УДК 81'373.46:81'373.612.2
DOI https://doi.org/10.24195/2616-5317-2026-42.22

СТРУКТУРНО-СЕМАНТИЧНА КАТЕГОРИЗАЦІЯ МЕТАФОРИЧНИХ ТЕРМІНІВ СФЕРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (НА МАТЕРІАЛІ АНГЛІЙСЬКОЇ, ПОЛЬСЬКОЇ ТА УКРАЇНСЬКОЇ МОВ)

Олег В. Тищенко

доктор філологічних наук, професор,
професор кафедри іноземних мов та перекладознавства
Львівський державний університет безпеки життєдіяльності,
Львів, Україна
професор філософського факультету
Університет Св. Кирила і Мефодія в Трнаві,
Трнава, Словаччина
e-mail: olkotiszczenko@gmail.com
ORCID ID: https://orcid.org/0009-0009-0811-2123
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57834809700

Марина Кучеренко

аспірантка кафедри іноземних мов та перекладознавства, викладач кафедри іноземних мов та перекладознавства
Львівський державний університет безпеки життєдіяльності,
Львів, Україна
e-mail: stepaniyuk@gmail.com
ORCID ID: https://orcid.org/0000-0002-4803-8089

АНОТАЦІЯ

У статті розглянуто когнітивно-інфомаційні засади термінів на позначення комп'ютерної безпеки, визначено їхні тематичні групи, пов'язані з ними ризики та загрози в сучасному цифровому просторі та дискурсивних практиках у неблизькоспоріднених германських та слов'янських терміносистемах.

Здійснено структурно-семантичний аналіз терміносистеми інформаційного захисту, зокрема, архітектури інформаційного простору, національної та міжнародної безпеки (предметні реалії на позначення розвідницької та шпигунської діяльності, нелегальні наркотрафіки, типи пасток тощо), системного адміністрування, комп'ютерних загроз з огляду на традиційні загальномовні та концептуальні метафори різних типів, їхню взаємодію та взаємопроникнення, типологію концептуальних сфер.

Виявляються онтологічні та прагматичні механізми семантичного термінотворення метафоричних термінів в англійській, українській та польській мовах, визначаються сфери їх концептуальної інтеграції, простежуються когнітивно-ономасіологічні засади термінологічної номінації (колірні, смакові, сенсорно-чуттєві, слухові, температурні тощо), встановлюються випадки таксономії, синонімії та антонімії як вузькоспеціальних, так і міжгалузевих метафоричних позначень.

Аналіз продемонстрував, що доменами для метафоричних термінів можуть бути медицина, військова сфера, метали та субстанції, родинні стосунки, архітектурні метафори, концептосфера clean-dirty, life-death тощо.

На окрему увагу заслуговує аналіз складних метафоричних термінів із погляду їх словотвірної та семантичної деривації та сполучуваності, їх моделювання за структурно-граматичною і семантико-мотиваційною ознаками.

Матеріалом для дослідження слугували фахові словники з інформаційної та кібербезпеки в трьох мовах, а також англомовні документи, дотичні до сфери захисту цифрової інформації.

Ключові слова: *інформаційна безпека, термінологічна номінація, типологія метафор, концептуальна інтеграція, структурно-граматична модель.*

Вступ. «Знання у вигляді інформації вербалізується та структурується згідно із законами мовної системи та фіксується й поширюється через мову. Як у генофонді зафіксовано інформаційний потенціал біологічних організмів, так і в знакових системах – інтелектуальний потенціал суспільства. Тому саме мова як інструмент мислення, пізнання й комунікації постійно еволюціонує і виступає об'єктом соціального наслідування, що обумовлює способи та можливості фіксації і передавання інформації як необхідної умови прогресу цивілізації» (Міщенко 2014: 5). У цьому контексті особливої ваги набуває мовна репрезентація фундаментальних категорій життєдіяльності, серед яких ключове місце посідає категорія безпеки. Адже в межах наукового дискурсу

безпека – це такі умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень (Заплатинський 2012: 45).

У Передмові до «Словника з інформації та інформаційної безпеки» Л. Г. Чистоклетов, О. Л. Хитра наголошують на необхідності адекватного розкриття професійних термінів, які наближені до сучасних проблем забезпечення інформаційної безпеки та визначеного кола діяльності суб'єктів, яким, згідно з їхнім правовим статусом, покладено зобов'язання дотримуватися відповідно до законодавства організаційно-правових заходів щодо запобігання, своєчасного виявлення, припинення чи нейтралізації реальних і потенційних загроз. Вагомість такої лексикографічної праці набуває глибинного змісту у звязку із «швидкоплинним процесом інформатизації суспільства» (Чистоклетов, Хитра 2023: 21).

Разом із тим при розгляді типів соціально-політичних небезпек дослідники звертають увагу на суттєвий вплив сучасних інформаційних технологій на особистість та безпеку суспільства і кібербезпеку й на інформаційно-психологічний вплив на людину, щоби змінити її поведінку, використати особисті дані, зокрема йдеться про інформаційні війни, вірусні атаки (Левченко, Землянська та ін. 2019: 33).

Варто зауважити, що в предметне поле інформаційної безпеки входять такі поняття та категорії: стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність і невірогідність інформації, яка використовується; негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних

інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України (Кушнерьов 2021).

У деяких комплексних рефлексіях із зазначеної проблематики увагу зосереджено на структурі інформаційного впливу, інструментах інформаційної війни загалом, комунікативних і когнітивно-психологічних особливостях системи інформаційних маніпуляцій (Худолій 2022: 1).

З огляду на сказане особливого значення набуває проблема державної зради та колабораційної діяльності загалом (див. детальніше: збірник «Нормативно-правові акти у сфері воєнної безпеки України» (2023) та практичний посібник «Розслідування колабораційної діяльності» (Письменський, Головкін та ін. 2023).

Той факт, що термінологія як складова частина мови розвивається за законами, властивими мові в цілому, дозволяє стверджувати, що семантична природа терміна не суперечить наявності в ньому експресивно-емоційних нашарувань, а подібні напластування не позбавляють терміна його сутності і не заважають виконувати головну функцію – позначати спеціальне поняття.

Найяскравішим доказом цього слугують терміни, утворені способом метафоричного переосмислення. При цьому метафоричне перенесення дехто розглядає як головний канал проникнення зазначених властивостей до терміносистем (Кришталь 2003: 4).

Актуальність студії. Нагальною є необхідність з'ясування впливу внутрішньої форми на значення терміна, відображення в ній історико-культурного та комунікативно-прагматичного аспектів мовної дійсності, аналіз структурно-семантичних особливостей англомовних термінів інформаційної галузі, відтак, визначення морфологічних та семантичних шляхів формування номенклатури інформаційної безпеки, що передбачає застосування сучасних міжпарадигмальних методик аналізу до механізмів термінологічної номінації.

У пропонованій розвідці пропонується вирішення таких основних **завдань:** виявити склад і типологію когнітивних метафор та з'ясувати специфіку їх концептуалізації у сфері інформаційної та кібербезпеки; в окремих випадках простежити когнітивно-ономасіологічні ознаки, покладені в основу їх внутрішньої форми та з'ясувати їх парадигмально-таксономічні зв'язки, мотиваційні ознаки (колоративні, сенсорно-звукові, температурні і т.н.), антонімічне протиставлення термінів тощо; уточнити сфери концептуальної метафоричної інтеграції з огляду на взаємодію концептофер у розглянутих термінологічних одиницях у межах відповідних термінологічних груп; виявити моделі семантичної та словотвірної деривації окремих метафоричних складних термінів з огляду на їхню сполучуваність та зв'язок з іншими субгалузями.

Матеріалом для дослідження слугували фахові лексикографічні праці та спеціалізовані видання, зокрема: «Словник ключових понять та абревіатур сектору безпеки» за заг. редакцією І.І. Мусієнка (далі – СКПСБ) (Мусієнко 2014).

«Англо-український глосарій термінів ІТ-технологій та кібербезпеки» (далі – АУГІТ) (Пальчевська та ін. 2025), «Словник з інформації та інформаційної безпеки» (Чистоклетов, Хитра 2023), термінологічний довідник «Інформаційна безпека» (Богуш та ін. 2004) та «Słownik terminów z zakresu bezpieczeństwa narodowego» (далі – STBN) (Zdrodowski 2008).

Крім того, залучено спеціальні англомовні джерела, зокрема, посібник «Virtualization for Security Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting» (Hoopes 2009).

Як і будь-яка інша галузева термінологія, термінологія інформаційної безпеки та комп'ютерної безпеки має свою специфічну концептуальну і семантичну структуру. Досліджуючи термін як носій когнітивної інформації, слід орієнтуватися на ідеї тих дослідників (Іващенко 2006; Стасюк 2020), які прирівнюють спеціальний термін до концепту, позаяк за

кожним терміном закріплена своєрідна система цінностей та уявлень, досвіду і стереотипів професійної діяльності.

Когнітивна ономасіологія вивчає номінативні одиниці мови з урахуванням людського досвіду, когніції, відчуттів. Цей гібридий напрям зорієнтований на доробок традиційного словотвору (К. Г. Городенська, В. О. Горпинич, С. Л. Карпіловська, Н. Ф. Клименко та ін.) та ідеї пропозитно-диктумної структури висловлювання і синтаксичної номінації з опертям на терміни семантичного синтаксису.

Наголосимо, що когнітивними механізмами метафор у сфері інформаційної безпеки є, на нашу думку, оцінка та розуміння процесу й результату метафоризації разом із семантико-мотиваційними особливостями знаків термінологічної номінації у сфері цивільної безпеки, відтворення структурно-семантичного характеру назв реалій, дій та загалом предметної сфери інформаційного захисту, наприклад, архітектури інформаційного простору та національної безпеки, системного адміністрування, захисту інформації, номенів, пов'язаних із розвідницькою діяльністю та шпигунством, спеціалізовані терміни та поняття цифрової безпеки, які вживаються у комп'ютерних науках, телекомунікаціях і т. ін. (реєстр таких фахових термінів детально прописано в «Англо-українському глосарії термінів ІТ-технологій та кібербезпеки» (АУГІТ).

Термінологізація, на думку дослідників, відбувається на основі метафоричних процесів, що ґрунтуються на переосмисленні назв за подібністю форми, розміру, розташування частин, на зовнішній та функціональній подібності (Булик-Верхола та ін. 2016: 68).

Відповідно до зазначених теоретичних засад продемонструємо ці міркування на прикладі ІТ-термінів у зіставлюваних мовах. Здебільшого це одиниці, які виникли шляхом розвитку багатозначних слів і формування міжгалузевих лексико-семантичних варіантів (ЛСВ). Для наочності основні концептуальні домени, що слугують джерелом метафоризації, та відповідні термінологічні приклади в трьох мовах систематизовано в Таблиці 1.

Таблиця 1

Концептуальні домени та приклади метафоричної номінації в терміносистемах інформаційної безпеки

Сфера-донор (source domain)	Концептуальна метафора (модель)	Приклади (Eng/Pl/UA)
Медицина	КОМП'ЮТЕРНИЙ ВІРУС – ЦЕ ХВОРОБА/ ОРГАНІЗМ	*Infection, vaccine, malware (En); Bakteria, infekcja, kwarantanna (Pl); Вірус, інфекція, карантин (UA)*
Військова справа	КІБЕРПРОСТІР – ЦЕ ПОЛЕ БОЮ	*Attack, shell, silver bullet, defense (En); Blokada usług, atak (Pl); Атака, захист, плацдарм (UA)*
Архітектура та дім	ІНФОРМАЦІЙНИЙ ПРОСТІР – ЦЕ СПОРУДА	*Firewall, gateway, back door, architecture (En); Brama, architektura (Pl); Архітектура, шлюз, чорний хід (UA)*
Родинні стосунки	ТЕРМІНОСИСТЕМА – ЦЕ РОДИНА	*Parent-child relationship, master-slave (En); Matka, potomek (Pl); Дочірнє підприємство / вузол (UA)*
Антропоморфізм (життя/смерть)	ПРОГРАМА – ЦЕ ЖИВА ІСТОТА	*Life-cycle, kill a process, dead link (En); Zabijanie procesu (Pl); Життєвий цикл, «вбити» процес (UA)*
Сенсорика та Смакові відчуття	ТЕРМІН – ЦЕ СУБСТАНЦІЯ/ ОБ'ЄКТ	*Cookies, honey pot, sweet spot (En); Ciastka (Pl); Печиво, медова пастка (UA)*
Колірна символіка	КОЛІР – ЦЕ СТАТУС/ТИП ОБ'ЄКТА	Black hole, white hat, blue-teaming (En); Czarna dziura (Pl); Чорна діра, «білі» хакери (UA)

Як свідчать дані таблиці, термінологізація у досліджуваних мовах часто спирається на медичну та військову сфери-домени. Зокрема, у польській мові фіксуються такі одиниці, як *bakteria, blokada usług, infekcja, kwarantanna* і под. Подібна тенденція зумовлена когнітивною подібністю між біологічними загрозами та цифровими деструктивними процесами. Відтак, як в українських дискурсивних практиках з ІТ-сфери, так і в їхніх польських відповідниках простежуються ідентичні семантичні механізми функціонування вторинних метафоричних номінацій, співвіднесених

із прототипом інфікування, зараження шкідливими програмами (англ. *malware*) на кшталт *хробак* (*Internet Relay Chat* (IRC) *Worm*) – це програма, яка поширюється через форуми повідомлень або чати, надсилаючи заражені файли або вебсайти через канали IRC (АУГІТ 2025: 151). В польській мові їм відповідає кілька оціночних спеціальних позначень *program złośliwy* – niepożądany program, który działa destrukcyjnie na system komputerowy. W skład złośliwego oprogramowania zalicza się: → *wirusy*, → *bakterie*, → *robaki*, → *furtki*, → *bomby logiczne*, → *konie trojańskie* (STBN: 108). **(Дослівно:** небажана програма, яка має руйнівний вплив на комп'ютерну систему. Шкідливе програмне забезпечення включає: *wirusy*, → *bakterie*, → *robaki*, → *furtki*, → *bomby logiczne*, → *konie trojańskie* (STBN: 108). На позначення осіб, які займаються такою шкідливою діяльністю, засвідчено деструктивний термін *włamywacz* (ang. *cracker*) – osoba, ktyra pokonuje zabezpieczenia systemu komputerowego i nielegalnie uzyskuje do niego dostęp. Celem niektyrych *włamywaczy* jest nielegalne uzyskanie informacji z systemu komputerowego lub skorzystanie z zasobów komputerowych. Jednak dla większości *włamywaczy* celem podstawowym jest wyłącznie *włamanie* się do systemu aby sprawdzić swoje umiejętności (STBN: 158) (**Дослівно:** особа, яка ламає безпеку комп'ютерної системи та незаконно отримує до неї доступ. Метою деяких хакерів є незаконне отримання інформації з комп'ютерної системи або використання комп'ютерних ресурсів. Однак для більшості хакерів основною метою є просто зламати систему, щоби перевірити свої навички).

У спеціальних українських лексикографічних джерелах також засвідчено ряд образно-метафоричних номенів, які представляють різні типи шкідливих програм через приписувану ключовому терміну ознаку, наприклад, *вірус вульгарний/, вірус-супутник/вірус-невидимка, вірус-привид (мутант)* тощо. Так, наприклад, під *паразитичним* розуміється комп'ютерний вірус, який при розповсюдженні своїх копій обов'язково змінює вміст програм, файлів або дискових секторів. *Вірус-привид* (*мутант*) здатен до самокодування. Останній містить алгоритми шифрування-розшифрування,

які виключають можливість повторення однакових ланцюжків байт вірусного коду; *вірус-невидимка* використовує спеціальні алгоритми, які маскують його присутність на диску (у деяких випадках і в оперативній пам'яті) (Чистоклетов, Хитра 2023: 38-40).

Отже, запропонована нами рефлексія метафоричних термінів у кількох мовах передбачає звернення до такого **методологічного інструментарію**. По-перше, необхідно виявити онтологічні і прагматичні механізми семантичного термінотворення зазначених термінів, визначити сфери їх концептуальної інтеграції, що передбачає інтепретацію одних понятєвих сфер через інші за допомогою інструментарію концептуального аналізу.

Останнім часом він постулюється в теорії концептуального блендінгу, до якої ми звертаємося в ході аналізу внутрішньої форми термінологічних одиниць, типів їх мотивованості. Зазначена теорія, свого часу опрацьована М. Тернером та Ж. Фоконьє («Блендінг та концептуальна інтеграція»), розглядається як різновид відображень чи проекцій між вихідними ментальними просторами, які переносяться на новий змішаний простір, так званий бленд, елементи якого об'єднуються і починають взаємодіяти (Fauconnier, Turner 2002). На думку дослідників, новизна теорії концептуальної інтеграції є дуже важливою для аргументації процесу і результату творення синестезійних метафор. Згідно з ідеями теорії блендінгу метафоризація не вичерпується проєкцією зі сфери-джерела у сферу-мішень, а включає формування змішаних ментальних просторів, що генерують смисли безпосередньо в самому процесі концептуальної інтеграції.

По-друге, залучення ключових понять когнітивної ономасіології і когнітивного термінознавства, зокрема і фреймового аналізу термінів англомовної термінології безпеки життєдіяльності відповідно до новітніх розробок у галузі когнітивного термінознавства. Застосування когнітивного підходу до різногалузевої термінології сприяє інтерпретації терміна як похідного від концептуалізації та категоризації світу (див. детальніше: Перхач 2017; Садовникова 2016; Тищенко

2024 та ін.). У цьому плані можуть прислужитися і спостереження К. С. Лектоварова над поняттєвим, образно-оцінним складниками когнітивного поля SECURITI з огляду на ядерну, медіальну і периферійну зони в сучасній англійській мовній картині світу, її ціннісним та нормативним складниками.

В авторитетних термінологічних опрацюваннях простежується стійка тенденція до з'ясування змісту, обсягу і співвідношення між такими поняттями, як словотворчий акт, мотивація, внутрішня форма і вмотивованість термінів (Д'яков та ін. 2000: 84-85).

Поза усіляким сумнівом, розглядані терміни варто розглядати крізь призму трьох типів мотивованості: морфологічний, за якого слово мотивується його складовими морфемами (структурні та словотвірні моделі термінотворення); фонетичний, за якого слово мотивується звуконаслідуванням (ономатопеїчні термінологічні формації) та семантичний, за якого переносне значення мотивується прямим значенням, що й передбачає аналіз термінологічних метафор, асоціативно-метонімічних перенесень та епонімів.

Результати дослідження. На англомовному фактажі розглянемо просторові, вітальні і онтологічні метафори, пов'язані з образом смерті. Також зауважимо, що анатомічно-соматичні реалізації переносного значення у зазначеній термінологічній сфері виявляються спорадично. Пор. *Hand coding* – ручне кодування, *руки організації* – це її ресурси, право приймати рішення та технічні можливості. Метафора підкреслює безпорадність та відсутність вибору перед обставинами (наприклад, застарілої інфраструктури чи ліцензійних обмежень (Пальчевська та ін. 2025). Ще рідше простежується соціоморфний, за термінологією деяких дослідників, суто технічний концепт *guest*. Наприклад, "They also help VMM developers design a more simplified VMM. Since hardware-assisted processors can now handle the compute-intensive calculations needed to manage the tasks of handing off platform control to a *guest OS*, the computational burden is reduced on the VMM".

Тут також простежуємо соціоморфні метафоричні моделі, наприклад, **процесор-обладнання-гість**: Since hardware-assisted

processors can now handle the compute-intensive calculations needed to manage the tasks of handing off platform control to a guest OS) (Hoopes 2009: 21). До цієї підгрупи можна ще віднести і таку розгорнуту сполуку *being adopted by the linux community*, в якому лексема *adoption* (усиновлення, прийняття в сім'ю), їх також можна віднести до соціоморфної моделі, оскільки вони спираються на структуру людських взаємин. У контексті ІТ цей образ переноситься на технологію: *Linux-спільнота* не просто «починає використовувати» програму, а «приймає її у свою родину», забезпечуючи підтримку, розвиток та визнання.

Чимало просторових метафор виникають за моделю ПЕРЕШКОДА-ВНУІШНІЙ ПРОСТІР ДОМУ-СПОРУДА-АРХІТЕКТУРА.

Так, лексема *groundbreaking* (***groundbreaking ideas***) походить від терміна, що описує початковий етап будівництва – закладання фундаменту або розкопування ґрунту для нової споруди. Джерелом образу є сфера будівництва та створення людиною нових об'єктів (артефактів). Фізична дія розбивання твердої поверхні землі переноситься на інтелектуальну сферу: ідея «пробиває» шар застарілих знань, щоби закласти основу (фундамент) для майбутньої структури.

До міжгалузевих метафор віднесемо і концепт ***clean*** у його зв'язку з процесами зараження вірусами, що є для сфери ІТ універсальним: «A virtUAl machine or some other mechanism is used so that the system can be brought back into a clean and uninfected initial state after an analysis run. Consequently, the protection of the underlying system is not so important. This form of analysis is called behavior analysis» (Hoopes 2009: 64). До цього концепта ми ще звернемося в ході аналізу номена *dirty botnet* та под.

До просторових метафор віднесемо циклічну метафору руху по колу: *protection rings,* назва семантично мотивована образом концентричних кіл, де кожне внутрішнє кільце є більш захищеним і має більше прав, ніж зовнішнє. Це нагадує структуру середньовічної фортеці з кількома рядами стін. В ІТ-сфері ця ідея стосується привілеїв процесора, «чим ближче до «центру» (Ring 0), тим більше влади

має програмний код, але тим важче туди потрапити». При цьому вирізняється ще *Ring*-1, -2, -3. Цей термін в аналізованому посібнику вжито близько 60 разів (наприклад, у розділі «The Virtual Machine Monitor and Ring-0 Presentation») (Hoopes 2009: 22); пор. також субгалузі «Virtualization Work» та «The Challenge: VMMs for the x86 Architecture», де зазначена номена виявляється найбільш продуктивною.

Водночас метафора прямого руху (техніко-побутова, за А. Худолієм) представлена таким номеном *streamed to systems on-demand*, де *streamed* (*потоковий*) первинно походить від природного образу водного об'єкта, але в сучасному ІТ-дискурсі вона вже стала частиною технічного «арсеналу». У цьому разі йдеться про передачу даних не цілим блоком, а безперервними частинами при перенесенні на програмне забезпечення або операційні системи; «VirtUAl software applications can even be streamed to systems on-demand without invoking a setup or installation procedure» (Hoopes 2009: 31). У розділі «An Introduction to VirtUAlization» (Chapter 1) автор зазначає: «Some application virtUAlization solutions such as VMware's Thin App offer the ability to stream the application to a user's desktop from a file server» (Hoopes 2009: 54). Пор. ще термін із підрозділу «Application VirtUAlization»: *malicious thread* (шкідливий потік) – потік виконання, який запускає шкідлива програма.

Найбільш продуктивними в аналізованій термінологічній концептосфері виявляються предметно-артефактні метафори. Розглянемо деякі з них.

До предметно-артефактних метафор у сфері діяльності агентури та інформаційної архітектури можна віднести ще такі термінологічні номени з додатковим прирощенням, зокрема, оціночно-аксіологійним компонентом семантики *Hook function* (Функція-перехоплювач) – користувацька функція, на яку перенаправляється виконання перехопленої API-функції, *a hooking technique* «that overwrites the initial instructions of a function»; за типологією семантичного синтаксису, це безсумнівний **дестинатив.** Зауважимо, що під дестинативом розуміється термін семантичного синтаксису та логічної семантики, що є мисленнєвим аналогом

призначення предмета, один із аргументів у структурі пропозиції або предикатно-аргументній структурі (Селіванова 2011: 118).

Щодо інших термінів із предметним метафоричним значенням, то з-поміж інших звернемо увагу на такі: *False positive* (Хибнопозитивне спрацювання) – хибне виявлення шкідливої поведінки, якої не було, *False negative* (Хибнонегативне спрацювання) – пропущена шкідлива активність, *Packet capture* (Захоплення пакетів) – перехоплення мережевих пакетів для подальшого аналізу, *Registry hive* (*Кущ реєстру*) – великий структурований файл реєстру Windows; *pocket litter* – кишенькове сміття «звичайні речі, що знаходяться в кишені: монети, квітки, ключі та ін.; ці речі можуть підтвердити легенду агента, якщо його спіймають» (СКПСБ 2014: 247), *brush contact/brush pass* – щітковий контакт, моментальна зустріч, «коротка зустріч між агентом та його керівником для передачі документів, грошей тощо» (СКПСБ 2014: 37). Обидва номени корелюють із ідеєю щітки і мітли у їхньому синтагматичному зв'язку із концептом бруду, очищенням. Варто згадати і такий образний контекст («If you are planning on rolling out a new wave of PCs for hundreds of call center agents or in a manufacturing environment (just think of how *dirty those shiny new*, underutilized PCs will get in just a few days on the shop floor»)), співвіднесений із поняттями чистого-брудного. Цікавим є ще і такий образний вислів *claiming to wear the virtUAlization hat,* що сягає ідіоми *to wear a hat.* В англомовній культурі означає «виконувати певну роль» або «мати певні обов'язки». У сфері IT цей образ переноситься на програмний продукт: компанія чи технологія «одягає капелюх віртуалізації», тобто заявляє про свою здатність виконувати функції платформи віртуалізації.

Наступна метафора *bunny suit* містить асоціативне порівняння спеціального захисного одягу із зовнішнім виглядом кролика. Термінологічне словосполучення також виникає на підставі концептуального блендінгу, зокрема зовнішньої подібності об'єктів, спроектованих на тварину і тип одягу; суцільний білий комбінезон із капюшоном, бахілами та рукавичками робить людину схожою на пухнасту

білу тварину. Слід також відзначити ассоціативно-символічний зв'язок із чистотою/крихкістю/м'якістю. У цій ситуації кролики асоціюються з чимось м'яким і стерильним, що підкреслює призначення костюма для «чистих кімнат» (*cleanrooms*), роботи в лабораторіях (АУГІТ 2025: 14).

З усією очевидністю локативна модель номінації (*вікно* як переосмислений символічний локус споруди, дому, внутрішнього простору) при позначенні окремих реалій у сфері розвідки наповнюється і таким терміном *window dressing* – легендована інформація «у розвідувальному жаргоні – додаткові матеріали, включені в «легенду» або операцію з дезінформування для того, щоб допомогти переконати супротивника чи стороннього спостерігача в достовірності того, що вони спостерігають» (СКПСБ 2014: 336).

Показовим виявляється і такий термін із предметним значенням, що сягає процедури медичного обстеження у розвідці: *barium meal* – «перевірка агента, якого підозрюють у зраді та якому надають заздалегідь неправдиву інформацію, а далі простежують, чи не потрапила вона до супротивника». Назва походить від медичної процедури, яка дозволяє лікарям простежити проходження слабо реактивного матеріалу в тілі людини. Як бачимо, концепт зради як аксіологійний додатковий конотат у цьому разі відіграє ключову роль.

Як зазначалося, донорською сферою мотивації окремих термінів може бути **медицина** (пор. *Levels of Malware Analysis Paranoia*), де вторинна концептуалізація термінів на позначення небезпек і ризиків може відбуватися через поняття смерті у його поєднанні **з ознакою кольору:** «a Blue Screen of Death or similar dangerous scenarios» (із розділу «Configuring the Virtual Machine») (Hoopes 2009: 101).

Зазначений термін представлений і в контексті, що мотивує необхідність захисту в ненадійних середовищах: «But useful scenarios abound. For example, installing a VMware codec to record videos of virtual machines is not a big deal, but when it **BSODs (Blue Screen of Death)** my Vista machine, it is very much an inconvenience» (із розділу «Protection in Untrusted Environments») (Hoopes 2009: 303) (Дослівно: «Але корисних сценаріїв предостатньо. Наприклад, встановлення кодека

VMware для запису відео віртуальних машин не є великою проблемою, але коли на моєму комп'ютері з Vista виникає BSOD (синій екран смерті, це створює великі незручності»).

Автор зауважує: «This seems like a silly recommendation, but given the level of incompatibility issues and serious consequences (hosed users and Blue Screens of Death), it is not surprising that major PC resellers like HP and Dell are offering XP downgrade paths...» (Hoopes 2009: 305).

Через образ смерті концептуалізується ще одна кіберномінація антропоморфного типу *hug of Death* («Обійми смерті»). Зрозуміло, що термін *обійми* стосується людських міжособистісних взаємин. У спеціальних лексикографічних розробках знаходимо такий коментар: «фраза «обійми смерті» описує ситуацію, коли розміщення матеріалу на певному сайті призводить до експоненційного зростання трафіку, внаслідок чого контент стає недоступним, зазвичай, унаслідок вірусного поширення» (АУГІТ 2026: 139).

Колоративні номени. В терміносистемі кібербезпеки також засвідчено колоративний номен, який в англійській мові утворений шляхом словоскладання, а український він покривається субстантивним словосполученням: *blue-box* – *синя коробка* – це електронний пристрій, який використовувався у 1960–1970-х роках для імітації тонів телефонного комутатора, зазвичай у діапазоні 2600 Гц, із метою керування комутацією міжміських дзвінків. Дозволяв користувачам переходити в режим оператора і безкоштовно перенаправляти дзвінки. Через можливість обходити оплату та складність відстеження дзвінків активно використовувався з незаконною метою (АУГІТ 2026: 123).

На семантичних протиставленнях морально-етичної концептуалізації дійсності (легітимізованої і нелегітимізованої, явної і прихованої, гласної і негласної) інформаційної діяльності спецслужб ґрунтуються і такі асоціативно-символічні термінологічні номени, як *black bag job* «негласний обшук; таємне проникнення в закрите приміщення з метою вилучення важливих документів, пошуку доказів тощо», *black list* – «чорний список; офіційний список осіб, які співпрацюють з ворогом, співчувають йому

або підозрюються в цьому, а також осіб, чия присутність загрожує безпеці дружніх сил» (СКПСБ 2014: 34), *black operations* «темні операції, (high-risk covert operations, usually of an unallowable nature, are termed «black operations»). The most common circumstances in which such operations are mounted concern the burglary of diplomatic premises» – нелегальні таємні операції, наприклад, проникнення зі зломом (часто в приміщення посольств)» (СКПСБ 2014: 35), *white list* – «особисті дані та інформація про місця розташування осіб, які можуть становити інтерес для розвідувальних чи контррозвідувальних органів та надавати їм інформацію чи допомогу у вже існуючих або нових сферах зацікавленості розвідки» (СКПСБ 2014: 336).

Семантика сірого кольору також пов'язується з негативно маркованими десигнатами у сфері збереження інформації, розвідувальної діяльності, наявними загрозами, які представлені як однослівними композитами на кшталт *graymail* – «загроза розкриття державної таємниці підзахисним у разі його переслідування у судовому порядку» (СКПСБ 2014: 142), так і аналітичними словосполуками *gray list* – «список осіб, чиї політичні погляди та мотиви невідомі, або які мають інформацію, що може бути корисною для США» (СКПСБ 2014: 142).

До речі, в польській фраземіці семантика сірого кольору мотивує незаконні дії в економічній сфері, пор. *szara strefa* – *тіньова економіка*, пор. ще *szara eminencja* – «йдеться про не дуже значну на перший погляд особу, яка завдяки різним прихованим вчинкам, діям, інтригам і маніпуляціям негативно впливає на прийняття рішень в сфері діяльності державних чи суспільних інституцій» (Bąba, Liberek 2002: 804).

Семантика чорного кольору у двомовних військових словниках представлена як міжгалузевими технічними термінами типу *black box* – *чорний ящик* (система, яку можна розглядати з погляду її входів і виходів, не маючи знань про її внутрішню роботу), так і спеціальними з донорською сферою ТВАРИНИ, КОМАХИ на позначення видів БПЛА: *Black Hornet* – *Чорний Шершень* (безпілотний розвідувальний мікролітальний апарат, поміщається у долоню – за планом

на озброєнні ЗСУ з 2022 р.) (Англо-український військовий словник 2026).

Аналогічні польські терміни також демонструють багатозначність метафоричного переосмислення, зокрема **czarna skrzynka** (англ. *black box*), що трактується як: «*1. Układ względnie odosobniony, którego budowa i zasady działania nie są znane... 2. Przenośnie urządzenie techniczne używane bez znajomości zasad jego funkcjonowania. 3. Urządzenie rejestrujące pozwalające odtworzyć przebieg wydarzeń*» (1. Відносно ізольована система, будова та принципи дії якої невідомі; 2. Переносно – технічний пристрій, що використовується без розуміння принципів його функціонування; 3. Реєструвальний пристрій для аналізу аварійних ситуацій) (STBN 2008: 29).

Важливою для когнітивного аналізу є примітка джерела про те, що «*wbrew nazwie czarna skrzynka nie jest wcale czarna*» (попри назву, чорна скринька зовсім не є чорною), оскільки її корпус фарбують у яскраво-помаранчевий колір для полегшення пошуку; це вказує на те, що в терміносистемах безпеки метафора **BLACK** маркує не фізичну ознаку, а гносеологічну «закритість» та інформаційну непрозорість об'єкта.

В спеціальних словниках безпеки польської мови виявлено **3 групи хакерів**, мотивованих ознакою кольору на аксіологійному полюсі добра і зла (йдеться здебільшого про метонімічне перенесення за моделлю предмет одягу → група людей, які займаються певною діяльністю). Вирізняються такі підгрупи хакерів за вартісно-оцінною шкалою: ***czarne kapelusze*** (ang. *black hat*) – są to hakerzy działający na granicy lub poza granicami prawa, nazywani też crackerami. Znalezionych błędów albo nie publikują w ogóle, wykorzystując je w nielegalny sposób, albo publikują od razu w postaci gotowych programów (tzw. exploitów) (np. script kiddies) (**Дослівно:** це хакери, які діють у межах закону або поза ним, також відомі як крекери. Вони або не публікують знайдені помилки, використовуючи їх незаконно, або одразу публікують їх як готові програми (відомі як експлойти); ***białe kapelusze*** (ang. *white hat*) – «hakerzy działający zupełnie legalnie lub też starający się nie robić szkód. Odkryte przez siebie dziury w bezpieczeństwie zwykle podają w formie, w której mogą zostać łatwo załatane przez autorów oprogramowania, lecz trudne do wykorzystania w celu zaszkodzenia komuś» (**Дослівно:**

«хакери, які діють легально або намагаються уникнути заподіяння шкоди, зазвичай представляють виявлені ними діри в безпеці у формі, яку автори програмного забезпечення можуть легко виправити, але їх важко використати для завдання шкоди комусь»); ***szare kapelusze*** (ang. *grey hat*) – «hakerzy, którzy przyjmują po części metody działania obu wyżej wymienionych grup. Kapelusze pochodzą ze starych czarno-białych westernów, gdzie na podstawie koloru kapelusza odróżniano tych dobrych od tych złych» (**Дослівно:** «хакери, які переймають деякі методи обох вищезазначених груп. Капелюхи походять зі старих чорно-білих вестернів, де колір капелюха відрізняв хороших хлопців від поганих») (STBN 2008: 49).

До міжгалузевих метафор можна віднести і **температурну ознаку номінації**, об'єктивовану у внутрішній формі словосполучення *hot site,* яке первинно описує стан високої енергії або температури. В ІТ-сфері цей образ переноситься на ступінь готовності інфраструктури, оскільки «гаряча» дільниця має актуальні дані, підключене обладнання та персонал. Вона буквально «палає» від активності, на відміну від «холодної» (*cold site*), яку потрібно спочатку «розігріти» (встановити програмне забезпечення, завантажити бекапи). Отже, у цьому разі простежуємо антонімію термінів.

Із такою ж внутрішньою формою зафіксовано ще кілька назв, утворених шляхом семантичного термінотворення. Це, зокрема, однослівна назва на позначення опредметненої дії в англомовному кіберпросторі *hotlinking* (український відповідник становить словосполучення A+N: *гарячі посилання*) та словосполука, що також постає за моделлю A+N: *hot add* – *гаряче додавання*. Щодо першої назви, то йдеться про такий тип кіберінтеракції, при якому вебсайт використовує посилання на інший вебсайт для завантаження зображень або інших файлів, замість збереження копії цих файлів і локального розміщення. Він фактично передає навантаження на інший сервер.

Деякі типи гарячих посилань стали більш поширеними через удосконалення інструментів соціальних платформ. Це посилання на образ з першоджерела, полегшене розвитком інтернет-технологій (АУГІТ 2026: 137).

Зі свого боку друга назва пов'язується з модусом динамічного додавання віртуального або фізичного обладнання до працюючої системи без її зупинки. Це дозволяє системним адміністраторам повторно розподіляти ресурси та послуги без відключення систем (АУГІТ 2026: 138).

Температурна ознака може поєднуватися з топономастичним кодом; такі відепонімні утворення у сфері кібезбезпеки, зазвичай, трапляються зрідка на відміну від медичної, автомобільної чи загалом науково-технічної, наприклад, *Kyoto cooling* – *Кіотське охолодження* – це енергоефективна альтернатива традиційним системам охолодження для центрів обробки даних та ІТ-інфраструктури. Воно використовує обертове теплове колесо (*кіотське колесо*) для перенесення тепла з теплого зворотного повітря до холоднішого зовнішнього, що значно знижує потребу в механічному охолодженні (АУГІТ 2026: 145).

Ще одна предметна метафора постала шляхом поєднання предметно-субстанційної (пісок – матеріальна субстанція) і просторово-локативної мотиваційних сфер – *sandbox* (пісочниця), що в спеціальній літературі трактується як контрольоване середовище для безпечного запуску непереві́реного програмного ПЗ (Hoopes 2009: 67). На прикладі архітектури інструменту *CWSandbox* (зокрема, взаємодії компонентів *cwsandbox.exe* та *cwmonitor.dll*) простежується реалізація метафори «контрольованої ізоляції»: «пісочниця» повністю перебирає на себе виконання шкідливого коду (*it is the sandbox that actually executes the malware*), імітуючи для нього роботу реальної системи. Важливим когнітивним аспектом є модель «введення в оману» (*tricking*), коли ПЗ «думає» (*thinks*), що взаємодіє з мережею чи сервером, хоча насправді всі його дії локалізовані всередині ізольованого простору, що дозволяє безпечно вивчати поведінку вірусу та зберігати копії створених ним файлів (*STORE_CREATED_FILES*) для подальшого аналізу (Hoopes 2009: 68).

Щодо донорського домена **МЕТАЛИ,** то в цьому разі вигідно вирізняється термін з етнокультурною і символічною мотивацією: *the silver bullet – срібна куля*. Терміноназву можна пов'язати з народними повір'ями про те, що *лише*

куля зі срібла може миттєво вбити перевертня або іншу надприродну істоту. Саме це уявлення переноситься на сферу розробки ПЗ та ІТ-інфраструктури, де у ролі *перевертня* виступає сам надзвичайно складний проект, а *срібна куля* – це код нових технологій чи методологій для швидкого й легкого вирішення наявних проблем (Brooks 1987: 10).

Прикладом практичної реалізації цієї метафори є такий контекст: «After realizing you had the answer all along, it will make your IT manager's day to learn this technology is the *silver bullet* that will satisfy the needs of the business while providing superior value in IT operations and infrastructure management and delivery» (Hoopes 2009: 15). (Дослівно: «Зрозумівши, що ви завжди мали відповідь, ваш ІТ-менеджер із задоволенням дізнається, що ця технологія – це *панацея*, яка задовольнить потреби бізнесу, забезпечуючи при цьому чудову цінність в управлінні ІТ-операціями, інфраструктурою та її наданні»). У цьому контексті ми спираємося на трактування М. І. Балли, за яким *silver bullet* відповідає значенню «панацея» – засіб, що дає швидкий і ефективний результат у складній ситуації (Балла 1996, 2: 412). Таке переосмислення підкреслює сподівання на технологію як на «магічний» інструмент, здатний миттєво усунути інфраструктурні обмеження.

Зауважимо, що при перекладі цього терміна українською мовою відбувається лексико-семантична трансформація із заміною образу у цільовому тексті (*панацея*). Така заміна зумовлена відсутністю в українській мові прямого фразеологічного еквівалента, який би одночасно поєднував міфологічне підґрунтя та значення «універсального вирішення складної технічної проблеми».

У словнику *Multitran* ***silver bullet*** «срібна куля» фіксується як військова метафора зі значенням «просте вирішення складної проблеми», *silver bullets* «гроші, що стягуються як воєнна позика», такі ж самі значення представлені в двомовних словниках військових термінів (Англо-український військовий словник 2026). Принагідно підкреслимо, що відносно-якісні прикметники (*silver*) можуть бути співвіднесені зі вторинною семантикою і звуженням термінологічної

одиниці на локальний ареал, свідченням чого є ще такий семантичний розвиток прикметника як *silver triangle* – південноамериканський регіон, що включає Перу, Болівію та Колумбію – країни, які історично були основними незаконними виробниками наркотиків (СКПСБ 2014: 286).

Звернемося ще до такого контексту: «While *big-frame*, ***big-iron*** servers continued to survive, the midrange and entry-level server market bustled with *new life* and opportunities for all but the most intense use cases» – «Хоча сервери з великим корпусом та потужним залізом продовжували виживати, ринок серверів середнього та початкового рівня *вирував новим життям* та можливостями для всіх, окрім найінтенсивніших випадків використання». Якщо придивитися уважніше, то у наведеному контексті, крім стертої вітальної метафори, виявляємо ще кілька параметричних ад'єктивних тропів за ознакою розміру (*big*), концептуально спроектованих на метонімію (*big-iron*, модель, субстанція, фактура, матеріал → виріб) (Hoopes 2009: 9).

Наступна метафорична полікомпонентна структура ґрунтується на концептуальному блендінгу, бо в цьому разі один образ накладається на інший: ***t****rap-and-emulate native SCSI commands.* Лексема *trap* (пастка) позначає механізм «захоплення» події» (у цьому разі наявна предметно-термінальна мотивація), а *emulate* (імітувати/наслідувати) походить від латинського *aemulus* 'намагання зрівнятися або точно скопіювати чиюсь поведінку (як актор на сцені)', тобто виражається ідея акціонального сценарію через метафори театральної гри. В ІТ-сфері цей образ трансформується на процес, коли гіпервізор перехоплює команду, яку гостьова ОС надсилає «*залізу*», і створює ілюзію її виконання. Тобто, метафора маркує контрольовану імітацію та непомітність процесу для гостьової системи. Зазначені метафоричні словосполучення можна розглядати як артефактно-інструментальні, бо *trap* тут відіграє роль віртуального знаряддя і/або віртуальної пастки.

Ось кілька типових вживань зазначеного терміна: «If an application is *booby-trapped* you will be able to examine and analyze (without suffering) the effects of the trap, then refresh

the image» (Hoopes 2009: 243) (Переклад: «Якщо застосунок містить *міну-пастку*, ви зможете дослідити та проаналізувати (не зазнавши шкоди) наслідки спрацювання цієї пастки, а потім відновити образ системи»). Цей контекст із розділу «Analyzing Time Bombs and Booby Traps» ілюструє використання військової метафори для опису шкідливого ПЗ.

Інший аспект функціонування терміна бачимо у підрозділі «The Popek and Goldberg Requirements»: «Privileged instructions are those that *trap* if the processor is in User Mode and do not trap if it is in Supervisor Mode» (Hoopes 2009: 24) (Переклад: «Привілейовані інструкції – це ті, що спричиняють *переривання (пастку),* якщо процесор перебуває в режимі користувача, і не спричиняють його в режимі супервайзера»). Неозброєним оком видно, що в цьому сегменті віртуальних рекомендацій додаткову функцію відіграють епоніми *Попек* та *Голдберг*; «Provides near-native CPU and memory performance; uses sophisticated techniques *to trap and emulate instructions* in runtime via binary patching» – «Забезпечує майже власну продуктивність процесора та пам'яті; використовує складні методи *для захоплення та емуляції* інструкцій під час виконання за допомогою бінарних патчів» (Hoopes 2009: 28); «Software products exist that *trap-and-emulate native SCSI commands* and translate them to other storage instructions in the background, making it possible for a disk array to look like a suite of tape drives and tape libraries to back up software and operating systems without any modification» («Існують програмні продукти, які *перехоплюють та емулюють рідні команди* SCSI та перетворюють їх на інші інструкції зберігання у фоновому режимі, що дозволяє дисковому масиву виглядати як набір стрічкових накопичувачів та стрічкових бібліотек для резервного копіювання програмного забезпечення та операційних систем без будь-яких модифікацій») (Hoopes 2009: 30). Даний контекст із розділу «An Introduction to VirtUAlization» ілюструє випадок, коли *trap if the processor is in user mode* (пастка, якщо процесор знаходиться в режимі користувача).

З наведеного переконуємося, що *trap* (пастка) у первинному значенні описує пристрій, призначений для раптового

захоплення об'єкта, який порушив певну межу або зробив невірний крок. В IT-дискурсі цей образ переноситься на виняткову ситуацію або переривання у випадку, коли програма в Ring 3 намагається виконати привілейовану команду (наприклад, звернутися прямо до диска), а процесор намагається її піймати «на гарячому».

З огляду на сказане не можна обійти увагою ще і такий метафоричний термін, як **honey trap**, пор. «*The term universally applied to operations undertaken to ensnare an unwary target in a compromising sexUAl encounter that may leave the victim vulnerable to blackmail that might result in espionage*» – медова пастка (використання інтимних відносин для компромату та шантажу жертви з метою змусити її зайнятись шпигунською діяльністю) (СКПСБ 2014: 147).

Розглянемо детальніше словотвірні моделі і сполучуваність термінів із компонентом *honey*. **Honeypot, або *горщик з медом*** – «комп'ютерна пастка, встановлена з метою попередити та протистояти спробам несанкціонованого доступу до інформаційних систем; зазвичай це контрольований сайт, який містить інформацію, яка може бути привабливою для зломщиків» (СКПСБ 2014: 147).

Як зазаначається у фаховій літературі, вирізняються кілька типів *Honeypotting*. Останні мають свої переваги, недоліки та складності; однак вибір між різними класифікаціями *honeypots* найчастіше ґрунтується на ризику проти потенційної вигоди. *Honeypots* із високою взаємодією можуть становити найбільшу загрозу безпеці, оскільки у разі їх компрометації зловмисник отримує повний контроль над усією операційною системою (Hoopes 2009: 120).

Зазначену термінологічну групу можна розглянути і за словотвірною, і за дистрибутивною структурою: A+N (local honeypot, virtUAl honeynet) N+N (honeypot placement, honeypot architecture), яка представлена кількома структурно-семантичними варіантами, утвореними за спільним зразком: *honeynet, honeymole, honeywall* і под. У спеціальній літературі наголошується, що *Honeywall* – це компонент, який контролює та моніторить увесь вхідний і вихідний трафік *honeynet*. Він дозволяє зловмисникам взаємодіяти з *honeypots*,

водночас запобігаючи атакам на інші системи. Ймовірно, звідси й метафора стіни як перешкоди або бар'єру (Hoopes 2009: 124), Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting) "A *honeywall* is used to control and monitor all inbound and outbound traffic to and from a honeynet. It allows attackers to interact with honeypots while preventing them from attacking other systems".

Щодо компонентного складу, то цей термін представлений різними варіантами двокомпонентних (рідше – трикомпонентних) утворень із ключовим композитним терміном, що виник у результаті концептуального блендінгу (синестезії смакової і просторово-локативної сфери, умістища, або в термінах когнітивної лінгвістики *контейнера*). Наприклад, цей складний термін може поєднуватися з абстрактними і віддієслівними іменниками: *honeypot network*, *honeypot detection* – із суфіксальними формантами **-tion** (honeypot *deception***)** або **-ment** (honeypot *deployment,* honeypot *deployment strategy*).

Детальніший аналіз дав змогу виявити такі продуктивні афікси в розгляданій ТГ термінів: суфікс **-ing-**, представлений у терміні *honeypot alerting* («Honeypot alerting mechanisms notify administrators when suspicious or malicious activity is detected within a honeypot environment. These alerts allow for rapid response and further investigation of potential threats» – *Honeypot alerting* – це механізми сповіщення, які інформують адміністраторів про підозрілу або шкідливу активність у *honeypot*-середовищі; такі сповіщення забезпечують швидке реагування та подальше дослідження потенційних загроз); суфікс **-ment-** у терміні *honeypot containment* («Honeypot containment ensures that compromised honeypots cannot be used to launch attacks against external systems. Containment mechanisms are a critical part of secure honeypot design" – *Honeypot containment* – це механізми ізоляції, які гарантують, що скомпрометований *honeypot* не може бути використаний для атак на зовнішні системи; ізоляція є ключовим елементом безпечного проєктування *honeypot*) (Hoopes 2009: 118); афікс **-tion-**, що виявляється у назвах *honeypot isolation* («Honeypot isolation ensures that a compromised

honeypot remains separated from production systems. Isolation techniques are essential to prevent attackers from pivoting into trusted networks» – *Honeypot isolation* – це ізоляція *honeypot*) та *honeypot collection* (Збір з медової пастки – збір зразків шкідливого ПЗ через пастки) (Hoopes 2009: 120); суфікс **-ility-** у терміні *honeypot scalability* («VirtUAlization allows honeypot deployments to be scaled quickly and efficiently. This scalability makes it possible to deploy large numbers of honeypots with minimal hardware requirements» – *Honeypot scalability* – це можливість швидкого та ефективного масштабування *honeypot*; завдяки віртуалізації можна розгортати велику кількість *honeypots* з мінімальними апаратними витратами) (Hoopes 2009: 123), а також знову **-ing-**, що характеризує окремі деривaційно-граматичні моделі з віддієслівним іменником (опредметнена дія або процес), які співвідносяться з герундіальними конструкціями *honeypotting* та *honeypot logging*. Другий семантико-структурний підтип також містить поєднання двох метафоричних складників в однослівній лексикалізованій назві, співвіднесеної з різними метафоричними когнітивними доменами, зокрема з асоціативно-епідигматичною ідеєю меду як чогось солодкого й привабливого та предметно-локативною семантикою «воріт» (*honeynet gateway*), «перешкоди» (*honeywall*) або просторовою ідеєю шляху чи лінії (*honeypot traffic*).

До цієї підгрупи ми відносимо і терміни з параметричною ознакою прикметника або іменника (високий – низький, великий – малий за інтенсивністю, розміром, мірою, проявом і под.): *high-interaction honeypot* або *low-interaction honeypot* (*honeypot* з низьким рівнем взаємодії).

Насамкінець розглянемо сенсорно-слухову концептуалізацію термінологічних номенів. Як відомо, слухові враження, концептуалізовані різними мовами відрізняються культурно та географічно. Так, у сфері інформаційної безпеки засвідчено термінологічну сполуку ***buzz word***, де простежується звуконаслідувальна мотивація терміна. Лексема *buzz* (дзижчання, гул) у прямому значенні описує безперервний вібруючий звук (наприклад, комах або натовпу). Цей сенсорно-слуховий акустичний ефект переноситься на сферу

інформації, адже йдеться про ситуацію, коли певний термін «звучить» звідусіль через масове повторення. У цьому разі метафора актуалізує високу інтенсивність слова, певного наративу у кіберпросторі, часто натякаючи на його нав'язливість, ажіотаж, при можливій відсутності глибокого змісту (створення ефекту шуму»).

Ознака **дестинативу** (спеціального створення шумового ефекту) об'єктивована в терміні в галузі кібербезпеки, в якому простежується синестезія звукової ознаки з ознакою кольору: ***blue noise*** – *синій шум* – це тип шуму з менш різким підвищенням частоти, ніж у фіолетового, і протилежним ефектом до рожевого, де інтенсивність зменшується. Його використовують для рандомізації та проектування шаблонів. Синій шум збільшується в гучності зі збільшенням частоти, але з меншою швидкістю, ніж подібний різновид шуму, який називається фіолетовим шумом. Синій шум також відомий як блакитний (АУГІТ 2026: 125).

Висновки. У результаті проведеного дослідження встановлено, що термінологія сфери інформаційної безпеки є складною динамічною системою, розвиток якої зумовлений як внутрішньомовними когнітивними процесами, так і зовнішніми геополітичними чинниками. Доведено, що в умовах військової агресії та інтенсивної цифровізації суспільства відбувається масштабна метафоризація фахової мови кібербезпеки, що вимагає перегляду традиційних підходів до її категоризації.

Аналіз структурно-семантичних особливостей метафоричних номінацій в англійській, українській та польській мовах дозволив виявити ключові сфери-донори, серед яких домінують медицина, військова справа, архітектура та родинні стосунки.

Встановлено, що метафоризація в цій галузі має опору в онтологічних і прагматичних механізмах, які дозволяють вербалізувати цифрові загрози через знайомі людині концептуальні домени (наприклад, «infekcja», «пастка», «firewall»). Зіставний аспект дослідження продемонстрував спільні риси у формуванні міжгалузевих лексико-семантичних варіантів, що свідчить про універсальний характер

когнітивно-інформаційних засад кібербезпекового дискурсу в германських та слов'янських мовах.

Перспективи подальших наукових розвідок вбачаємо у глибшому аналізі прагматичного потенціалу складних метафоричних термінів у перекладному вимірі. З погляду методологічної перспективи актуальним постає здійснення моделювання та розбудова термінофрейму SAFETY, який лежить в основі концептуальної структури англомовної термінології безпеки та охоронної діяльності як окремих структур знання, співвіднесених із фреймовими структурами *safety*, *hazards* та *risk* (Тищенко 2017). Такий підхід дозволить більш детально простежити динаміку появи нових термінологічних одиниць під впливом розвитку штучного інтелекту та сучасних засобів інформаційно-психологічних операцій.

ЛІТЕРАТУРА

Англо-український військовий словник. 2026. URL: https://english-military-dictionary.org.ua (дата звернення: 20.02.2026).

Балла М. І. Англо-український словник : у 2 т. Київ : Освіта, 1996. Т. 2: L–Z. 712 с.

Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: термінологічний навчальний довідник. Київ : ТОВ «Д.В.К.», 2004. 508 с.

Булик-Верхола Г. В., Наконечна С. З., Теглівець Ю. В. Основи термінознавства : навч. посібник. 3-тє вид., доп. Львів : Вид-во Львівської політехніки, 2016. 192 с.

Д'яков А. С., Кияк Т. Р., Куделько З. Б. Основи термінотворення: семантичні та соціолінгвістичні аспекти. Київ : КМ Academia, 2000. 216 с.

Заплатинський В. М. Логіко-детермінантні підходи до розуміння поняття «Безпека». *Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини*. 2012. Вип. 5. С. 41–49.

Іващенко В. Л. Концептуальна репрезентація спеціальних знань у мові (на матеріалі мистецтвознавчої термінології): монографія. Київ : Вид. дім Дмитра Бураго, 2006. 328 с.

Кришталь С. М. Структурно-семантичний аналіз метафоричних термінів підмови фінансів в англійській і українській мовах: дис. ... канд. філол. наук: 10.02.17. Донецьк, 2003. 210 с.

Кушнерьов О. С. (укл.). Безпека інформації : конспект лекцій. Суми : Сумський державний університет, 2021. 99 с.

Левченко О. Г., Землянська О. В. та ін. Безпека життєдіяльності та цивільний захист : підручник. Київ : Каравела, 2019. 268 с.

Лектоваров К. С. Вербалізований концепт SECURITY в англомовній картині світу : автореф. дис. ... канд. філол. наук: 10.02.04. Одеса, 2017. 20 с.

Міщенко А. Л. Термінологічні засади технологічно-орієнтованого галузевого перекладу (на матеріалі німецької, української і англійської мов): навч.-метод. посібник. Кіровоград : Видавець Лисенко В. Ф., 2014. 156 с.

Мусієнко І. І. (ред.). Словник ключових понять та абревіатур сектору безпеки: англо-українсько-російський. Харків : Оберіг, 2014. 428 с.

Пальчевська О. С., Добровольська С. Р. та ін. Англо-український глосарій термінів ІТ-технологій та кібербезпеки. Львів : Львівський державний університет безпеки життєдіяльності, 2025. 266 с.

Перхач Р.-Ю. Т. Термінологія в інструкціях до медичних препаратів: лінгвокогнітивний та лінгвокультурний аспекти (на матеріалі української, польської, німецької мов): дис. ... канд. філол. наук: 10.02.15. Львів, 2017. 235 с.

Письменський Є. О., Головкін С. В. та ін. Розслідування колабораційної діяльності: практ. посібник. Київ : ВД Дакор, 2023. 260 с.

Садовникова Г. В. Когнітивно-інформаційна природа термінів автомобілебудівництва в англійській, німецькій та українській мовах: дис. ... канд. філол. наук: 10.02.17. Київ, 2016. 261 с.

Селіванова О. О. Лінгвістична енциклопедія. Полтава : Довкілля-К, 2011. 844 с.

Стасюк Т. В. Терміносфера новітніх технологій: лінгвосоціокогнітивні чинники формування та розвитку: дис. ... д-ра філол. наук: 10.02.15. Київ, 2020. 488 с.

Тищенко О. В. Мовна концептуалізація небезпеки та ризику в науковій та наївній моделях світу: до проблеми лінгвістики безпеки. *Studia slawistyczne: etnolingwistyka i komunikacja międzykulturowa*. 2017. Zeszyt IV. S. 69–89.

Тищенко О. В. Особливості перекладу та типологія автотранспортних термінів (на матеріалі української, англійської, німецької, польської та італійської мов). *Львівський філологічний часопис*. 2024. №15. С. 113–121. DOI: https://doi.org/10.32447/2663-340X-2024-15.15

Худолій А. О. Інформаційна війна 2014–2022 рр.: монографія. Острог : Вид-во Національного університету «Острозька академія», 2022. 208 с.

Чистоклетов О. О., Хитра О. Л. Словник з інформації та інформаційної безпеки. Львів : Растр-7, 2023. 250 с.

Brooks F. P. No silver bullet – Essence and accident in software engineering. *Computer*. 1987. Vol. 20 (4). P. 10–19. DOI: https://doi.org/10.1109/MC.1987.1663532

Fauconnier G., Turner M. The Way We Think: Conceptual Blending and The Mind's Hidden Complexities. New York : Basic Books, 2002. 340 p.

Hoopes J. Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting. Burlington : Syngress Publishing, Inc.; Elsevier, 2009. 423 p.

Zdrodowski B. (red.). Słownik terminów z zakresu bezpieczeństwa narodowego. 6-te wyd. Warszawa : Akademia Obrony Narodowej; Wiedza, 2008. 184 s.

STRUCTURAL AND SEMANTIC CATEGORIZATION OF METAPHORICAL TERMS IN THE FIELD OF INFORMATION SECURITY (BASED ON ENGLISH, POLISH, AND UKRAINIAN)

Oleh V. Tyshchenko

Doctor of Philology, Professor,
Professor at the Department of Foreign Languages and Translation Studies
Lviv State University of Life Safety,
Lviv, Ukraine
Professor at the Faculty of Arts
University of St. Cyril and Methodius in Trnava,
Trnava, Slovakia
e-mail: olkotiszczenko@gmail.com
ORCID ID: https://orcid.org/0009-0009-0811-2123
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57834809700

Maryna Kucherenko

PhD Student at the Department of Foreign Languages and Translation Studies,
Lecturer at the Department of Foreign Languages and Translation Studies
Lviv State University of Life Safety,
Lviv, Ukraine
e-mail: stepaniyuk@gmail.com
ORCID ID: https://orcid.org/0000-0002-4803-8089

SUMMARY

The article examines the cognitive and informational foundations of computer security terms, identifies their thematic groups, associated risks, and threats in the modern digital space and discursive practices across distantly related Germanic and Slavic terminological systems.

A structural and semantic analysis of the information protection terminological system has been carried out, specifically covering information space architecture, national and international security (entities denoting reconnaissance and espionage activities, illegal drug trafficking, types of traps, etc.), system administration, and computer threats, considering traditional linguistic and conceptual metaphors of various types, their interaction, interpenetration, and the typology of conceptual spheres.

The study reveals the ontological and pragmatic mechanisms of semantic term formation of metaphorical terms in English, Ukrainian, and Polish, defines the areas of their conceptual

integration, and traces the cognitive and onomasiological foundations of terminological nomination (color, taste, sensory-perceptual, auditory, temperature, etc.). Instances of taxonomy, synonymy, and antonymy of both highly specialized and interdisciplinary metaphorical designations are established.

The analysis demonstrated that the source domains for metaphorical terms include medicine, the military sphere, metals and substances, family relations, architectural metaphors, and the concept spheres of "clean-dirty" and "life-death".

Particular attention is paid to the analysis of complex metaphorical terms in view of their word-forming and semantic derivation, compatibility, and modeling based on structural-grammatical and semantic-motivational features.

The research material consisted of specialized dictionaries of information and cybersecurity in three languages, as well as English-language documents related to the field of digital information protection.

Key words: *information security, terminological nomination, metaphor typology, conceptual integration, structural-grammatical model.*

REFERENCES

Balla M. I. (1996). Anhlo-ukrainskyi slovnyk [English-Ukrainian dictionary]. T. 2: L–Z. Kyiv : Osvita [in Ukrainian].

Bohush V. M., Kryvutsa V. H., Kudin A. M. (2004). Informatsiina bezpeka: Terminolohichnyi navchalnyi dovidnyk [Information security: Terminological educational reference book]. Kyiv : D.V.K. [in Ukrainian].

Brooks F. P. (1987). No silver bullet – Essence and accident in software engineering. *Computer.* 20(4), pp. 10–19. https://doi.org/10.1109/MC.1987.1663532 [in English].

Bulyk-Verkhola H. V., Nakonechna S. Z., Tehlivets Yu. V. (2016). Osnovy terminoznavstva [Fundamentals of terminology studies] (3rd ed.). Lviv : Polytechnic Publishing House [in Ukrainian].

Chystokletov O. O., Khytra O. L. (2023). Slovnyk z informatsii ta informatsiinoi bezpeky [Dictionary of information and information security]. Lviv : Rastr-7 [in Ukrainian].

Diakov A. S., Kyiak T. R., Kudelko Z. B. (2000). Osnovy terminotvorennia: semantychni ta sotsiolinhvistychni aspekty [Fundamentals of term formation: semantic and sociolinguistic aspects]. Kyiv : KM Academia [in Ukrainian].

Fauconnier G., Turner M. (2002). The Way We Think: Conceptual Blending and The Mind's Hidden Complexities. New York : Basic Books [in English].

Hoopes J. (2009). Virtualization for security: Including sandboxing, disaster recovery, high availability, forensic analysis, and honeypotting. Syngress Publishing, Inc.; Elsevier [in English].

Ivaschenko V. L. (2006). Kontseptualna reprezentatsiia spetsialnykh znan u movi (na materiali mystetstvoznavchoi terminolohii) [Conceptual representation

of special knowledge in language (based on the material of art criticism terminology)]. Kyiv : Dmytro Buraho Publishing House [in Ukrainian].

Kryshtal S. M. (2003). Strukturno-semantychnyi analiz metaforychnykh terminiv pidmovy finansiv v anhliiskii i ukrainskii movakh [Structural and semantic analysis of metaphorical terms of the sublanguage of finance in English and Ukrainian languages]: Doctoral dissertation. Donetsk [in Ukrainian].

Kushnerov O. S. (Comp.). (2021). Bezpeka informatsii: konspekt lektsii [Information security: lecture notes]. Sumy : Sumy State University [in Ukrainian].

Lektovarov K. S. (2017). Verbalizovanyi kontsept SECURITY v anhlomovnii kartyni svitu [Verbalized concept SECURITY in the English-language picture of the world]: Extended abstract of Doctoral dissertation. Odessa [in Ukrainian].

Levchenko O. H., Zemlianska O. V. At al. (2019). Bezpeka zhyttiediialnosti ta tsyvilnyi zakhyst [Life safety and civil protection]. Kyiv : Karavela [in Ukrainian].

Mishchenko A. L. (2014). Terminolohichni zasady tekhnolohichno-oriientovanoho haluzevoho perekladu (na materiali nimetskoi, ukrainskoi i anhliiskoi mov) [Terminological foundations of technology-oriented branch translation (based on German, Ukrainian and English languages)]. Kirovograd : Lysenko V. F. [in Ukrainian].

Musiienko I. I. (Ed.). (2014). Slovnyk kliuchovykh poniat ta abreviatur sektoru bezpeky: anhlo-ukrainsko-rosiiskyi [Dictionary of key concepts and abbreviations of the security sector: English-Ukrainian-Russian]. Kharkiv : Oberih [in Ukrainian].

Palchevska O. S., Dobrovolska S. R. at al. (2025). Anhlo-ukrainskyi hlosarii terminiv IT-tekhnolohii ta kiberbezpeky [English-Ukrainian glossary of IT and cybersecurity terms]. Lviv : Lviv State University of Life Safety [in Ukrainian].

Perkhach R.-Yu. T. (2017). Terminolohiia v instruktsiiakh do medychnykh preparativ: linhvokohnityvnyi ta linhvokulturnyi aspekty (na materiali ukrainskoi, polskoi, nimetskoi mov) [Terminology in instructions for medical drugs: linguo-cognitive and linguo-cultural aspects (based on Ukrainian, Polish, German languages)]: Doctoral dissertation. Lviv [in Ukrainian].

Pysmenskyi Ye. O., Holovkin S. V. (2023). Rozsliduvannia kolaboratsiinoi diialnosti [Investigation of collaboration activities]. Kyiv : VD Dakor [in Ukrainian].

Sadovnykova H. V. (2016). Kohnityvno-informatsiina pryroda terminiv avtomobilebudivnytstva v anhliiskii, nimetskii ta ukrainskii movakh [Cognitive-informational nature of automobile construction terms in English, German and Ukrainian languages]: Doctoral dissertation. Kyiv [in Ukrainian].

Selivanova O. O. (2011). Linhvistychna entsyklopediia [Linguistic encyclopedia]. Poltava : Dovkillia-K. [in Ukrainian].

Stasiuk T. V. (2020). Terminosfera novitnikh tekhnolohii: linhvosotsiokohnityvni chynnyky formuvannia ta rozvytku [Terminosphere of the newest technologies: linguo-socio-cognitive factors of formation and development]: Doctoral dissertation. Kyiv [in Ukrainian].

Tyshchenko O. V. (2017). Movna kontseptualizatsiia небезпеки ta ryzyku v naukovii ta naivnii modeliakh svitu: do problemy linhvistyky bezpeky [Linguistic conceptualization of danger and risk in scientific and naive models of the world: on the problem of security linguistics]. *Studia slawistyczne: etnolingwistyka i komunikacja międzykulturowa*, (4), pp. 69–89 [in Ukrainian].

Tyshchenko O. V. (2024). Osoblyvosti perekladu ta typolohiia avtotransportnykh terminiv (na materiali ukrainskoi, anhliiskoi, nimetskoi, polskoi ta italianskoi mov) [Features of translation and typology of motor vehicle terms (based on Ukrainian, English, German, Polish, and Italian)]. *Lvivskyi filolohichnyi chasopys* [*Lviv Philological Journal*], (15), pp. 113–121. https://doi.org/10.32447/2663-340X-2024-15.15 [in Ukrainian].

Viiskovyi hlosarii [Military glossary]. (2026). https://english-military-dictionary.org.ua [in Ukrainian].

Khudolii A. O. (2022). Informatsiina viina 2014–2022 rr. [Information war 2014–2022]. Ostroh : National University of Ostroh Academy [in Ukrainian].

Zaplatynskyi V. M. (2012). Lohiko-determinantni pidkhody do rozuminnia poniattia "Bezpeka" [Logical-determinant approaches to understanding the concept of "Security"]. *Visnyk Kamianets-Podilskoho natsionalnoho universytetu imeni Ivana Ohiienka. Fizychne vykhovannia, sport i zdorovia liudyny* [*Bulletin of the Ivan Ohienko Kamianets-Podilskyi National University. Physical Education, Sports and Human Health*], (5), pp. 41–49 [in Ukrainian].

Zdrodowski B. (red.) (2008). Słownik terminów z zakresu bezpieczeństwa narodowego. 6-te wyd. Warszawa : Akademia Obrony Narodowej; Wiedza [in Polish].

Дата першого надходження статті до видання: 27.02.2026
Дата прийняття статті до друку після рецензування: 08.04.2026
Дата публікації (оприлюднення) статті: 29.05.2026