International Science Journal of Education & Linguistics
2026; 5(2): 33-41
https://isg-journal.com/isjel/
doi: 10.46299/j.isjel.20260502.05
ISSN: 2720-684X

Антонімічні відношення в сучасній англомовній терміносистемі кібербезпеки

Владислав Жовтяк
Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна
ORCID 0009-0002-2043-7421

Анотація: У статті здійснено комплексний структурно-семантичний аналіз антонімічних відношень в англомовній терміносистемі кібербезпеки. Актуальність дослідження зумовлена динамічним розвитком цифрових технологій та стрімким поповненням спеціалізованої лексики, що потребує системного осмислення її парадигматичної організації. Антонімія розглядається не як стилістичне явище, властиве загальновживаній лексиці, а як структуроорганізувальний механізм терміносистеми, що відображає логічну архітектуру галузі та концептуальну бінарність кіберпростору.

Матеріалом дослідження слугував «Англо-український словник термінів з інформаційних технологій та кібербезпеки», з якого методом суцільної вибірки було виокремлено 142 антонімічні пари. Методологічну основу становить інтеграція логічної теорії опозицій, структурної семантики, компонентного аналізу та сучасного термінознавства. Антонімічні пари класифіковано на контрадикторні, контрарні, комплементарні та векторні. Компонентний аналіз дозволив визначити диференційні семи, що формують семантичну протилежність, а кількісний підрахунок – установити продуктивність кожного типу.

Результати засвідчили домінування контрадикторних антонімів (46%), що відображає бінарну логіку безпеки. Векторні антоніми (32%) репрезентують процесуальний характер галузі. Комплементарні пари (14%) формують структурні моделі в межах криптографічних і доступових систем, тоді як контрарні антоніми (8%) виявилися найменш продуктивними, що пояснюється прагненням технічної системи до чіткої класифікації станів.

Тематичне групування продемонструвало нерівномірний розподіл антонімії в межах груп. Найбільш репрезентативним є група «Безпека та її порушення» (21,8%), що формує концептуальне ядро терміносистеми. Високі показники також зафіксовано у сферах «Криптографія» (19,0%) та «Доступ та авторизація» (16,9%). Отримані результати підтверджують, що антонімія виконує когнітивну та структурну функцію, моделюючи ключові опозиції «захист – загроза», «доступ – обмеження», «шифрування – дешифрування».

Ключові слова: терміносистема кібербезпеки, антонімія, контрадикторні антоніми, векторна антонімія, термінологія, структурна семантика, тематична група, парадигматичні відношення.

1. Вступ

Сучасний розвиток інформаційних технологій та поширення цифрових загроз сприяють стрімкому поповненню англомовної терміносистеми кібербезпеки новими поняттями та термінами. У цьому контексті антонімічні відношення набувають особливої важливості, оскільки вони забезпечують точність, однозначність і уніфікацію термінологічних одиниць у науково-технічних та професійних комунікаціях. Вони допомагають чіткіше структурувати термінологічне поле, визначати протилежні явища чи процеси, що є критично важливим у сфері інформаційної безпеки, де помилка у розумінні терміна може призвести до серйозних наслідків.

2. Об'єкт і предмет дослідження

Об’єктом дослідження виступає англомовна терміносистема кібербезпеки як сукупність спеціалізованих лексичних одиниць, а його предметом – антонімічні відношення в цій терміносистемі, їх структурно-семантичні типи та моделі творення.

Узагальнюючи сучасні лінгвістичні підходи до визначення терміна, пропонуємо розглядати його як окрему лексичну одиницю або словесну конструкцію, що репрезентує спеціалізовану інформаційно-когнітивну структуру та номінує професійне поняття в межах певної галузі знань [1]. Термін функціонує як інструмент фахової комунікації, покликаний забезпечувати точність, однозначність і концептуальну впорядкованість передавання спеціалізованої інформації. Його сутність полягає не лише в номінативній функції, а й у здатності інтегруватися в цілісну терміносистему, де кожна одиниця перебуває у взаємозв’язках з іншими елементами на основі логіко-поняттєвих відношень.

Аналіз чинного законодавства України та нормативно-правових актів провідних держав світу засвідчує наявність дефініційної варіативності й певної семантичної невизначеності понять, що формують ядро терміносистеми кібербезпеки. Відсутність уніфікованих підходів до тлумачення базових категорій зумовлює неоднорідність їх інтерпретації в науковому, правовому й прикладному дискурсах, що, своєю чергою, ускладнює гармонізацію міжнародної термінології у сфері цифрової безпеки.

Згідно з глосарієм ресурс-центру комп’ютерної безпеки National Institute of Standards and Technology, кібербезпека визначається як діяльність, спрямована на запобігання пошкодженню, забезпечення захисту та відновлення комп’ютерів, електронно-комунікаційних систем і сервісів, дротових та електронних комунікацій, включно з інформацією, що в них міститься, з метою гарантування її доступності, цілісності, конфіденційності та невідмовності (переклад наш). У цьому визначенні акцентовано функціонально-процесуальний аспект поняття та його зв’язок із базовими принципами інформаційної безпеки [2].

Відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека трактується як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства й цифрового комунікативного середовища, а також своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці у кіберпросторі. У цьому випадку поняття розкривається переважно через безпеково-державницьку парадигму, що відображає стратегічний та соціально-політичний вимір кібербезпеки [3].

Отже, зіставлення наведених дефініцій свідчить про багатовимірність концепту кібербезпеки, який поєднує технічний, організаційний, правовий і соціальний аспекти. Англомовна термінологія цієї галузі загалом відповідає сучасним вимогам до термінів, зокрема таким як системність, дефінітивність, точність, контекстуальна незалежність, стислість, однозначність, експресивна нейтральність та інтернаціональний характер. Терміносистема кібербезпеки постає як цілісна структурована сукупність взаємопов’язаних одиниць, організованих на поняттєвому, ієрархічному та концептуальному рівнях, що забезпечує її функціональну стабільність і здатність до подальшого розвитку в умовах динамічних технологічних змін. Антонімія у спеціальній лексиці має системний характер і відображає логічну організацію предметної галузі.

3. Мета та задачі дослідження

Мета дослідження – здійснити комплексний аналіз антонімічних відношень в англомовній терміносистемі кібербезпеки, визначити їх структурно-семантичні типи та моделі формування. Для досягнення поставленої мети передбачено розв’язання таких завдань:

проаналізувати теоретичні підходи до вивчення антонімії в сучасній лінгвістиці, встановити типи антонімічних опозицій та моделі їх творення.

4. Аналіз літератури

Проблематика антонімічних відношень у термінології посідає вагоме місце в сучасних лінгвістичних дослідженнях. Аналіз наукових праць українських дослідників засвідчує комплексний підхід до вивчення парадигматичних відношень у спеціальних терміносистемах.

У статті О. В. Колган «Антонімія української гірничої термінології» (2008) здійснено аналіз структурних і семантичних типів антонімів у галузевій терміносистемі. Дослідниця доводить, що антонімія в термінології має системний характер і відображає логічні опозиції, закладені в самій науковій картині світу. Авторка виокремлює лексичні, словотвірні та контекстуальні антоніми, підкреслюючи продуктивність префіксальної моделі творення термінів із протилежним значенням [4]. Праця є важливою для розуміння механізмів формування антонімічних пар у спеціальних мовах.

Проблему термінологічної антонімії на теоретичному рівні розглядає О. І. Павлова (2003). У своїй роботі дослідниця акцентує увагу на специфіці антонімії в терміносистемах порівняно із загальновживаною лексикою. Зокрема, наголошується на тому, що термінологічна антонімія ґрунтується не лише на семантичній протилежності, а й на логічній взаємозумовленості понять. Науковець пропонує класифікацію антонімів за типом протиставлення (градуальні, комплементарні, векторні), що має важливе методологічне значення для аналізу спеціальної лексики [5].

Антонімічні відношення у вузькогалузевій терміносистемі досліджує Н. А. Цимбал (1998) на матеріалі термінології органічної хімії. Дослідниця доводить, що антонімія є одним із засобів структуризації наукового знання, оскільки дозволяє систематизувати поняття за принципом протиставлення. У роботі простежено словотвірні моделі антонімії, зокрема використання префіксів для вираження протилежності, що є релевантним для аналізу сучасних технічних терміносистем [6].

Особливості антонімічних відношень у англійській галузевій терміносистемі розглянуто у дослідженні О. В. Янковець (2019), присвяченому прикордонній термінології. Авторка аналізує структурні моделі антонімічних пар та підкреслює роль контексту у встановленні протилежності термінів. У роботі зазначено, що антонімія в спеціальній лексиці має чітко визначений функціональний характер і відображає нормативні параметри професійної діяльності [7].

Вагомий внесок у дослідження галузевої антонімії зробила Н. Р. Біян (2013) у статті «Антонімічні терміни галузі туризму в англійській мові». Вона аналізує структурно-семантичні особливості антонімічних пар у терміносистемі туризму та доводить, що протиставлення в спеціальній лексиці зумовлене насамперед логічною організацією професійної сфери. Дослідниця виокремлює лексичні та словотвірні антоніми, звертаючи увагу на продуктивність афіксальних моделей (зокрема префіксальної опозиції) та на роль контексту у виявленні протилежності. Праця демонструє, що антонімія в англомовній терміносистемі має системний характер і виконує функцію чіткого структурування галузевих понять, що є релевантним для аналізу термінології кібербезпеки [8].

Теоретичне осмислення взаємозв'язку синонімії та антонімії у процесах термінотворення запропоновано у праці Р. І. Дудок (2013) «Синонімічно-антонімічні відношення у термінотворенні». Дослідниця розглядає парадигматичні відношення як важливий чинник формування та розвитку терміносистем і підкреслює, що синонімія й антонімія в термінології не є випадковими явищами, а відображають етапи становлення наукового знання, конкуренцію термінів і процеси стандартизації. У роботі наголошується на тому, що синонімічні ряди часто виникають унаслідок запозичень або паралельного функціонування національних та іншомовних відповідників, тоді як антонімічні пари формують концептуальні

опозиції в межах певної галузі [9]. Такий підхід дозволяє розглядати синонімічно-антонімічні відношення як взаємопов'язані механізми системної організації термінології.

Отже, проаналізовані праці засвідчують, що антонімічні відношення є системним явищем в галузевих терміносистемах і виконують важливу структуроутворювальну функцію. Досвід дослідження гірничої, хімічної, прикордонної термінології, тощо створює теоретичне підґрунтя для аналізу відповідних відношень в англомовній терміносистемі кібербезпеки, де процеси термінотворення та стандартизації є особливо динамічними.

Водночас аналіз джерел свідчить про відсутність комплексних досліджень, присвячених системному вивченню антонімічних відношень саме в англомовній терміносистемі кібербезпеки. З огляду на динамічність розвитку цієї галузі, активні процеси термінотворення, запозичення та стандартизації, проблема парадигматичних відношень у межах кібербезпекової термінології потребує окремого комплексного аналізу. Саме це зумовлює наукову новизну й доцільність обраного напряму дослідження.

5. Методи досліджень

Антонімія в терміносистемі кібербезпеки має системний і концептуально вмотивований характер. Дослідження антонімії в терміносистемі кібербезпеки здійснюється на перетині логічного та структурно-семантичного підходів. Методологічною основою слугує положення про те, що термінологія відображає концептуальну організацію спеціального знання, а семантичні опозиції є засобом її внутрішньої структуризації. Антонімія в цьому випадку не розглядається як стилістичний ресурс, властивий загальномовній лексиці, а інтерпретується як інструмент категоризації та формалізації професійного досвіду.

У роботі використано класифікацію антонімів на контрадикторні, контрарні, комплементарні та векторні, що не належить одному авторові, а сформувалася на перетині логіки, структурної семантики та когнітивної лінгвістики. В її основі лежить арістотелівська традиція логічної опозиції, згодом розвинена в межах аналітичної філософії та сучасної лексичної семантики.

У структурній семантиці системне осмислення антонімії здійснив Дж. Лайонз , уперше чітко відділивши логічну опозицію від власне лексичної антонімії. У його концепції антонімія постає як структурований тип семантичних відношень, інтегрований у систему лексикону [10].

Подальший розвиток типології здійснив А. Круз, виокремивши *complementary opposites, gradable antonyms, converses, reversives ma directional opposites* [11]. Особливо продуктивними для аналізу технічної термінології є *reversives i directional opposites*, що відображають векторні або процесуальні зміни стану (наприклад, типу *encrypt / decrypt, connect / disconnect*). У межах цієї типології антонімія розглядається як спосіб моделювання динамічних відношень у спеціалізованих галузях знання.

Важливий внесок у пояснення механізмів антонімії зроблено в межах компонентного аналізу, розробленого Дж. Кац і Дж. Фодор [12]. У цьому підході антонімія трактується як опозиція диференційних сем, тобто мінімальних смислових ознак. Наприклад, протиставлення secure / insecure може бути пояснене через наявність або відсутність семи [+protected]. Така інтерпретація дозволяє обґрунтувати високу продуктивність префіксальної антонімії в термінології кібербезпеки.

У сучасній лексичній семантиці антонімія осмислюється також у когнітивному вимірі. Так, М.Л. Мерфі наголошує, що антонімія є не лише формально-логічним, а й когнітивним механізмом структурування знання [13].

Українська лінгвістична традиція також розглядає антонімію як системну категорію лексики. Ф. Бацевич аналізує семантичні відношення як механізми організації мовної системи [14], а М. Кочерган підкреслює логічну природу контрадикторних і контрарних відношень [15].

Матеріалом нашого дослідження слугував *Англо-український словник термінів з інформаційних технологій та кібербезпеки* [16], який містить 4000 одиниць.

Отже, запропонована в дослідженні класифікація антонімів у словнику кібербезпеки ґрунтується на поєднанні логічної моделі Арістотеля, семантичної теорії Дж. Лайонса, розгорнутої типології А. Круза, компонентного аналізу Дж. Каца і Дж. Фодора, когнітивної інтерпретації М. Мерфі.

Контрадикторність встановлюється на основі критерію повного взаємного заперечення значень, що виявляється через деривaційні маркери заперечення або бінарну семантичну структуру поняття. Контрарність визначається через наявність градуальної шкали, в межах якої фіксуються протилежні полюси. Комплементарність установлюється на підставі взаємодоповнювального характеру понять, які формують структурну пару в межах однієї концептуальної моделі. Векторність аналізується як протилежність напрямку процесу або дії, що є особливо релевантним для технічної термінології, де значна частина номінацій позначає операції.

Методика передбачає поєднання суцільної вибірки термінів із словника, компонентного аналізу їх значень та контекстуальної верифікації у фахових джерелах. Компонентний аналіз дозволяє встановити набір сем, що формують опозицію, та визначити тип антонімічного зв’язку.

Кількісний підрахунок здійснюється з урахуванням повторюваності структурних моделей, що дає змогу визначити продуктивність кожного типу антонімії. Отримані показники інтерпретуються не лише статистично, а й концептуально, з огляду на те, що терміносистема кібербезпеки функціонує в умовах бінарної логіки «захист – загроза», «доступ – обмеження», «шифрування – дешифрування». Саме ця концептуальна бінарність пояснює домінування контрадикторних та векторних опозицій.

Таким чином, методичні засади дослідження ґрунтуються на інтеграції логічної теорії опозицій, лексичної семантики та сучасного термінознавства. Такий підхід забезпечує системність аналізу та дозволяє розглядати антонімію не як периферійне явище, а як структурний принцип організації терміносистеми кібербезпеки.

Загалом у словнику було зафіксовано 142 антонімічні пари, які розподіляються наступним чином:

1. Контрадикторні антоніми виражають відношення заперечення, коли один член пари логічно виключає інший, а третій варіант неможливий. У досліджуваній термінології кібербезпеки цей тип є найпродуктивнішим і становить близько половини усіх виявлених прикладів (65 пар, 46%). Їх характерною ознакою є деривація за допомогою префіксів *un-, in-, non-, dis-, de-, наприклад: authorized – unauthorized, secure – insecure, encrypted – unencrypted, trusted – untrusted, compliant – non-compliant, enabled – disabled, activated – deactivated, verified – unverified.* Отже, контрадикторність відображає бінарну логіку кібербезпеки: доступ дозволено / доступ заборонено, система захищена / система не захищена.

2. Комплементарні антоніми, які складають близько сьомої частини виявлених антонімічних пар (20, 14%), позначають взаємодоповнювальні, але не обов’язково деривaційно пов’язані поняття. Вони не мають ступеневої градації, але формально не є заперечними формами одне одного, наприклад: *public key – private key, symmetric encryption – asymmetric encryption, plaintext – ciphertext, login – logout, online – offline*. Такі поняття взаємно виключаються, але утворюють структурну пару в межах однієї концептуальної моделі. Наприклад, *public key* функціонує лише в антонімічному співвідношенні з *private key*. Ці пари реалізують структурну двочленність криптографічної системи.

3. Контрарні антоніми виражають протилежні полюси певної шкали, допускаючи проміжні значення. У терміносистемі кібербезпеки цей тип менш поширений, оскільки галузь тяжіє до бінарності, наприклад: *secure – vulnerable, active – passive, open – closed, internal – external.* Наприклад, між *secure* і *vulnerable* можливий спектр станів безпеки. Система може

бути частково захищеною, тобто знаходитись між двома полюсами. Контрарність відображає ступеневу модель ризику та загроз.

4. Векторні антоніми позначають протилежні напрями дії або процесу. Вони є особливо характерними для кібербезпекової термінології, оскільки галузь описує процеси. До прикладу: *encrypt – decrypt, encode – decode, connect – disconnect, grant – revoke, install – uninstall, upload – download, lock – unlock.* Ці пари відображають протилежний напрямок операції в межах одного процесу. Векторна антонімія становить 32% усіх випадків і є другою за продуктивністю після контрадикторної.

Зобразимо отримані дані в таблиці 1.

Таблиця 1. Типи антонімії в англомовній термінології кібербезпеки

Типи антонімів	Кількість антонімічних пар	Відсотки
контрадикторні	65	46%
векторні	45	32%
комплементарні	20	14%
контрарні	12	8%
Всього	142	100%

З метою виявлення системності антонімічних відношень в англомовній терміносистемі кібербезпеки було здійснено також їх тематичне групування за семантичними мікрополями. Такий підхід дозволяє простежити функціонування антонімії не лише на рівні окремих лексичних опозицій, а й у межах структурованих підсистем галузі. У результаті аналізу виокремлено такі тематичні групи антонімів: криптографія (*encryption – decryption, plaintext – ciphertext, public key – private key*), доступ та авторизація (*authorized – unauthorized, allow – deny, login – logout*), безпека та її порушення (*secure – insecure, protection – exposure, integrity – corruption*), мережеві процеси (*connect – disconnect, online – offline, upload – download*), шкідливі процеси та протидія (*attack – defense, exploit – patch, infect – disinfect*), а також дані та керування системою (*input – output, enable – disable, backup – data loss*).

Представимо отримані кількісні дані у таблиці 2.

Таблиця 2. Тематична класифікація антонімів в англомовній термінології кібербезпеки

Тематична група	Кількість антонімічних пар	Відсотки
Безпека та її порушення	31	21,8%
Криптографія	27	19,0%
Доступ та авторизація	24	16,9%
Шкідливі процеси	22	15,5%
Дані та керування	20	14,1%
Мережеві процеси	18	12,7%
Всього	142	100%

6. Результати досліджень

Як видно з таблиці 1, у досліджуваному матеріалі переважають контрадикторні антоніми, які становлять близько половини аналізованих антонімічних пар (46%), на 20 пар менше представлено векторні антоніми (третина матеріалу, 32%), комплементарні становлять сьому частку (14%), а найменше представлено контрарні антоніми (8%).

Кількісний тематичний аналіз 142 антонімічних пар, представлений у таблиці 2, засвідчив нерівномірний розподіл антонімії у межах тематичних мікрополів терміносистеми кібербезпеки. Найбільш репрезентативним виявилося мікрополе «Безпека та її порушення» (21,8%). Друге місце посідає мікрополе «Криптографія» (19,0%). Мікрополе «Доступ та авторизація» охоплює 24 пари (16,9%). Далі за схожими кількісними показниками йдуть групи

«Шкідливі процеси» (15,5%) та «Дані та керування» (14,1%). Найменш представленим є мікрополе «Мережеві процеси» (12,7%).

Таким чином, у терміносистемі кібербезпеки переважають контрадикторні антоніми, що свідчить про наявність чітких полярних концептів у мовному представленні понять. Кількісний розподіл антонімічних пар у тематичних групах показує нерівномірність їхньої репрезентації, з переважанням груп «Безпека та її порушення» та «Криптографія». Менш представленими є сфери «Мережеві процеси» та «Дані та керування», що вказує на специфіку фокусування термінології на критично важливих аспектах кібербезпеки. Загалом, аналіз підкреслює тематичну концентрацію антонімічних відношень у ключових сферах дисципліни.

7. Перспективи подальшого розвитку досліджень

Перспективи подальших досліджень убачаємо в поглибленому аналізі синонімічних відношень у словнику англомовної термінології кібербезпеки, а також у вивченні функціонування антонімічних і синонімічних кореляцій цих термінів у межах кінодискурсу.

8. Висновки

Отже, найпродуктивнішим типом є контрадикторна антонімія, що відображає бінарну логіку безпеки (дозволено / заборонено, захищено / не захищено). Векторна антонімія демонструє процесуальний характер галузі. Комплементарні пари формують структурні моделі (public/private, symmetric/asymmetric). Контрарність у кібербезпеці обмежена, оскільки технічні системи прагнуть чіткої класифікації станів. Таким чином, антонімія у словнику кібербезпеки є не лише мовним явищем, а відображенням логічної архітектури галузі, що переважно базується на бінарних опозиціях та процесуальних векторах.

Запропоноване тематичне групування демонструє, що антонімія в терміносистемі кібербезпеки виконує структуроорганізувальну функцію, відображаючи ключові концептуальні опозиції галузі та логіку протиставлення процесів, станів і ролей.

Найбільш репрезентативним виявилося мікрополе «Безпека та її порушення» (21,8%), що свідчить про те, що концептуальне ядро досліджуваної системи вибудовується навколо бінарної опозиції *захист – загроза*, яка визначає когнітивну структуру галузі. Саме в цьому полі найвиразніше реалізується протиставлення стабільності та ризику, контрольованості та компрометації. Висока частотність антонімів у секторі «Криптографія» (19,0%). зумовлена процесуальною природою шифрування, де кожна операція передбачає зворотну. Це поле формує операційний каркас системи безпеки. Антонімія у групі «Доступ та авторизація» (16,9%) відображає логіку дозволу й обмеження, що є базовим принципом інформаційної безпеки. Значна кількість опозицій у цій групі підтверджує нормативний характер галузі, орієнтованої на регулювання прав доступу. Антонімічні зв’язки у групі «Шкідливі процеси» (15,5%) відображають динаміку протидії: атака — захист, експлуатація — усунення вразливості. Це поле демонструє конфліктну модель функціонування кіберпростору. Мікрополе «Дані та керування» (14,1%) репрезентує операційно-адміністративний рівень системи, де протиставлення пов’язані з управлінням, інсталяцією, запуском і зупинкою процесів. Хоча кількісно мікрополе «Мережеві процеси» (12,7%) поступається іншим групам, його роль є структурно важливою, адже саме мережеві дії забезпечують функціонування всієї інфраструктури.

Загалом розподіл демонструє, що антонімія в англомовній терміносистемі кібербезпеки концентрується насамперед у зонах концептуальної напруги — там, де відбувається протиставлення безпеки й загрози або реалізується операційна оберненість процесів.

Список літератури:

1) Жовтяк, В. (2024). Лінгвістичні маркери англомовних термінів кібербезпеки. *Grail of Science*, 414–416. https://doi.org/10.36074/grail-of-science.06.09.2024.053

2) National Institute of Standards and Technology. (n.d.). *Glossary of cyber security terms*. https://csrc.nist.gov/glossary/term/cybersecurity

3) Закон України № 2163-VIII. (2017, жовтень 5). *Про основні засади забезпечення кібербезпеки України*. https://zakon.rada.gov.ua/laws/show/2163-19

4) Колган, О. В. (2008). Антонімія української гірничої термінології. *Проблеми української термінології*, (620), 200–203. http://vlp.com.ua/node/1148

5) Павлова, О. И. (2003). Особенности терминологической антонимии. У *Матеріали Міжнародної науково-методичної конференції "Треті Каразінські читання: методика і лінгвістика – на шляху до інтеграції"* (с. 134–136). Харківський національний університет імені В. Н. Каразіна.

6) Цимбал, Н. А. (1998). Антонімічні відношення в термінології органічної хімії. *Українська термінологія і сучасність*, 188–192.

7) Янковець, О. В. (2019). Особливості антонімічних відношень у англійській прикордонній терміносистемі. У *Гуманітарні, природничі та точні науки як фундамент суспільного розвитку: VIII Всеукраїнська науково-практична конференція* (с. 71–73).

8) Біян, Н. Р. (2013). Антонімічні терміни галузі туризму в англійській мові. *Наукові записки. Серія "Філологічна"*, (36), 6–10. http://nbuv.gov.ua/UJRN/Nznuoaf_2013_36_4

9) Дудок, Р. І. (2013). Синонімічно-антонімічні відношення у термінотворенні. *Записки з романо-германської філології*, 1(30). http://www.irbis-nbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/zrgf_2013_1_11.pdf

10) Lyons, J. (1977). *Semantics* (Vols. 1–2). Cambridge University Press.

11) Cruse, D. A. (2000). *Meaning in language: An introduction to semantics and pragmatics*. Oxford University Press.

12) Katz, J. J., & Fodor, J. A. (1963). The structure of a semantic theory. *Language, 39*(2), 170–210.

13) Murphy, M. L. (2003). *Semantic relations and the lexicon*. Cambridge University Press.

14) Бацевич, Ф. С. (2004). *Основи комунікативної лінгвістики*. Академія.

15) Кочерган, М. П. (2010). *Загальне мовознавство*. Академія.

16) Гладун, А. Я., Пучков, О. О., Субач, І. Ю., & Хала, К. О. (2018). *Англо-український словник термінів з інформаційних технологій та кібербезпеки*. ІСЗЗІ КПІ ім. Ігоря Сікорського.

Antonymic relations in the modern english cybersecurity terminology system

Vladyslav Zhovtiak
Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine
ORCID 0009-0002-2043-7421

Abstract: The article presents a comprehensive structural and semantic analysis of antonymic relations in the modern English cybersecurity terminology system. The relevance of the study is stipulated by the rapid development of digital technologies and the continuous expansion of specialized vocabulary, which requires systematic linguistic interpretation. Antonymy is treated not as a stylistic phenomenon typical of general language but as a structural principle that reflects the logical architecture of the field and the conceptual binary nature of cyberspace.

The research material was drawn from the *English-Ukrainian Dictionary of Information Technology and Cybersecurity Terms*, from which 142 antonymic pairs were identified through continuous sampling. The methodological framework integrates logical theory of oppositions,

structural semantics, componential analysis, and contemporary terminology studies. The identified pairs were classified into four types: contradictory, contrary, complementary, and vector antonyms. Componential analysis was applied to determine the differential semantic features forming opposition, while quantitative analysis enabled the identification of productive patterns.

The findings demonstrate the dominance of contradictory antonyms (46%), which reflect the binary logic of cybersecurity. Vector antonyms (32%) represent the procedural nature of the field. Complementary pairs (14%) structure key conceptual models within cryptographic and access systems, whereas contrary antonyms (8%) are the least productive, due to the tendency of technical systems toward clear state classification rather than gradability.

Thematic classification revealed an uneven distribution of antonymy across thematic groups. The most representative group is “Security and Its Violations” (21.8%), forming the conceptual core of the terminology system. Significant representation is also observed in “Cryptography” (19.0%) and “Access and Authorization” (16.9%). These results confirm that antonymy performs both cognitive and structural functions, modeling key oppositions such as protection vs. threat, access vs. restriction, and encryption vs. decryption.

Keywords: cybersecurity terminology, antonymy, contradictory antonyms, vector opposition, structural semantics, terminology studies, thematic groups, paradigmatic relations.