий API
- Shadow IT – тіньова IT
- Shamoon – вірус Shamoon
- Shape Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання форм
- Shared Network Attack Analysis – аналіз атак на спільну мережу
- Shared Printer Device Protection – захист спільних принтерів
- Shared Printer Privacy Breach Attack Analysis – аналіз атак на порушення приватності спільних принтерів
- Shared Responsibility Model – модель спільної відповідальності
- Shell – оболонка
- Shellcode – шелл-код
- Shopping System Protection – захист шопінг-систем
- Shoulder Surfing – підгляд
- Side-channel Attack – атака за допомогою побічних каналів
- Signature – підпис, сигнатура
- Signature-based Detection – сигнатурне виявлення
- Simple Mail Transfer Protocol (SMTP) Relay Attack – атака на ретрансляцію SMTP
- Simulated Phishing – імітація фішингу

- Simulation System Breach Attack Handling Strategies – стратегії обробки атак на порушення імітаційних (симуляційних) систем
- Single Point of Failure (SPOF) – єдина точка відмови
- Single Sign-on (SSO) Attack – атака на єдиний вхід
- Sinkholing – сінкхолінг
- Situation Awareness – обізнаність про ситуацію
- Smart Agriculture System Protection – захист розумних аграрних систем
- Smart App Privacy Breach Attack Analysis – аналіз атак на порушення приватності розумних додатків
- Smart Aviation System Protection – захист розумних авіаційних систем
- Smart Building Control System Protection – захист розумних систем контролю будівель
- Smart Car System Protection – захист розумних автомобільних систем
- Smart Charging System Breach Attack Analysis – аналіз атак на порушення розумних систем заряджання
- Smart City System Protection – захист розумних міських систем
- Smart Cloud Privacy Breach Attack Analysis – аналіз атак на порушення приватності розумних хмар
- Smart Commerce System Protection – захист розумних комерційних систем
- Smart Contract Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління смарт-контрактами
- Smart Contract Vulnerability – вразливість смарт-контракту
- Smart Defense and Security System Protection – захист розумних оборонних та безпекових систем
- Smart Device Attack Analysis – аналіз атак на розумні пристрої

- Smart Device Protection – захист розумних пристроїв
- Smart Device Security – безпека розумних пристроїв
- Smart Education System Privacy Breach Attack Analysis – аналіз атак на порушення приватності розумних освітніх систем
- Smart Endpoint Security – безпека розумних кінцевих точок
- Smart Energy System Protection – захист розумних енергетичних систем
- Smart Entertainment System Protection – захист розумних розважальних систем
- Smart Environmental System Protection – захист розумних екологічних систем
- Smart Events and Conferences System Protection – захист розумних систем подій та конференцій
- Smart Gaming Device Privacy Breach Attack Handling Strategies – стратегії обробки атак на порушення приватності розумних ігрових пристроїв
- Smart Grid System Protection – захист розумних енергосистем (smart grid)
- Smart Healthcare System Protection – захист розумних медичних систем
- Smart Home Network Security – безпека мережі розумного дому
- Smart Home System Protection – захист розумних домашніх систем
- Smart Hospital and Healthcare System Protection – захист розумних лікарняних та медичних систем
- Smart Industrial System Protection – захист розумних промислових систем
- Smart Infrastructure System Protection – захист розумних інфраструктурних систем
- Smart Land Transportation System Protection – захист розумних наземних транспортних систем

- Smart Lighting and Illumination Control System Protection – захист розумних систем контролю освітлення та ілюмінації
- Smart Local Government System Protection – захист розумних систем місцевого самоврядування
- Smart Malware Attack Analysis – аналіз розумних атак шкідливого ПЗ
- Smart Manufacturing System Protection – захист розумних виробничих систем
- Smart Meter Privacy Breach Attack Handling Strategies – стратегії обробки атак на порушення приватності розумних лічильників
- Smart Mining System Protection – захист розумних гірничодобувних систем
- Smart Monitoring System Protection – захист розумних систем моніторингу
- Smart Network Breach Attack Handling Strategies – стратегії обробки атак на порушення розумних мереж
- Smart Railway and Public Transportation System Protection – захист розумних залізничних та громадських транспортних систем
- Smart Real Estate System Protection – захист розумних систем нерухомості
- Smart Renewable Energy System Protection – захист розумних систем відновлюваної енергетики
- Smart Robot Security – безпека розумних роботів
- Smart School System Protection – захист розумних шкільних систем
- Smart Security Device Privacy Breach Attack Analysis – аналіз атак на порушення приватності розумних пристроїв безпеки
- Smart Security System Protection – захист розумних систем безпеки

- Smart Shopping System Protection – захист розумних шопінг-систем
- Smart Social Networking and Communication System Protection – захист розумних соціальних мереж та систем зв'язку
- Smart Surveillance Protection – захист розумних систем спостереження
- Smart System Protection for Small and Medium Enterprises – захист розумних систем для малих та середніх підприємств
- Smart Transportation Network Protection – захист розумної транспортної мережі
- Smart Transportation System Protection – захист розумних транспортних систем
- Smart Transportation Technology System Protection – захист розумних транспортних технологій
- Smart Travel and Tourism Breach Attack Handling Strategies – стратегії обробки атак на порушення розумних систем подорожей та туризму
- Smart Urban Infrastructure System Protection – захист розумних міських інфраструктурних систем
- Smart Water Transportation System Protection – захист розумних водних транспортних систем
- Smart Work and Office System Protection – захист розумних робочих та офісних систем
- Smartphone – смартфон
- Smartphone Privacy Breach Attack Analysis – аналіз атак на порушення приватності смартфонів
- Smartphone Security – безпека смартфона
- Smartphone-based Attack Analysis – аналіз атак на основі смартфону
- Smishing (SMS-Phishing) – смішинг (SMS-фішинг)
- SMS Bombing – SMS-бомбардування

- Sniffer – сніффер
- Snowden Revelations – розкриття Сноудена
- Social App Privacy Breach Attack Analysis – аналіз атак на порушення приватності соціальних додатків
- Social Engineering – соціальна інженерія
- Social Engineering Attack Analysis – аналіз атак соціальної інженерії
- Social Engineering Attack Handling Strategies – стратегії обробки атак соціальної інженерії
- Social Engineering Toolkit (SET) – набір інструментів для соціальної інженерії
- Social Media Platform Privacy Breach Attack Analysis – аналіз атак на порушення приватності платформ соціальних мереж
- Social Media Platform Security – безпека платформ соціальних медіа
- Social Network Attack Handling Strategies – стратегії обробки атак на соціальні мережі
- Social Network Phishing Attack Analysis – аналіз атак фішингу в соціальних мережах
- Social Network Protection – захист соціальних мереж
- Software Bill of Materials (SBOM) – відомість матеріалів програмного забезпечення
- Software Composition Analysis (SCA) – аналіз складу програмного забезпечення
- Software-defined Perimeter (SDP) – програмно-визначений периметр
- Source Code Review – огляд вихідного коду
- Spam over Internet Telephony (SPIT) – спам через інтернет-телефонію
- Spear Phishing – цільовий фішинг

- Speech Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання мовлення
- Spillage – витік інформації
- Spoofing – спуфінг
- Spyware – шпигунське ПЗ
- SQL Injection – ін'єкція SQL
- Square Attack – атака Square
- SS7 Attack – атака на SS7
- Stack Canary – канарієць стека
- Stack Overflow – переповнення стека
- Stagefright – вразливість Stagefright
- Steganalysis – стеганоаналіз
- Steganography – стеганографія
- Stingray – стрінгрей, IMSI-слоувер
- Storage Security – безпека зберігання (даних)
- Storm Worm – черв'як Storm
- Strategic Cyber Defense – стратегічний кіберзахист
- Streaming Technology Breach Attack Handling Strategies – стратегії обробки атак на порушення технологій стрімінгу
- Stress Testing – стрес-тестування
- Structured Threat Information Expression (STIX) – структуроване вираження інформації про загрози
- Supply Chain Attack – атака на ланцюг постачання
- Supply Chain Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління ланцюгами поставок
- Supply Chain Tracking Privacy Breach Attack Analysis – аналіз атак на порушення приватності при відстеженні ланцюгів поставок
- Surveillance and Security Control System Protection – захист систем контролю спостереження та безпеки

- Surveillance Camera Privacy Breach Attack Analysis – аналіз атак на порушення приватності камер спостереження
- Suspicious Behavior Analysis – аналіз підозрілої поведінки
- Sustainability Hacking Attack Handling Strategies – стратегії обробки хакерських атак на системи сталого розвитку
- Swatting – сваттинг
- Symmetric Encryption – симетричне шифрування
- SYN Flood – SYN-флуд
- Sync-Based Tampering Attack Handling Strategies – стратегії обробки атак на спотворення на основі синхронізації
- System Hardening – загартовування системи
- System Protection – захист системи

T

- Taint Analysis – аналіз забруднених даних
- Tamper Detection – виявлення несанкціонованого втручання
- Tamper-proofing – захист від втручання
- Target – ціль
- Targeted Attack – цільова атака
- Targeted Attack Analysis – аналіз цілеспрямованих атак
- Targeted Attack Handling Strategies – стратегії обробки цілеспрямованих атак
- Targeted Attack Protection – захист від цілеспрямованих атак
- Targeted Malware Attack Analysis – аналіз цілеспрямованих атак шкідливого ПЗ
- Targeted Threat Analysis – аналіз цілеспрямованих загроз
- Task Scheduler Attack – атака через планувальник завдань
- TCP Hijacking – перехоплення TCP
- TCP/IP Stack Fingerprinting – визначення стеку TCP/IP
- Teardrop Attack – атака Teardrop

- Technical Debt in Security – технічний борг у безпеці
- Technological Bend Attack Analysis – аналіз атак на технологічні вигини
- Telecom Fraud – телекомунікаційне шахрайство
- Telemetry – телеметрія
- Telemetry Data Security – безпека даних телеметрії
- Tender Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління тендерами
- Teredo Tunneling Attack – атака через тунелювання Teredo
- Test – тест
- Text Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання тексту
- Thermal Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через термальне розпізнавання
- Threat – загроза
- Threat Actor – суб'єкт загрози
- Threat Containment – стримування загроз
- Threat Detection – виявлення загроз
- Threat Hunting – полювання на загрози
- Threat Intelligence – розвідка загроз
- Threat Intelligence Platform (TIP) – платформа розвідки загроз
- Threat Landscape – ландшафт загроз
- Threat Management – управління загрозами
- Threat Modeling – моделювання загроз
- Threat Predictive Analysis – прогнозний аналіз загроз
- Threshold Cryptography – порогова криптографія
- Ticket – квиток (автентифікації)

- Time Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання часу
- Time-based One-time Password (TOTP) – одноразовий пароль на основі часу
- Time-of-check to Time-of-use (TOCTOU) Attack – атака "час перевірки – час використання"
- Time-to-live (TTL) Attack – атака на час життя пакета
- Token – токен
- Tokenization – токенізація
- Tone Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання тону
- Tor (The Onion Router) – Tor (цибулевий маршрутизатор)
- Torshammer – атака Torshammer
- Total Virus – загальна вірусна активність
- Traffic – трафік
- Traffic Analysis – аналіз трафіку
- Traffic Control System Breach Attack Analysis – аналіз атак на порушення систем контролю дорожнього руху
- Traffic Light Protocol (TLP) – протокол світлофора
- Training and Education System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем навчання та освіти
- Transaction – транзакція
- Transaction Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління транзакціями
- Transient Execution Attack – атака на транзитивне виконання
- Transport Layer Security (TLS) Downgrade Attack – атака на пониження рівня TLS
- Trapdoor – люк, бекдор

- Travel Application Privacy Breach Attack Analysis – аналіз атак на порушення приватності додатків для подорожей
- Triple DES (3DES) – потрійний DES
- Trojan Horse – троянський кінь
- Trust Boundary – межа довіри
- Trusted Computing Base (TCB) – надійна обчислювальна база
- Trusted Execution Environment (TEE) – довірене середовище виконання
- Trusted Platform Module (TPM) – довірений платформовий модуль
- Tunnel – тунель
- Tunneling Protocol Abuse – зловживання тунельними протоколами
- Two-factor Authentication (2FA) – двофакторна автентифікація
- Type Confusion – плутанина типів

U

- UDP Flood – UDP-флуд
- UEBA (User and Entity Behavior Analytics) – аналіз поведінки користувачів та об'єктів
- Ukrainian Power Grid Attack – атака на енергосистему України
- Unauthorized Access – несанкціонований доступ
- Unauthorized Software – несанкціоноване ПЗ
- Underflow Attack – атака на переповнення вниз
- Unified Threat Management (UTM) – єдине управління загрозами
- Unknown Threat – невідома загроза
- Unmanaged Device – некерований пристрій

- Unpatched Vulnerability – незалатана вразливість
- Unstructured Data Protection – захист неструктурованих даних
- Untrusted Input – недовірливий ввід
- Uptime vs. Security – час безвідмовної роботи vs. безпека
- Urban Infrastructure System Protection – захист міських інфраструктурних систем
- URL Filtering – фільтрація URL
- USB Drop Attack – атака через підкинуту USB-флешку
- User Account Control (UAC) Bypass – обхід контролю облікових записів користувача
- User Behavior Analytics (UBA) – аналіз поведінки користувачів
- User Identity Management – управління ідентичністю користувача
- User Security Awareness – обізнаність користувачів у питаннях безпеки
- User Tracking – відстеження користувачів
- User Training and Awareness – навчання та підвищення обізнаності користувачів

V

- V2X security (Vehicle-to-everything security) – безпека V2X (зв'язку транспорт-усе)
- VAPT (Vulnerability Assessment and Penetration Testing) – VAPT (оцінка вразливостей та тестування на проникнення)
- VBA macro virus – макровірус на VBA
- Vehicle Embedded Device Protection – захист вбудованих пристроїв транспортного засобу
- Vendor risk management – управління ризиками постачальників

- Verification – верифікація
- Verification code leakage – витік коду підтвердження
- Vibration Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання вібрацій
- Victim – жертва (атаки)
- Video Cloning Attack Handling Strategies – стратегії обробки атак клонування відео
- Video Game Protection – захист відеоігор
- Virtual Cloud Attack Analysis – аналіз атак на віртуальну хмару
- Virtual Local Area Network (VLAN) Protection – захист віртуальної локальної мережі (VLAN)
- Virtual Machine (VM) – віртуальна машина (ВМ)
- Virtual Machine Escape – втеча з віртуальної машини
- Virtual private network (VPN) leak – витік VPN
- Virtual Private Network (VPN) Protection / Security – захист / безпека віртуальної приватної мережі (VPN)
- Virtual Reality Device Breach Attack Handling Strategies – стратегії обробки атак на порушення пристроїв віртуальної реальності
- Virtual Reality Privacy Breach Attack Analysis – аналіз атак на порушення приватності у віртуальній реальності
- Virtualization security – безпека віртуалізації
- Virus – вірус (комп'ютерний вірус)
- Virus total – сервіс VirusTotal
- Visa security – безпека платіжних систем Visa
- Vishing – вішинг (голосовий фішинг)
- Visual cryptography – візуальна криптографія
- Voice Attack Handling Strategies – стратегії обробки голосових атак

- Voice Cloning Attack Handling Strategies – стратегії обробки атак клонування голосу
- Voice over Internet Protocol (VoIP) Communication Protection – захист зв'язку через Voice over IP (VoIP)
- Voice over IP (VoIP) attack – атака на VoIP
- Voice over IP (VoIP) Network Protection / Security – захист / безпека мережі Voice over IP (VoIP)
- Voice over IP (VoIP) Privacy Breach Attack Analysis – аналіз атак на порушення приватності Voice over IP (VoIP)
- Voice over IP (VoIP) System Protection – захист систем Voice over IP (VoIP)
- Voice phishing – фішинг за допомогою голосу (вішинг)
- Voice Recognition Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання голосу
- Voice Technology Privacy Breach Attack Analysis – аналіз атак на порушення приватності голосових технологій
- Voiceprint (Recognition) Privacy Breach Attack Analysis – аналіз атак на порушення приватності через розпізнавання голосового відбитка
- Volatile memory forensics – форензика волатильної пам'яті
- Volumetric Attack – об'ємна атака (тип DDoS)
- Vote flipping attack – атака на зміну голосів
- VPN (Virtual Private Network) – віртуальна приватна мережа (ВПМ)
- Vulnerability Analysis – аналіз вразливостей
- Vulnerability Analysis and Patching – аналіз та усунення вразливостей
- Vulnerability assessment – оцінка вразливостей
- Vulnerability chaining – ланцюжок вразливостей
- Vulnerability Database – база даних вразливостей

- Vulnerability disclosure program – програма розкриття вразливостей
- Vulnerability Exploitation Attack Analysis – аналіз атак з використанням вразливостей
- Vulnerability Exposure – експозиція (виявленість) вразливостей
- Vulnerability management lifecycle – життєвий цикл управління вразливостями
- Vulnerability Patching – виправлення (закриття) вразливостей
- Vulnerability scanning – сканування на вразливості

W

- WAF (Web application firewall) – веб-брандмауер (WAF)
- War dialing – вардіалінг
- War driving – вардрайвінг
- Wardening – загартування (системи)
- Warehouse Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління складами
- Warez – нелегальне програмне забезпечення
- Water and Wastewater Networks Control System Protection – захист систем контролю водних та стічних мереж
- Water holing / Watering hole attack – атака "водопій"
- Watermarking – нанесення водяних знаків (цифрових)
- Weak cipher – слабкий шифр
- Weak entropy – слабка ентропія
- Wearable Device Breach Attack Handling Strategies – стратегії обробки атак на порушення носимих пристроїв
- Wearable Device Local Network Security – безпека локальної мережі для носимих пристроїв

- Wearable Device Protection – захист носимих пристроїв
- Wearable Devices System Protection – захист систем носимих пристроїв
- Web Application Security – безпека веб-додатків
- Web cache poisoning – отруєння веб-кешу
- Web Exploitation Attack Handling Strategies – стратегії обробки атак на експлуатацію веб-вузлів
- Web Filtering – веб-фільтрація
- Web fingerprinting – веб-фінгерпринтинг
- Web Infrastructure Protection – захист веб-інфраструктури
- Web Page Protection – захист веб-сторінок
- Web shell – веб-шелл
- Web skimming – веб-скімінг
- Website Protection – захист веб-сайту
- Whaling – китобійний фішинг (цільовий на керівників)
- White box testing – тестування білого ящика
- Whonix – дистрибутив Whonix (для анонімності)
- Wi-Fi cracking – злом Wi-Fi
- Wi-Fi Network Protection – захист мережі Wi-Fi
- Wi-Fi Pineapple – пристрій Wi-Fi Pineapple (для тестування)
- Wi-Fi Privacy Breach Attack Analysis – аналіз атак на порушення приватності Wi-Fi
- Wi-Fi protected access (WPA3) – захищений доступ Wi-Fi (WPA3)
- Wi-Fi protected setup (WPS) attack – атака через WPS
- Wildcard certificate abuse – зловживання wildcard-сертифікатами
- Wiper Malware – віпуюче шкідливе ПЗ
- Wired and Wireless Communication Networks System Protection – захист систем проводових та бездротових мереж зв'язку

- Wired equivalent privacy (WEP) attack – атака на WEP
- Wireguard protocol – протокол Wireguard
- Wireless Communication Security – безпека бездротового зв'язку
- Wireless Injection Attack Analysis – аналіз атак на ін'єкцію в бездротові мережі
- Wireless Interface Breach Attack Analysis – аналіз атак на порушення бездротових інтерфейсів
- Wireless intrusion prevention system (WIPS) – система запобігання вторгненню в бездротові мережі (WIPS)
- Wireless Internet Network Breach Attack Handling Strategies – стратегії обробки атак на порушення бездротових інтернет-мереж
- Wireless Network Attack Handling Strategies – стратегії обробки атак на бездротові мережі
- Wireless Network Protection / Security – захист / безпека бездротових мереж
- Wireless Network System Breach Attack Analysis – аналіз атак на порушення бездротових мережевих систем
- Wireless Sensor Privacy Breach Attack Analysis – аналіз атак на порушення приватності бездротових сенсорів
- Work and Office System Protection – захист робочих та офісних систем
- Workforce Management System Breach Attack Handling Strategies – стратегії обробки атак на порушення систем управління персоналом
- Workplace Device Security – безпека пристроїв на робочому місці
- Workstation – робоча станція
- Wormable vulnerability – вразливість, що дозволяє поширення черв'яків

- WPA2 handshake attack – атака на рукостискання WPA2
- Write blocker – блокувальник запису (форензика)

X

- X.509 certificate – сертифікат X.509
- Xen hypervisor security – безпека гіпервізору Xen
- XML external entity (XXE) attack – XXE атака
- XML signature wrapping – обгортка XML-підпису
- XOR Encryption – XOR шифрування
- XSS auditor – аудитор XSS
- XSS filter evasion – ухилення від фільтрів XSS

Y

- Y2K38 problem – проблема 2038 року
- YARA rules – правила YARA
- Yara-L – мова Yara-L (для логів)
- YubiKey – апаратний ключ YubiKey

Z

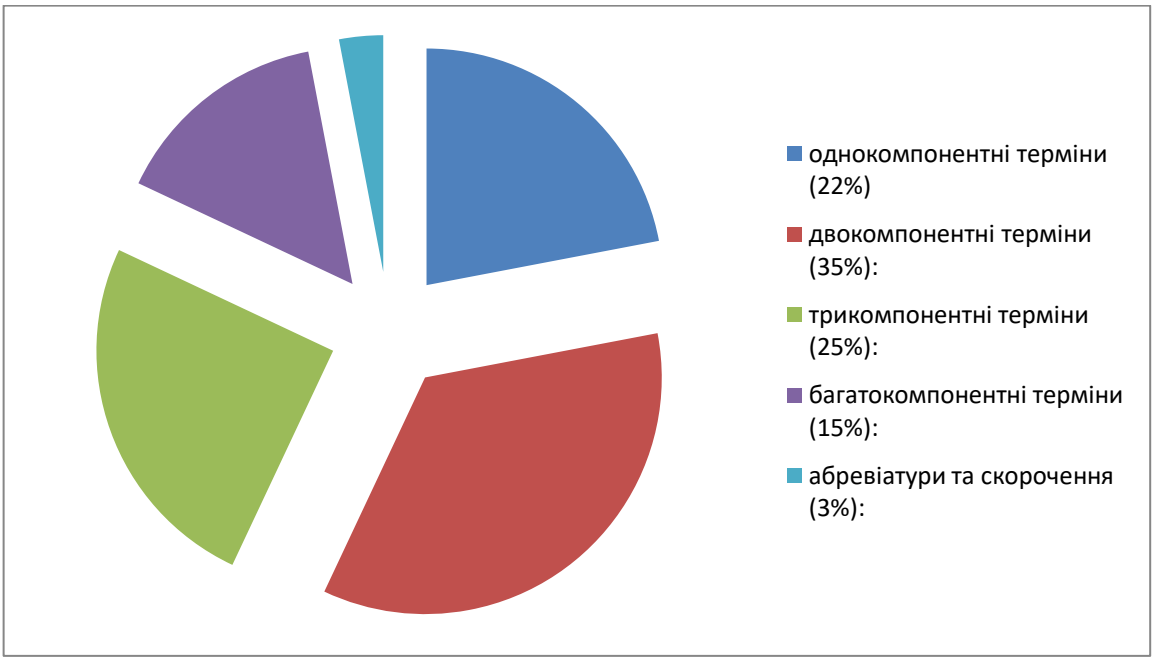
- Zero-day exploit – експлойт нульового дня
- Zero-day Exploit Analysis – аналіз експлойтів нульового дня
- Zero-Day Exploit Handling Strategies – стратегії обробки експлойтів нульового дня
- Zero-Day Threat Detection Strategies – стратегії виявлення загроз нульового дня
- Zero-knowledge proof – доказ з нульовим розголошенням
- Zero-trust architecture – архітектура нульової довіри
- Zigbee protocol security – безпека протоколу Zigbee
- Zombie computer – комп'ютер-зомбі
- Zombie Network – зомбі-мережа (ботнет)
- Zombie process attack – атака через зомбі-процес
- Zone transfer attack – атака трансферу зони DNS

Додаток Б

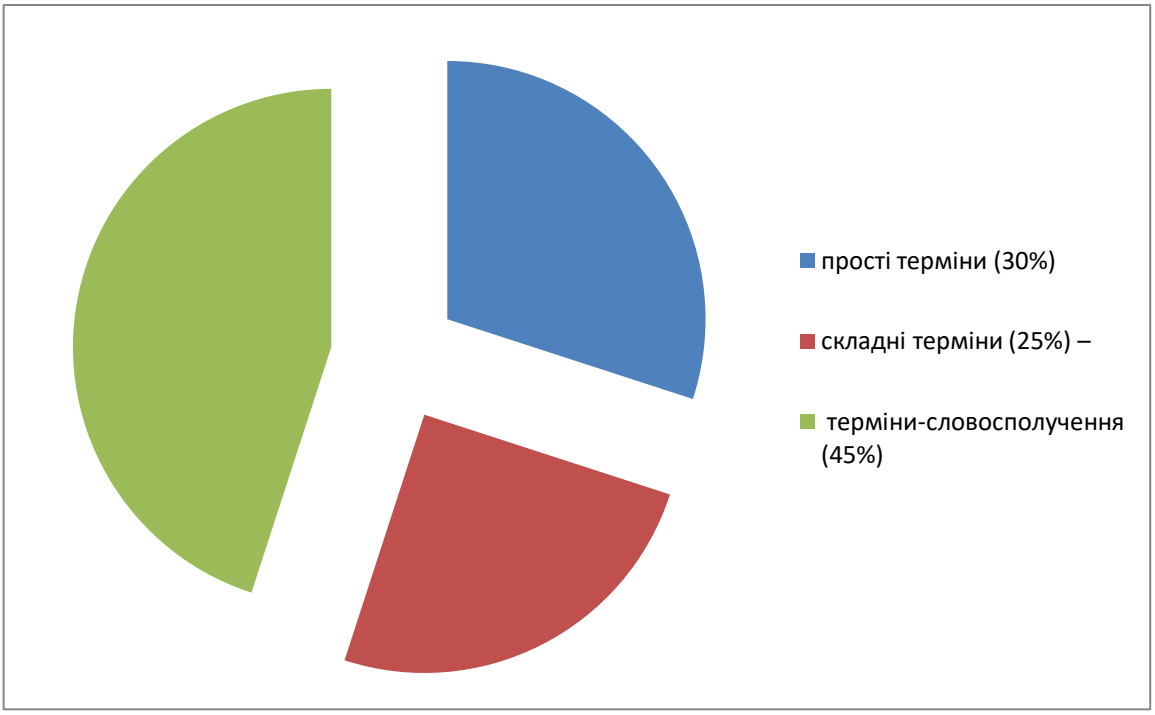
Діаграми

Періоди розвитку англомовної термінології

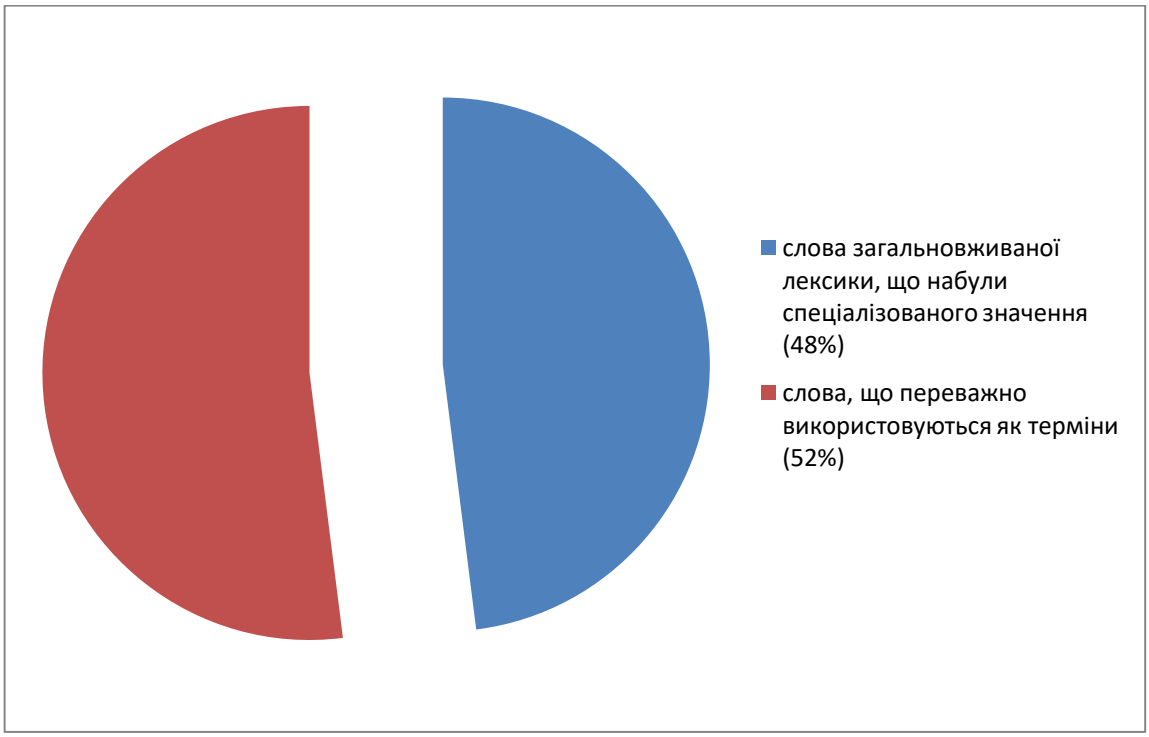
Структурні моделі в англомовній терміносистемі кібербезпеки



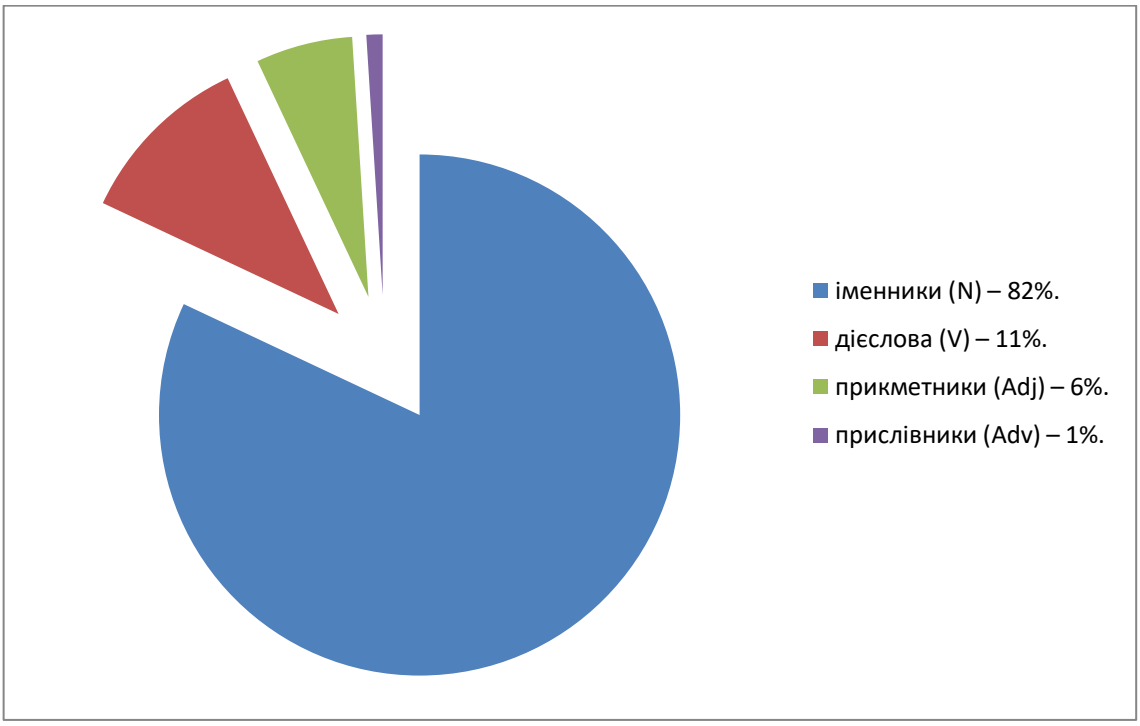
Класифікація англомовних термінів кібербезпеки за будовою



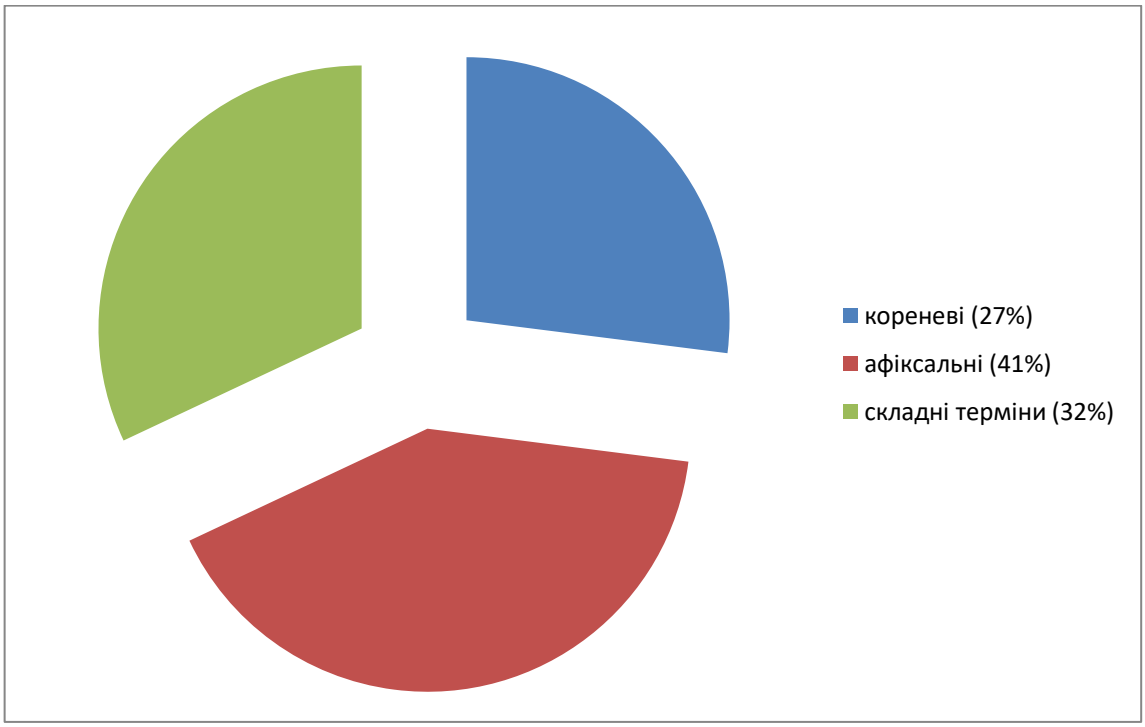
Класифікація простих англомовних термінів кібербезпеки



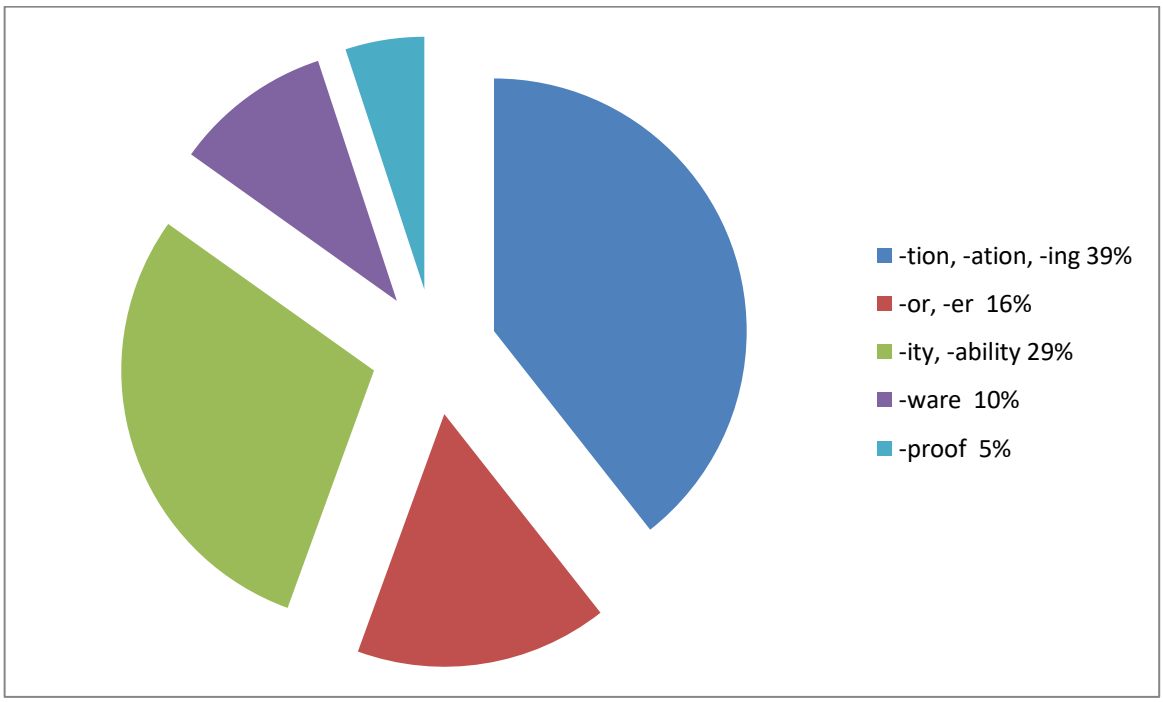
Класифікація англомовної термінології кібербезпеки ха частинами мови



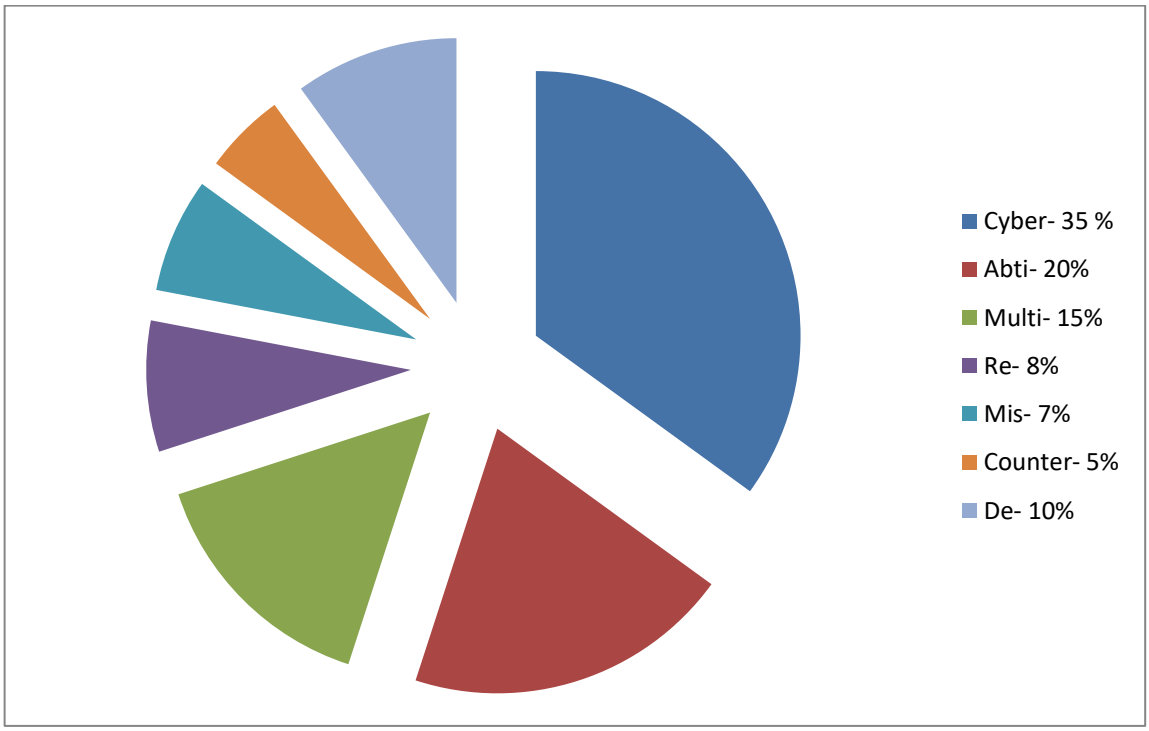
Прості англомовні терміни кібербезпеки



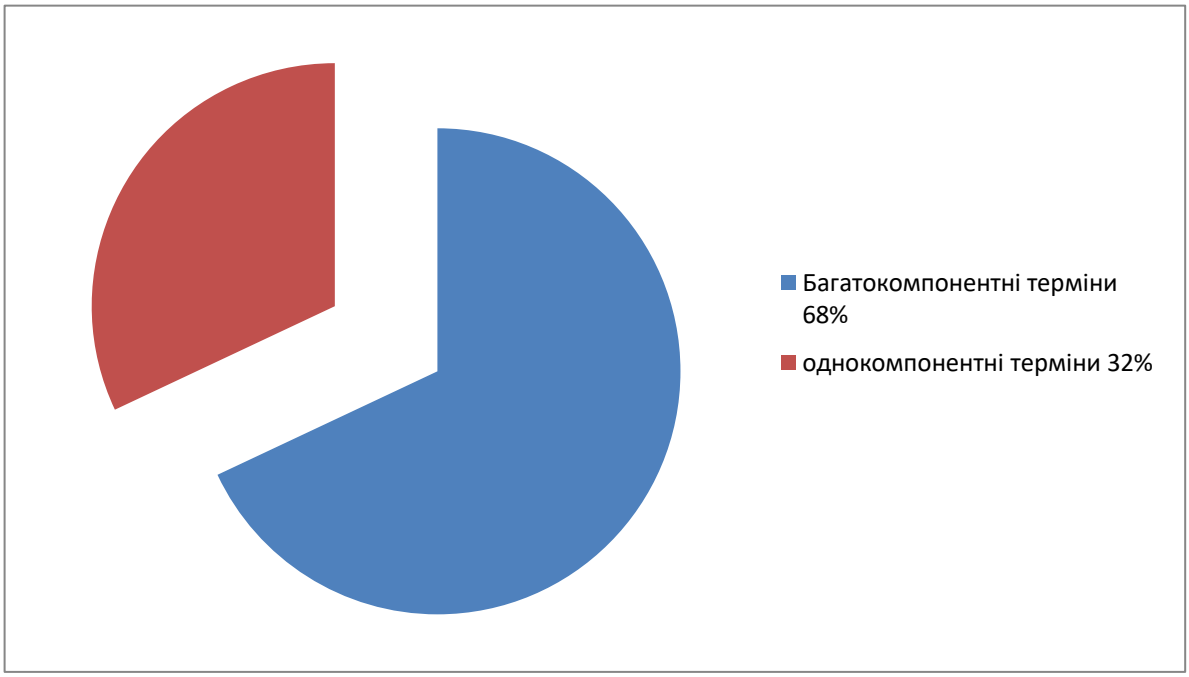
Продуктивні суфікси англомовних термінів кібербезпеки



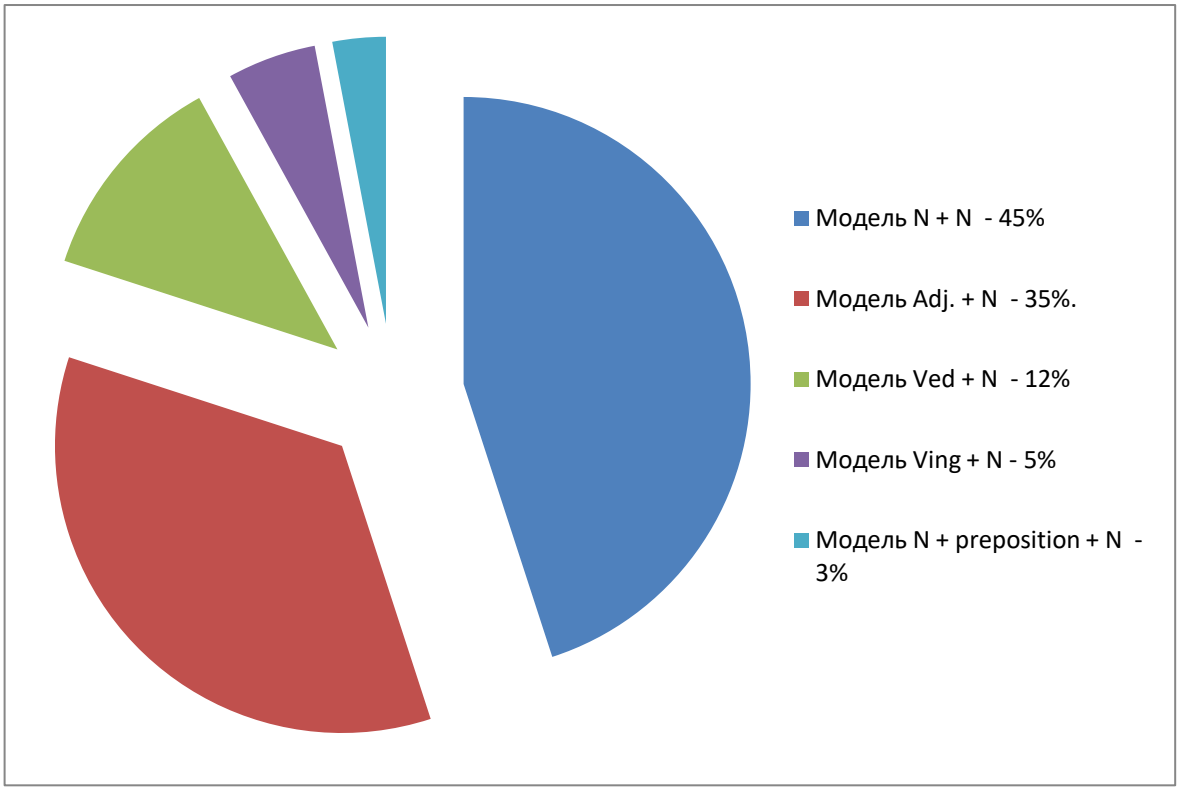
Продуктивні префікси англомовних термінів кібербезпеки



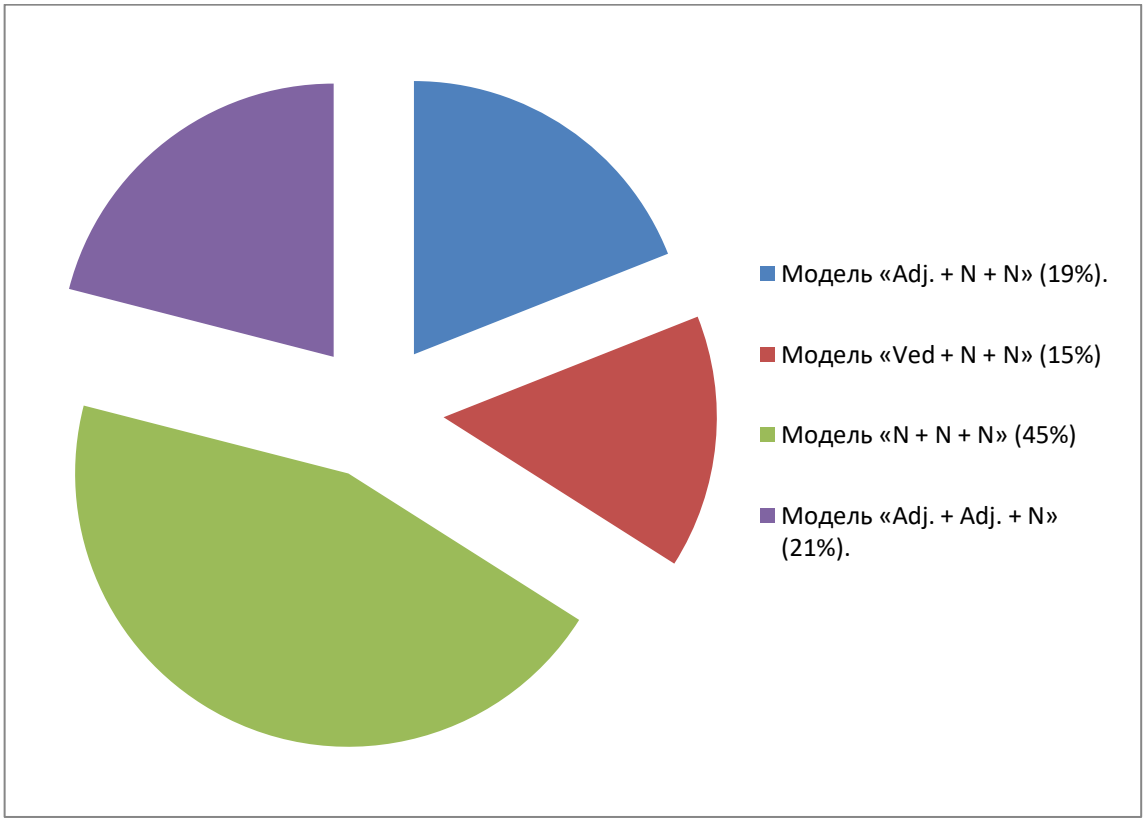
Відношення однокомпонентних та багатокомпонентних англомовних термінів кібербезпеки



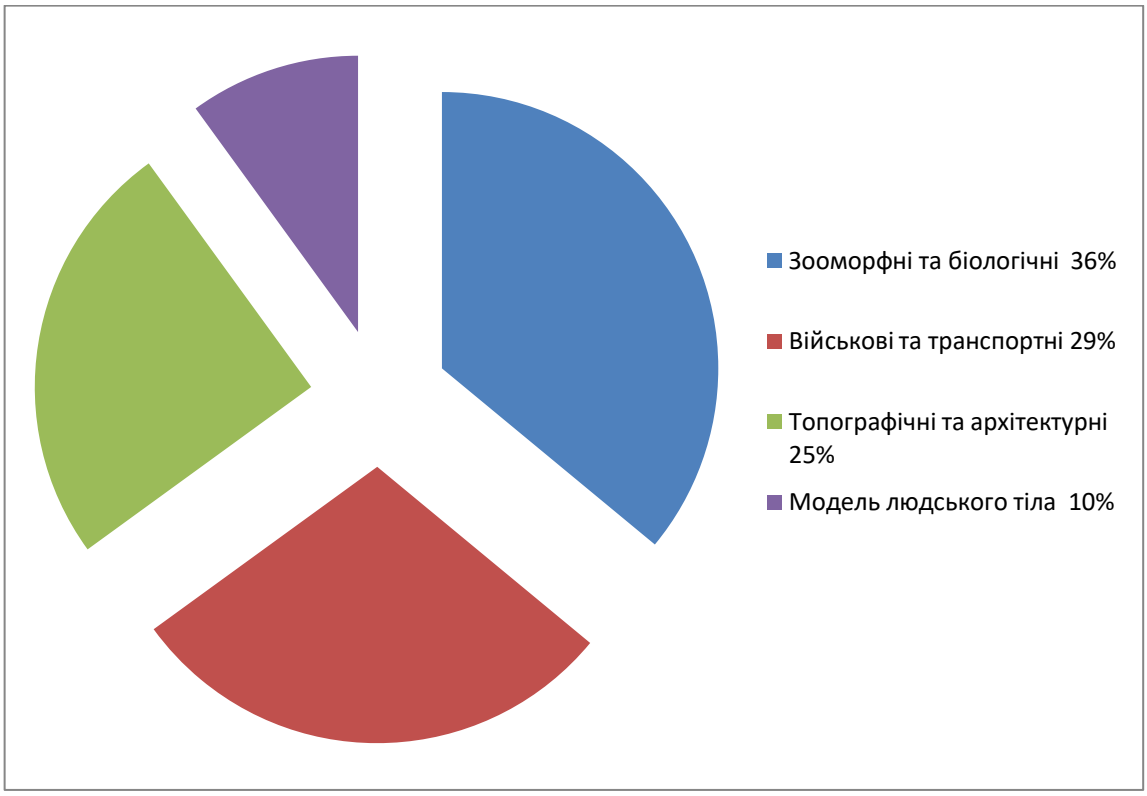
Продуктивні моделі англомовних двукомпонентних термінів кібербезпеки



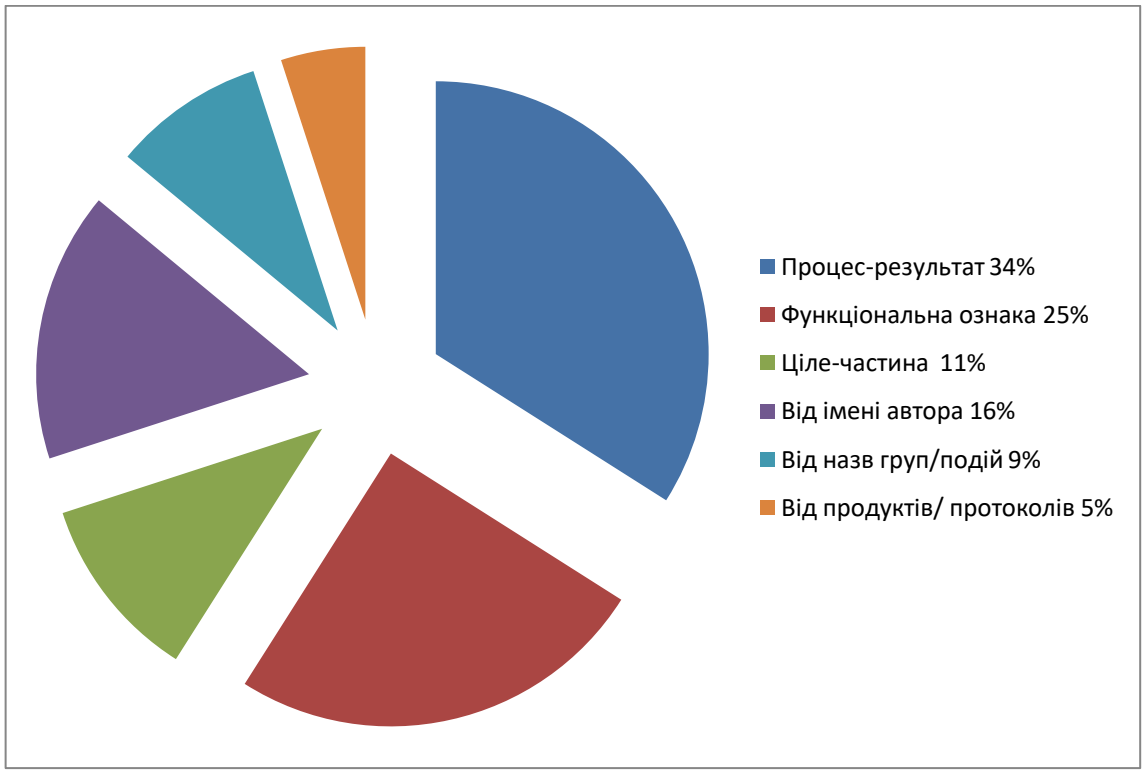
Продуктивні моделі англомовних багатокомпонентних термінів кібербезпеки



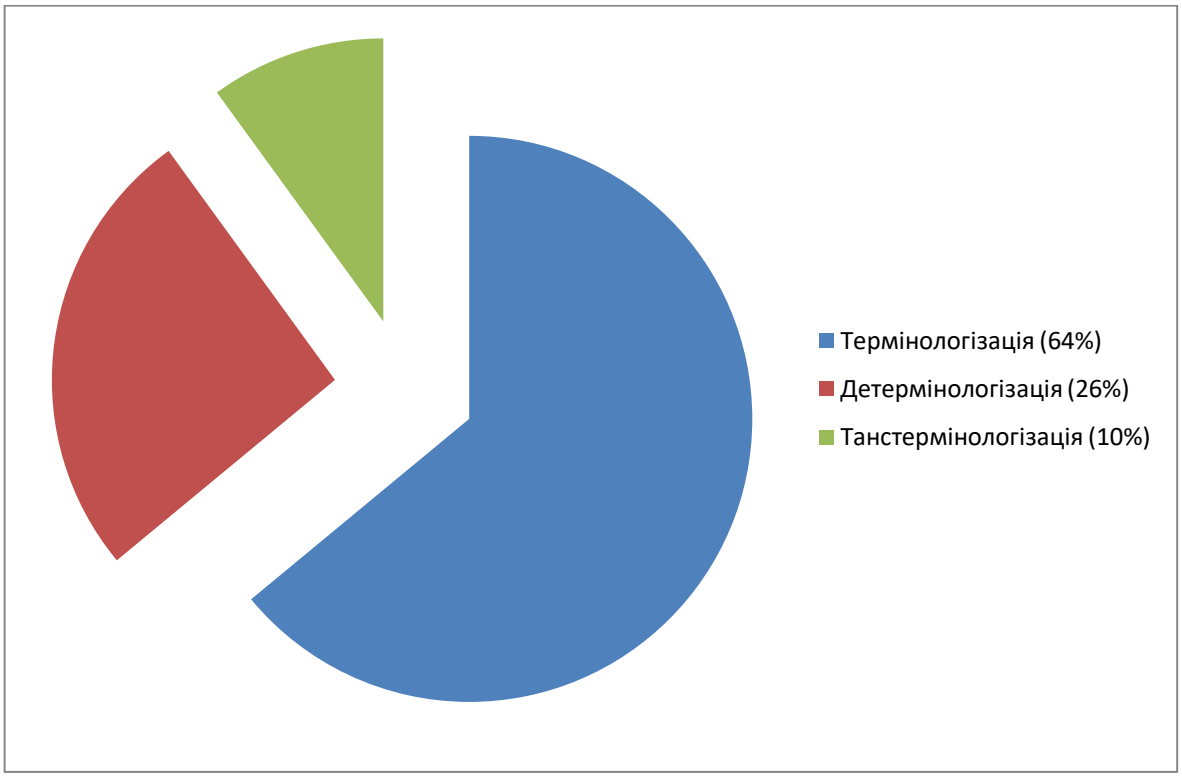
Терміни-метафори в англомовній терміносистемі кібербезпеки



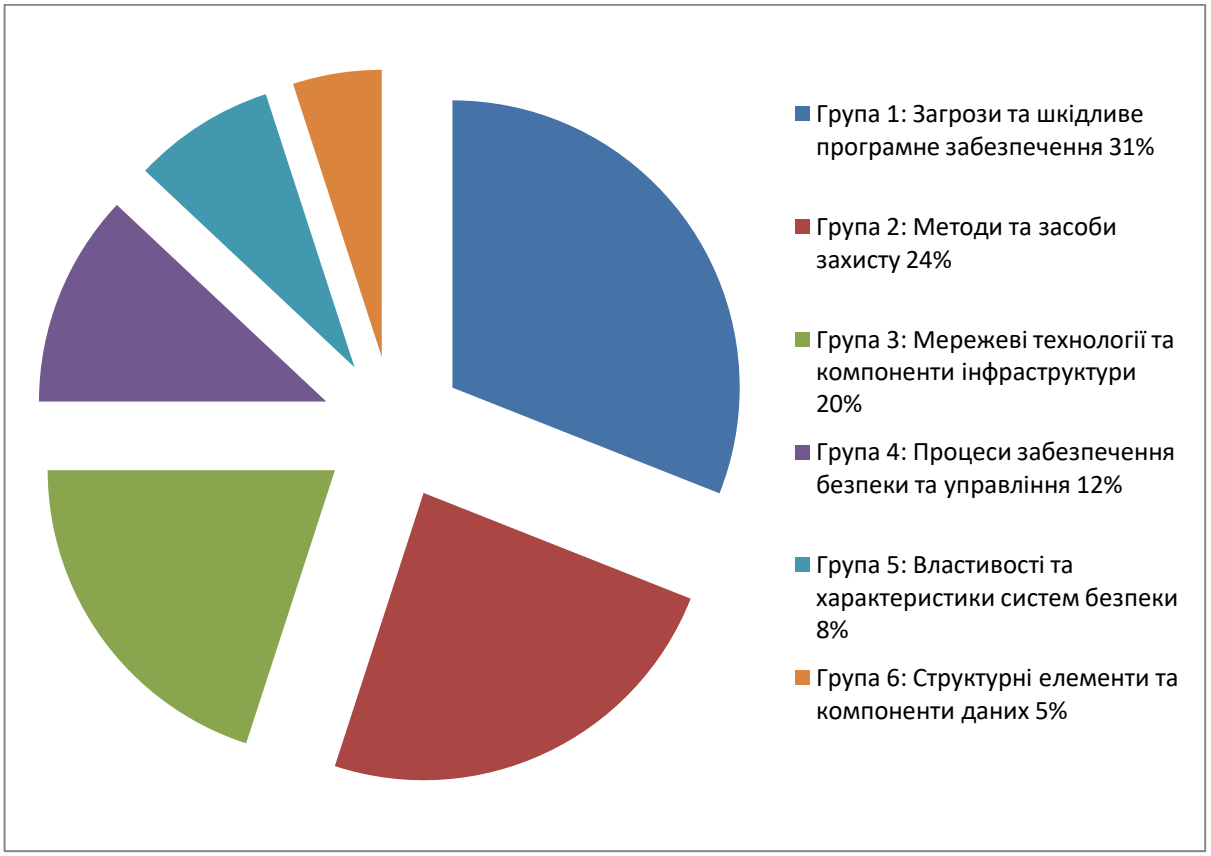
Терміни-метонімії в англомовній терміносистемі кібербезпеки



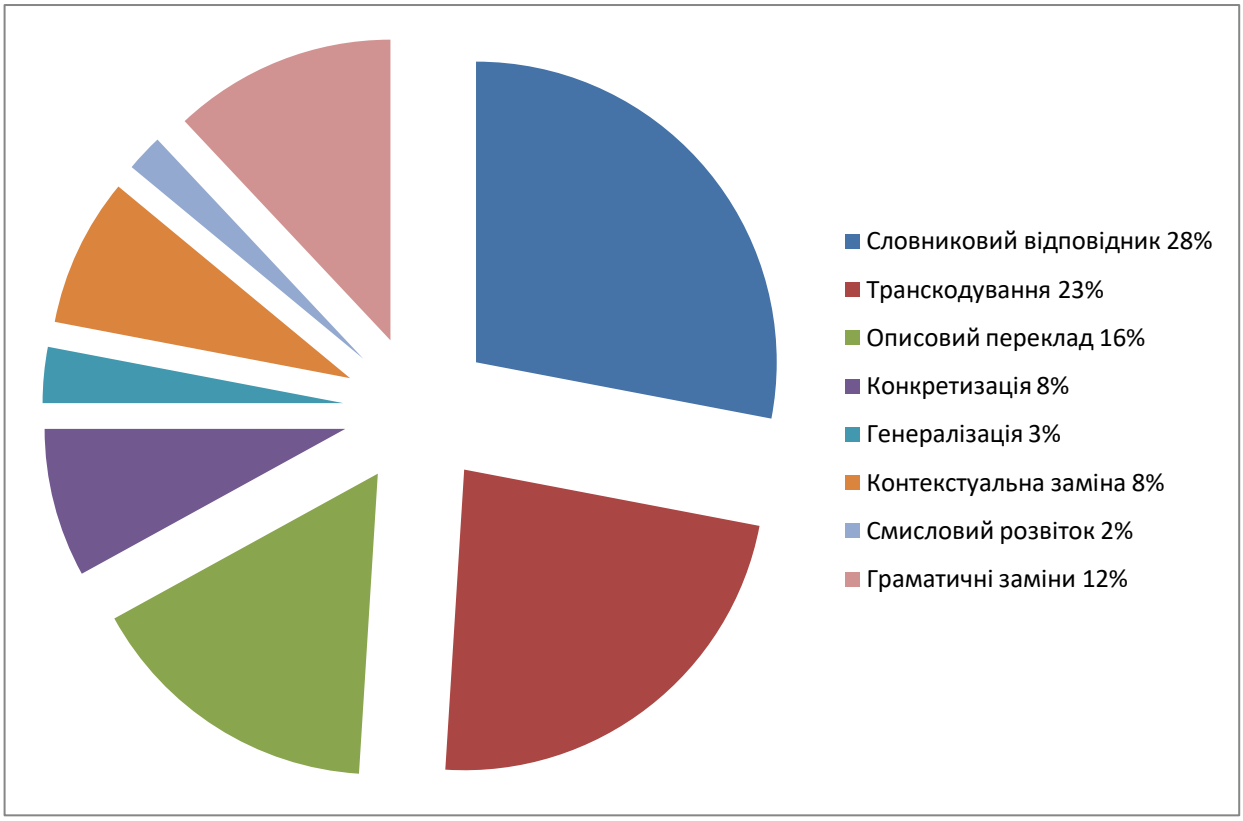
Семантичні процеси в англомовній терміносистемі кібербезпеки



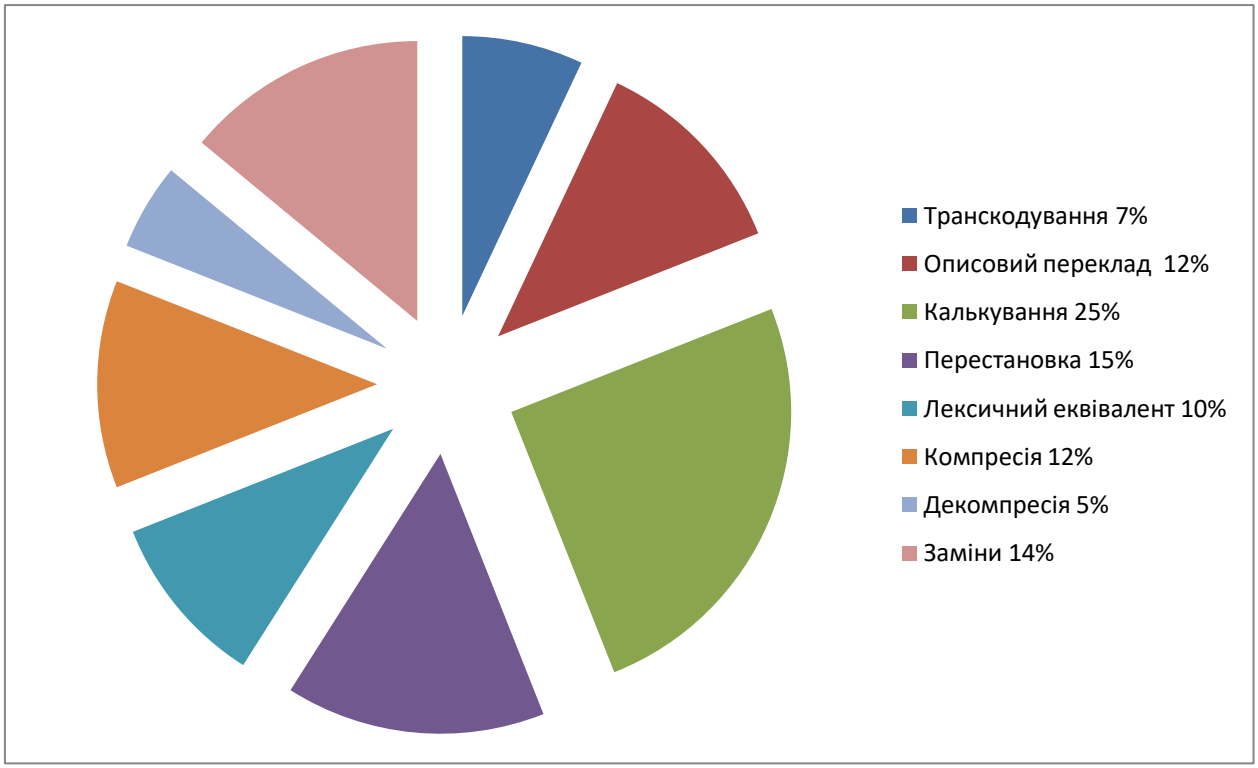
Тематичні групи англомовної терміносистеми кібербезпеки



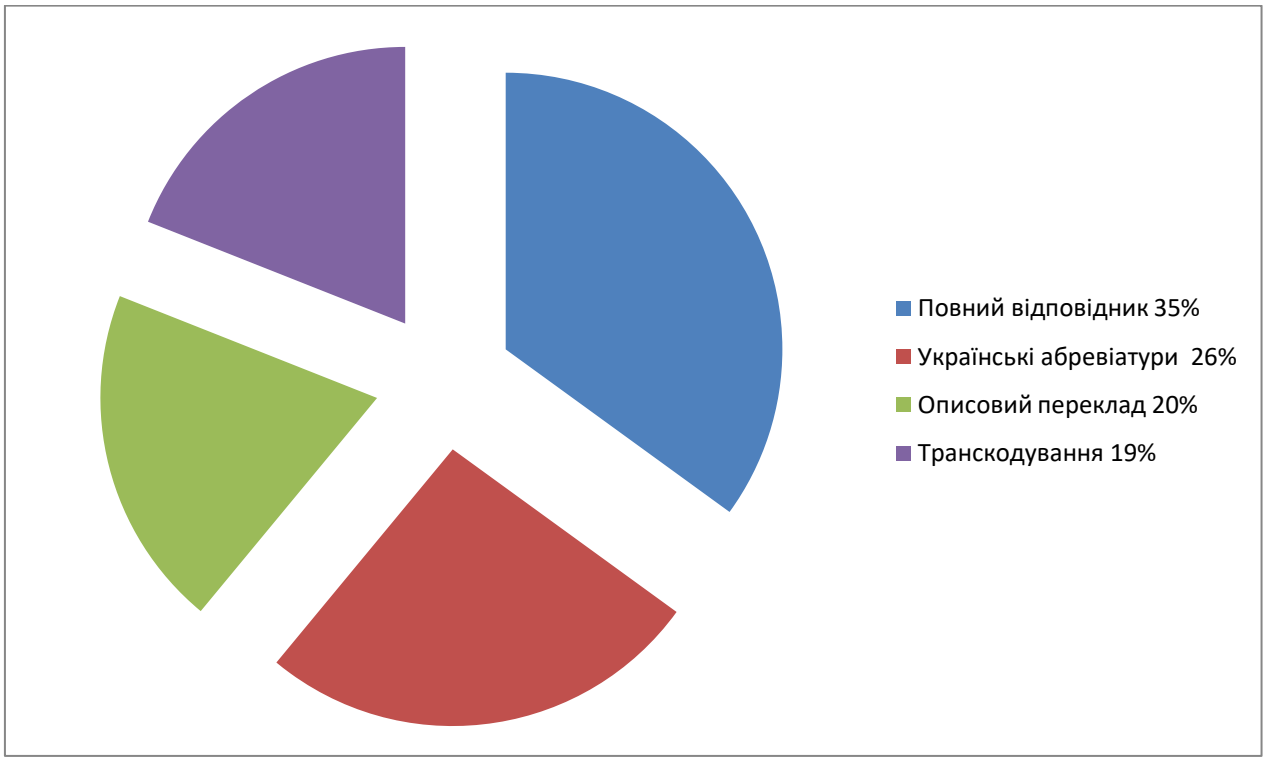
Способи перекладу англомовних однокомпонентних термінів кібербезпеки



Способи перекладу англомовних однокомпонентних термінів кібербезпеки



Способи перекладу англомовних термінів –скорочень кібербезпеки



Польова організація англомовних термінів кібербезпеки

Додаток В

Публікації

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

ТИЖДЕНЬ НАУКИ-2025

Гуманітарний факультет

Збірник тез доповідей щорічної
науково-практичної конференції серед студентів, викладачів, науковців,
молодих учених і аспірантів
14–18 квітня 2025 року

УДК 811.111’276.6:044
Кузнєцова І. В.[1], Животченко О. М.[2]
[1] канд. філол. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. ГФ-314м НУ «Запорізька політехніка»

ЩОДО ЕТИМОЛОГІЇ СЛОВА «КІБЕРБЕЗПЕКА»

Сучасні вітчизняні та зарубіжні дослідження в галузі термінознавства охоплюють не лише вже сформовані термінологічні системи, а й ті, що знаходяться на етапі становлення. Вони спрямовані на глибоке вивчення мовних процесів у науці, використовуючи широкий теоретичний та практичний досвід аналізу існуючих терміносистем. Останнім часом спостерігається зростаючий інтерес до термінологічної системи кібербезпеки, яка активно формується. Теоретичні аспекти її системного опису передбачають дослідження внутрішньосистемних зв’язків, історичної еволюції та розширення словотворчих можливостей. Важливим напрямом аналізу є вивчення лінгвокультурного аспекту семантики термінів кібербезпеки, що дозволяє простежити їхній вплив на комунікативні процеси у цій сфері.

З розвитком галузі з’являються нові поняття та відповідні терміни, які фіксуються у різних мовах, зокрема англійській та українській. Терміносистема кібербезпеки містить систему базових понять, що сформувалися історично та зберігають відносну стійкість у мовах-носіях цієї терміносистеми.

Як відомо, термін «кібербезпека» набув особливої актуальності у

Як відомо, термін «кібербезпека» набув особливої актуальності у зв’язку зі стрімким розвитком цифрових технологій та зростанням кількості кібератак у глобальному кіберпросторі. Поняття кібербезпеки охоплює заходи щодо захисту комп’ютерних систем, мереж та даних від зовнішніх загроз. Етимологічний аналіз цього терміна дозволяє прослідкувати його витоки від давньогрецького кореня, пов’язаного із поняттям управління, до сучасного розуміння захисту цифрового простору. Слово «кібербезпека» (англ. *cybersecurity*) є складним неологізмом, що походить від поєднання двох основ: «кібер-» (*cyber-*) та «безпека» (*security*). Термін «кібер-» має коріння в давньогрецькому слові *kybernetes* (κυβερνήτης), що означає «*керманич*» або «*пілот*» тобто мистецтво управління кораблем. Згодом цей термін досліджував французький учений

94

А. Ампер, а через сто років «вдруге відкрив» американець Н. Вінер [1, с. 56]. Це слово стало основою для наукового терміна «*кібернетика*» (*cybernetics*), який він увів у науковий обіг у 1948 році для позначення науки про управління системами та комунікацію між ними. Саме Н. Вінер уже ніби в наш час назвав кібернетику наукою про зв'язок у живих організмах і машинах.

Як відомо, кібернетика – наука про загальні закономірності процесів управління та передавання інформації в машинах, живих організмах і суспільстві, відповідно до тлумачного словника, наука про загальні закономірності процесів управління та передавання інформації в машинах, живих організмах і суспільстві.

Згодом, з розвитком цифрових технологій, приставка «кібер» почала використовуватися для позначення всього, що стосується комп’ютерних систем, мереж та віртуального простору.

Другий компонент – «безпека» (*security*) – має латинське походження (*securitas*), що означає «*спокій*», «*впевненість*», «*захищеність*». У контексті інформаційних технологій поняття набуло специфічного значення, яке охоплює захист, попередження ушкоджень, відновлення роботи систем і забезпечення конфіденційності інформації. В основі цього поняття лежить прагнення до забезпечення стійкості та надійності систем, що є важливим компонентом сучасного цифрового суспільства. Сучасне вживання цього елемента у складі складених термінів (*cyberspace, cybercrime, cyberattack*) свідчить про його універсальність і здатність адаптуватися до нових технологічних реалій [2].

адаптуванням до нових технологічних реалій [2].

Поєднання компонент «кібер» і «безпека» утворює термін, що означає забезпечення захищеності цифрових технологій та інформаційних систем від кібератак і зовнішніх загроз. За визначенням міжнародних стандартів, кібербезпека – це комплекс заходів, спрямованих на попередження, виявлення та нейтралізацію загроз у кіберпросторі. Сучасне розуміння цього терміну виникло в умовах постійного розвитку цифрових технологій та зростання кіберзагроз, що робить його актуальним для різних галузей знань і практичних застосувань. Термін «кібербезпека» з'явився в українській мові наприкінці XX – початку XXI століття у зв'язку з розвитком інформаційних технологій та загроз у цифровому середовищі [4].

З моменту широкого впровадження Інтернету у 1990-х роках термін «кібербезпека» зазнав значної еволюції. Спочатку поняття охоплювало суто технічні аспекти захисту мереж і систем, проте згодом воно розширилося і включило правові, соціальні та економічні аспекти. Зростання числа кібератак, витоків даних і шахрайства у цифровій сфері спонукало розробку нових методів захисту, що привело до появи

додаткових понять, таких як «кіберрезилієнтність» – здатність систем відновлювати свою роботу після атак. Це свідчить про те, що поняття кібербезпеки постійно адаптується до вимог часу і технологічного прогресу [3].

Проведений аналіз етимології терміну «кібербезпека» демонструє, що його сучасне значення є результатом складного історичного процесу, який поєднує давньогрецькі корені, розвиток кібернетики та стрімкий розвиток цифрових технологій. Синтез складових «кібер» та «безпека» створює міждисциплінарне поняття, що охоплює не лише технічний, але й соціально-психологічний аспект захисту інформаційних систем [2]. Сучасна термінологія характеризується високою структурною системністю та економією мовних ресурсів, що відповідає потребам цифрової епохи. Однак повна стандартизація термінів залишається відкритим питанням, яке потребує подальших досліджень і міждисциплінарного обговорення. Розуміння історичних витоків і еволюції поняття «кібербезпека» має важливе практичне значення для розробки ефективних стратегій захисту інформаційних систем та формування нормативно-правової бази у глобальному кіберпросторі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика [Електронний ресурс] / О. А. Баранов. – 2014. – № 2 (42). – С. 54–62. – Режим доступу : http://ippi.org.ua/sites/default/files/ 14boavpk.pdf (дата звернення: 2025.03.25).

(дата звернення: 2025.03.25).

2. Жовтяк В. А. Структурні особливості англомовних термінів кібербезпеки [Електронний ресурс] / В. А. Жовтяк // Закарпатські філологічні студії. – Режим доступу : https://doi.org/10.32782/tps2663-4880/2024.34.1.13 (дата звернення: 2025.03.21).

3.The Origins of a Term that Defines Our Industry [Electronic resource]. – Access mode : https://www.fortian.com.au/blog/what-is-cyber-security-the-origins-of-a-term-that-defines-our-industry.html (aceess date: 2025.03.22).

4.What’s in a Name? The Origin of Cyber- [Electronic resource]. – Access mode : https://www.ciso.inc/blog-posts/origin-cyber/ (aceess date: 2025.03.22).

Міністерство освіти і науки України
Національний університет «Запорізька політехніка»

МАТЕРІАЛИ
І Міжнародної науково-практичної конференції
«АКТУАЛЬНІ ПРОБЛЕМИ ДИСКУРСОЛОГІЇ, ПЕРЕКЛАДОЗНАВСТВА ТА МЕТОДИКИ ВИКЛАДАННЯ»

до 125-річчя
Національного університету «Запорізька політехніка»

21 листопада 2025 р.

Запоріжжя
2025

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) слабке 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 англомовної 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 :