ВІСНИК науки та освіти
ISSN 2786-6165 (ONLINE) №3(45) 2026
Bulletin of Science and Education

УДК 81'42:004.738.5:327.88

https://doi.org/10.52058/2786-6165-2026-3(45)-1053-1066

Лунгол Ольга Миколаївна кандидат педагогічних наук, доцент, завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0001-8128-0072

Габорець Ольга Андріївна доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0001-7791-6795

Тулінов Валентин Сергійович кандидат юридичних наук, доцент, заступник директора Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0002-3972-348X

ЛІНГВІСТИЧНІ АСПЕКТИ ІДЕНТИФІКАЦІЇ МАНІПУЛЯТИВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ МЕТОДАМИ OSINT-АНАЛІЗУ

Анотація. У статті досліджено актуальну проблематику ідентифікації маніпулятивного контенту в цифровому середовищі, що набуває критичного значення в умовах гібридної війни та безперервних інформаційно-психологічних операцій. Визначено, що традиційні технічні засоби кіберзахисту та базові алгоритми автоматизованої модерації є об’єктивно недостатніми для ефективної протидії комплексним соціотехнічним загрозам. Такі загрози еволюціонують і дедалі частіше цілеспрямовано експлуатують когнітивні вразливості користувачів, обходячи стандартні фільтри безпеки завдяки гнучким мовним конструкціям. У цьому контексті науково обґрунтовано нагальну необхідність застосування нового міждисциплінарного підходу, що гармонійно поєднує інструментарій прикладного лінгвістичного аналізу з передовими методами розвідки на основі відкритих джерел (OSINT). У межах дослідження проаналізовано та систематизовано

ключові лінгвістичні маркери, а також когнітивні тригери маніпулятивного впливу. Серед них особлива увага приділяється створенню ефекту штучного дефіциту часу для провокування імпульсивних рішень, стилістичній імітації офіційної лексики державних чи міжнародних інституцій з метою формування безпідставної довіри, а також експлуатації «тригера безпеки», що апелює до базових страхів людини, таких як загрози втрати коштів, персональних даних, життя тощо. У роботі доведено, що філологічний (зокрема, семантико-прагматичний та емоційно-експресивний) скринінг текстів виступає високоефективним первинним фільтром для точного виявлення деструктивних і маніпулятивних наративів на ранніх етапах їх поширення. Своєю чергою, залучення OSINT-інструментарію забезпечує формування надійної технічної доказової бази. Вона є критично необхідною для деанонімізації джерел загрози, аналізу інфраструктури зловмисників через перевірку доменних імен, SSL-сертифікатів, цифрових слідів, побудови соціальних графів зв'язків та визначення масштабів скоординованих кібератак або фішингових кампаній.

На основі отриманих результатів авторами розроблено, концептуально обґрунтовано та успішно апробовано на актуальному практичному кейсі комплексну чотирьохетапну синергетичну модель ідентифікації маніпулятивного контенту. Ця інноваційна модель послідовно охоплює: первинний лінгвістичний скринінг тексту; екстракцію цифрових артефактів; проведення детального OSINT-аналізу вилучених артефактів; фінальну атрибуцію загрози з формуванням комплексного профілю суб'єкта атаки.

Практичне значення одержаних результатів полягає у підвищенні аналітичних та операційних спроможностей правоохоронних органів, підрозділів кримінального аналізу та фахівців із кібербезпеки.

Впровадження запропонованої методології створює наукове та практичне підґрунтя для переходу від реактивного реагування до проактивного виявлення, документування та нейтралізації інформаційно-психологічних операцій, фішингових мереж і тіньової інфраструктури кіберзлочинців ще на етапі їх початкового розгортання в глобальній мережі Інтернет.

Ключові слова: маніпулятивний контент; OSINT-аналіз; лінгвістичні маркери; гібридна війна; інформаційно-психологічні операції (ІПСО); когнітивні тригери; кібербезпека; соціальна інженерія.

Lunhol Olha PhD, Docent, Head of the Department of Operational-Search Activity and Information Security of the Educational and Scientific Institute for the Training Specialists for Criminal Police Units named after E.O. Didorenko of Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0001-8128-0072

Haborets Olha PhD, Docent, Associate Professor of the Department of Operational-Search Activity and Information Security of the Educational and Scientific Institute for the Training Specialists for Criminal Police Units named after E.O. Didorenko of Donetsk State University of Internal Affairs, Kropyvnytskyi, ehttps://orcid.org/0000-0001-7791-6795

Tulinov Valentyn, PhD, Docent, Deputy Director of the Educational and Scientific Institute for Training Specialists for Criminal Police Units named after E.O. Didorenko of Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0002-3972-348X

LINGUISTIC ASPECTS OF IDENTIFYING MANIPULATIVE ONLINE CONTENT THROUGH OSINT TECHNIQUES

Abstract. The article explores the pressing issue of identifying manipulative content in the digital environment, which is of critical importance in the context of hybrid warfare and continuous information and psychological operations. It is determined that traditional technical means of cyber defense and basic algorithms of automated moderation are objectively insufficient to effectively counter complex socio-technical threats. Such threats evolve and increasingly purposefully exploit users' cognitive vulnerabilities, bypassing standard security filters through flexible linguistic constructs. In this context, the urgent need to apply a new interdisciplinary approach that harmoniously combines the tools of applied linguistic analysis with advanced open-source intelligence (OSINT) methods is scientifically substantiated.

Within the scope of the study, key linguistic markers, as well as cognitive triggers of manipulative influence, are analyzed and systematized. Among them, special attention is paid to creating the effect of an artificial time deficit to provoke impulsive decisions, the stylistic imitation of the official vocabulary of state or international institutions to build unfounded trust, and the exploitation of the "security trigger," which appeals to basic human fears, such as threats of losing funds, personal data, life, etc. The paper proves that philological (in particular, semantic-pragmatic and emotional-expressive) screening of texts serves as a highly effective primary filter for the accurate detection of destructive and manipulative narratives at the early stages of their spread. In turn, the involvement of OSINT tools ensures the formation of a reliable technical evidence base. It is critically necessary for the deanonymization of threat sources, the analysis of attackers' infrastructure through the verification of domain names, SSL certificates, digital footprints, the construction of social connection graphs, and the determination of the scale of coordinated cyberattacks or phishing campaigns.

Based on the obtained results, the authors have developed, conceptually substantiated, and successfully tested on a relevant practical case a comprehensive four-stage synergetic model for identifying manipulative content. This innovative model sequentially encompasses: primary linguistic screening of the text; extraction of digital artifacts; conducting a detailed OSINT analysis of the extracted artifacts; and the final threat attribution with the formation of a comprehensive profile of the threat actor. The practical significance of the obtained results lies in enhancing the analytical and operational capabilities of law enforcement agencies, criminal analysis units, and cybersecurity specialists. The implementation of the proposed methodology creates a scientific and practical foundation for transitioning from reactive response to proactive detection, documentation, and neutralization of information and psychological operations, phishing networks, and the shadow infrastructure of cybercriminals even at the stage of their initial deployment on the global Internet.

Keywords: manipulative content; OSINT analysis; linguistic markers; hybrid warfare; information and psychological operations (PSYOP); cognitive triggers; cybersecurity; social engineering.

Постановка проблеми. Стрімка цифровізація суспільних процесів зумовила якісну трансформацію загроз у цифровому середовищі. У сучасному глобалізованому світі мережа Інтернет стала не лише універсальним майданчиком для комунікації, але й домінантним каналом поширення деструктивного та маніпулятивного контенту. У контексті сучасної гібридної війни інформаційний простір перетворюється на повноцінне поле протистояння, де цілеспрямований вплив на свідомість людей набуває рис системних інформаційно-психологічних операцій.

Головним інструментом такого впливу виступає мова. Автори маніпулятивних текстів цілеспрямовано використовують специфічні лінгвістичні конструкції для експлуатації когнітивних тригерів аудиторії, таких як страх за власну безпеку, відчуття терміновості або апеляція до псевдоавторитетних джерел. Подібний контент конструюється за чіткими соціолінгвістичними шаблонами: він спрямований на провокування швидкого емоційного реагування користувачів та штучне зниження рівня критичного аналізу отриманої інформації.

Ураховуючи експоненційне зростання обсягів інформації в мережі, людський фактор залишається найбільш уразливою ланкою, а традиційні алгоритми модерації або базові семантичні фільтри виявляються вкрай неефективними перед динамічними маніпулятивними загрозами. Це зумовлює гостру потребу фахівців з інформаційної безпеки в симетричній технологічній відповіді – залученні методів розвідки на основі відкритих

джерел (OSINT) для автоматизованого збору та моніторингу цифрових слідів маніпуляторів.

Проте ефективність застосування OSINT-інструментів суттєво обмежується без інтеграції глибокого лінгвістичного аналізу. Виокремлення суто технічних метаданих (IP-адрес, часу публікації, зв'язків між акаунтами тощо) не дає повної картини без розуміння семантичної та прагматичної сутності поширюваного контенту. Це зумовлює гостру потребу в ґрунтовному науковому осмисленні проблеми та розробці комплексних алгоритмів, які б органічно поєднували технологічні можливості OSINT із методологією прикладної лінгвістики. За таких умов ідентифікацію маніпулятивного контенту доцільно розглядати як системний міждисциплінарний виклик, що вимагає переходу від ручного аналізу текстів до проактивних, автоматизованих моделей виявлення інформаційних загроз.

Аналіз останніх досліджень і публікацій. Проблематика виявлення маніпулятивного контенту, протидії дезінформації та застосування методів розвідки на основі відкритих джерел (OSINT) перебуває в центрі уваги сучасної вітчизняної та зарубіжної науки. Протягом 2022–2025 років відбувся концептуальний зсув: OSINT із суто військової та правоохоронної дисципліни трансформувався у ключовий інструмент забезпечення комплексної інформаційної безпеки. Зокрема, у новітніх дослідженнях у сфері права та безпеки (наприклад, на сторінках фахового видання «Аналітично-порівняльне правознавство» [1]) ґрунтовно аналізується роль відкритої розвідки у протидії масштабним інформаційним війнам та фіксується безпрецедентний розмах цілеспрямованих інформаційно-психологічних операцій (ІПСО).

Водночас профільні аналітики, зокрема, фахівці Molfar [2] акцентують увагу на технологічному вимірі: інтеграції алгоритмів штучного інтелекту (AI OSINT) та інструментів обробки природної мови (NLP) для автоматизованого розпізнавання тональності тексту та виявлення згенерованих маніпулятивних матеріалів.

Вагомий базис для розуміння технологічного та психологічного вимірів кіберзагроз формують праці українських учених. Сучасні концепції розкриття механізмів поширення маніпулятивних наративів у соціальних мережах і традиційних медіа [3] зосереджені на ефективності фактчекінгу та мінімізації ризиків ненавмисного поширення деструктивного контенту.

Важливим фундаментом для розуміння легітимності застосування цифрових інструментів є праці, у яких детально розкрито інноваційні методи та цифрові технології в оперативно-розшуковій діяльності [4 – 6]. Важливим є питання психологічного підґрунтя маніпуляцій у мережі, зокрема специфіка експлуатації когнітивних вразливостей користувачів та

методологічні засади деанонімізації та атрибуції суб'єктів гібридної агресії в національному кіберпросторі за допомогою інструментів OSINT.

Актуальними є дослідження К. Іванової та Т. Гудзь щодо OSINT як інструменту протидії дезінформації та deepfake-технологіям у системі інформаційної безпеки України [7], А. Главацької, О. Ангельської, І. Опірського щодо використання OSINT як нової загрози з деанонімізації особи в Інтернет просторі, Є. Філюка [9] з дослідження методів верифікації відкритих джерел та виявлення дезінформації з використання OSINT-інструментів та ін. Проте, незважаючи на значний масив новітніх наукових розвідок, інтеграція OSINT-інструментарію з прикладним лінгвістичним аналізом залишається фрагментарною. Більшість наявних праць зосереджується або на суто технічних алгоритмах (таких, як мережевий аналіз, виявлення ботоферм, аналіз метаданих тощо), або на загальнотеоретичних аспектах ІПСО та соціальної інженерії. Бракує комплексних міждисциплінарних досліджень, які б пропонували чіткі алгоритми лінгвістичної ідентифікації маніпулятивного контенту, таких, як аналіз семантики, прагматики, емоційно-експресивної лексики тощо з одночасною або подальшою верифікацією джерел його походження методами OSINT-аналізу. Саме потреба в поєднанні філологічного інструментарію з цифровою розвідкою для ефективного і доказового виявлення маніпуляцій у мережі Інтернет зумовлює актуальність і своєчасність нашого дослідження.

Мета статті полягає у комплексному науковому обґрунтуванні та розробленні міждисциплінарної методології ідентифікації маніпулятивного контенту в мережі Інтернет шляхом органічної інтеграції інструментарію прикладного лінгвістичного аналізу з методами розвідки на основі відкритих джерел (OSINT).

Досягнення поставленої мети передбачає вирішення таких завдань, як виокремлення та систематизацію ключових лінгвістичних маркерів (семантичних, прагматичних, синтаксичних та емоційно-експресивних), що свідчать про прихований інформаційно-психологічний вплив у цифрових текстах; визначення ефективних алгоритмів верифікації джерел походження деструктивного контенту та його авторів за допомогою сучасних OSINT-інструментів; формування практичної моделі синергетичного застосування філологічного та цифрового розвідувального інструментарію для підвищення загального рівня інформаційної безпеки та ефективності протидії гібридним кіберзагрозам.

Виклад основного матеріалу. У структурі сучасної організованої кіберзлочинності та гібридних інформаційних операцій маніпулятивний контент постає як складна соціотехнічна загроза. Його еволюція свідчить про перехід від хаотичних інформаційних повідомлень до системного

тіньового бізнесу, що часто функціонує за моделлю «сервісу». Ключовою особливістю такого контенту є те, що первинним об'єктом атаки стає не програмно-апаратна інфраструктура, а безпосередньо людина як носій інформації та найуразливіша ланка будь-якої системи безпеки.

Ефективність маніпулятивних кампаній у мережі Інтернет ґрунтується на експлуатації когнітивних механізмів прийняття рішень через специфічні мовні конструкції. Проведене дослідження дозволяє виокремити декілька рівнів лінгвістичних маркерів, що сигналізують про маніпулятивну природу контенту:

- семантико-прагматичний рівень, що включає використання емоційно насичених формулювань та «шокового» контенту для зниження рівня критичного аналізу інформації. Типовими є наративи, пов'язані з базовими потребами – безпекою, фінансовою допомогою або загрозою втрати активів;
- когнітивні тригери, коли у текстах системно застосовуються маркери терміновості (наприклад, «негайно», «лише сьогодні») та апеляція до авторитету офіційних джерел, наприклад, імітація лексики державних структур, благодійних фондів або відомих брендів), див. табл. 1;
- стилістична імітація через маніпулятивні повідомлення, яка часто стилізуються під офіційне інформування, використовуючи формалізовану лексику та специфічні адміністративні процедури для створення ілюзії легітимності.

Таблиця 1

Приклади когнітивних тригерів

Тип когнітивного тригеру	***Лінгвістичні та стилістичні маркери***	***Типові приклади маніпулятивних фраз***	***Психологічна мета впливу***
Штучний дефіцит часу (терміновість)	Імперативні форми дієслів, прислівники часу, лексика з семантикою обмеженості (кількості або часу), використання знаків оклику та Caps Lock.	«НЕГАЙНО перейдіть за посиланням!»; «Ваша заявка анулюється через 2 години»; «Лише сьогодні: залишилося 50 гарантованих виплат».	Штучне стимулювання стану стресу; блокування аналітичного (критичного) мислення; примус до швидких, імпульсивних дій.

Тип когнітивного тригеру	*Лінгвістичні та стилістичні маркери*	*Типові приклади маніпулятивних фраз*	*Психологічна мета впливу*
Апеляція до державного авторитету	Офіційно-діловий стиль, канцеляризми, абревіатури, посилання на нормативні акти, закони чи державні програми (часто вигадані або спотворені).	«Згідно з постановою Кабінету Міністрів України № 456-В...»; «Офіційне сповіщення від Національного банку»; «Державна програма підтримки».	Формування безумовної довіри; експлуатація соціального рефлексу підпорядкування офіційним структурам; маскування фішингового наміру.
Імітація міжнародних / благодійних інституцій	Лексика гуманітарної сфери, використання назв відомих трастових організацій (ООН, Червоний Хрест, фонди ЄС тощо), слова-магніти («допомога», «грант» і т.д.).	«Фонд ООН у справах біженців схвалив вашу заявку»; «Фінансова допомога від Європейського Союзу для українців»; «Отримайте компенсацію від Червоного Хреста».	Експлуатація надії та стану соціально-економічної вразливості цільової аудиторії; зниження порогу підозрілості до зовнішніх посилань.
Тригер безпеки (страх втрати)	Лексика загрози та попередження, категоричні стверджувальні конструкції, слова з негативною семантикою («крадіжка», «злом», «блокування» тощо).	«УВАГА! Ваш рахунок заблоковано через підозрілу активність»; «Зафіксовано вхід з іншого пристрою»; «Терміново оновіть дані, інакше ваші кошти буде конфісковано».	Провокування почуття тривоги та паніки; примус до добровільного розкриття конфіденційних даних (паролів, CVV-кодів) нібито задля власного «порятунку».

Особливого значення набуває фактор часу. Масове поширення таких повідомлень часто припадає на вечірній або нічний період, коли рівень когнітивної уваги користувача знижений через втому, що підвищує схильність до швидкого прийняття рішень без належної перевірки.

В той час, як лінгвістичний аналіз дозволяє ідентифікувати факт маніпуляції та розкрити її внутрішню комунікативну структуру, методи розвідки на основі відкритих джерел відіграють вирішальну роль у формуванні об'єктивної доказової бази щодо джерела походження загрози, її справжніх масштабів та інфраструктури поширення. У контексті сучасної гібридної війни дослідження маніпулятивного контенту не може обмежуватися аналізом лише окремих інцидентів чи характеристикою загроз у межах однієї локальної мережі. Для глибокого розуміння системності таких атак доцільно залучати інтерактивні аналітичні платформи, що надають масив даних про кіберінциденти у глобальному вимірі.

Одним із потужних інструментів такого класу є інтерактивна платформа Threat Map від Check Point Software Technologies, яка забезпечує комплексну візуалізацію напрямків та інтенсивності атак у режимі реального часу. З наукової та практичної точок зору інтеграція подібних платформ у процес OSINT-аналізу має кілька ключових переваг. По-перше, це дає емпіричне підтвердження того, що інформаційні вкиди є не хаотичними явищами, а системною складовою загальної картини гібридних загроз. Платформи глобального моніторингу дозволяють досліднику спостерігати зміну інтенсивності атак у часі та просторі, а також простежувати чітку кореляцію між сплесками розповсюдження маніпулятивного контенту та конкретними геополітичними або соціально-військовими подіями. По-друге, використання часового та просторового вимірів дозволяє фіксувати хвилі цілеспрямованої активності: наприклад, значне збільшення маніпулятивних або фішингових розсилок у моменти штучного загострення інформаційної напруги в суспільстві. Такий рівень географічної та часової деталізації є критично важливим. Він дозволяє не просто констатувати наявність маніпулятивної лексики в повідомленні, а й застосовувати кількісні методи, часові ряди та моделі прогнозування кіберзагроз з урахуванням факторів гібридного впливу. Таким чином, синергія лінгвістики та глобального OSINT-моніторингу дозволяє розкривати закономірності функціонування маніпулятивних кампаній як складної, багаторівневої системної загрози

Інтеграція OSINT-інструментарію у процес лінгвістичної ідентифікації передбачає:

- аналіз інфраструктури поширення через перевірку зовнішніх URL-посилань, що містяться в тексті. Використання доменів, які не співвід-

носяться з офіційними ресурсами, є ключовим технічним індикатором, що підтверджує лінгвістичну підозру у фішингу чи маніпуляції.

- деанонімізація суб'єктів через застосування методів OSINT для атрибуції (встановлення приналежності) контенту до конкретних кластерів кіберзагроз. Цей процес дозволяє вийти за межі аналізу одного тексту до виявлення цілих кампаній, що діють за моделлю Phishing-as-a-Service (PhaaS).

- кореляційний аналіз, що полягає у співставленні піків поширення певних лінгвістичних наративів із геополітичними або соціально-військовими подіями, що підтверджує їхній характер як елементів інформаційно-психологічних операцій.

Розробка дієвої системи ідентифікації маніпулятивного контенту вимагає переходу від фрагментарного використання окремих методів до побудови єдиного дослідницького алгоритму. Пропонована синергетична модель включає чотири послідовні етапи:

1. *Лінгвістичний первинний скринінг*. На цьому етапі текст аналізується на наявність когнітивних тригерів. Дослідник (або автоматизована система на базі NLP) фіксує маркери маніпуляції: імперативні конструкції, штучне створення ефекту дефіциту часу («негайно», «тільки сьогодні»), використання емоційно-забарвленої лексики та підміну понять. Цей етап дозволяє відфільтрувати підозрілий контент із загального інформаційного потоку.

2. *Екстракція цифрових артефактів.* З тексту, що має ознаки маніпулятивності, вилучаються елементи, які можуть слугувати точками входу для цифрової розвідки. До таких артефактів належать: гіперпосилання, нікнейми авторів або адміністраторів каналів, номери телефонів, криптогаманці, хештеги та специфічні сленгові вирази, що можуть вказувати на приналежність до певного кіберзлочинного угруповання.

3. *Глибокий OSINT-аналіз та побудова соціальних графів***.** Вилучені артефакти досліджуються за допомогою спеціалізованого програмного забезпечення (наприклад, Maltego, SpiderFoot, або спеціалізованих Telegram-парсерів). Дослідник встановлює зв'язки між артефактами: перевіряє історію реєстрації доменних імен (Whois), аналізує SSL-сертифікати, здійснює зворотний пошук за зображеннями (Reverse Image Search) та виявляє мережу афілійованих акаунтів або ботоферм, які синхронно поширюють ідентичний контент.

4. *Атрибуція загрози та формування профілю.* На фінальному етапі зібрані технічні та лінгвістичні дані зіставляються з відомими індикаторами компрометації (IoC) та профілями кіберзлочинних кластерів. Це дозволяє довести, що виявлений текст є не простою помилкою чи клікбейтом, а

спланованою інформаційно-психологічною операцією або елементом Phishing-as-a-Service інфраструктури.

Ефективність запропонованого алгоритму можна продемонструвати на прикладі аналізу гібридної фішингової кампанії, спрямованої на громадян України на початку 2026 року.

Кампанія експлуатувала соціально чутливу тему «нових європейських грантів на відновлення житла».

На першому етапі (лінгвістичний скринінг) було зафіксовано повідомлення, що масово поширювалося у регіональних Telegram-каналах. Лінгвістичний аналіз виявив: стилістичну імітацію (текст копіював офіційний стиль комунікації державних органів – використання абревіатур, посилання на неіснуючі постанови Кабінету Міністрів України і т.д.; емоційно-експресивні маркери – наявність слів-магнітів («гарантована виплата», «швидке оформлення») у поєднанні з тригером втрати («фонд вичерпується, залишилося 200 місць»); синтаксичні аномалії – нетипова побудова речень, що свідчила про можливе використання інструментів машинного перекладу з російської мови.

На етапі екстракції артефактів було виділено скорочене URL-посилання, замасковане під державний портал реєстрації, та контактний акаунт «технічної підтримки».

Застосування OSINT-інструментарію дозволило провести дослідження. Аналіз доменного імені показав, що ресурс був зареєстрований лише за 48 годин до початку розсилки через офшорного реєстратора, що є типовою ознакою фішингової інфраструктури.

Перевірка SSL-сертифіката виявила ще 12 подібних доменів, розгорнутих на одній IP-адресі. Зворотний пошук за нікнеймом «технічної підтримки» дозволив знайти зв’язок із тіньовими форумами, де зловмисники орендували PhaaS-інфраструктуру для збору персональних та банківських даних користувачів.

Таким чином, комплексне застосування лінгвістичного аналізу дозволило вчасно звернути увагу на маніпулятивний характер комунікації, тоді як методи OSINT забезпечили технічне підтвердження загрози та дозволили правоохоронним органам своєчасно ініціювати блокування всієї мережі шкідливих ресурсів, а не лише окремого повідомлення.

Висновки. У результаті проведеного комплексного дослідження обґрунтовано, що в умовах гібридної інформаційної війни та стрімкої еволюції організованої кіберзлочинності, зокрема поширення моделі Phishing-as-a-Service, ідентифікація маніпулятивного контенту вимагає переходу від фрагментарних методів до системних міждисциплінарних підходів.

Доведено, що традиційні алгоритми модерації або ізольований аналіз суто технічних метаданих є недостатніми для ефективної протидії сучасним соціотехнічним загрозам.

Систематизовано ключові лінгвістичні маркери маніпулятивного впливу. Встановлено, що зловмисники цілеспрямовано конструюють тексти з використанням когнітивних тригерів (штучний дефіцит часу, апеляція до авторитету державних структур, експлуатація почуття страху або надії), що дозволяє їм долати критичне мислення користувачів на емоційному рівні. Саме філологічний (семантико-прагматичний) аналіз виступає первинним фільтром, що дозволяє виокремити деструктивний наратив із загального інформаційного потоку.

Доведено, що методи OSINT є невід'ємною складовою доказової бази. Інтеграція OSINT-інструментарію, наприклад, аналіз доменних імен, SSL-сертифікатів, побудова соціальних графів через спеціалізоване ПЗ тощо, дозволяє трансформувати лінгвістичну підозру в технічно підтверджений факт кібератаки, деанонімізувати суб'єктів загрози та встановити реальні масштаби інформаційно-психологічної операції.

Розроблено та апробовано на практичному кейсі комплексну чотирьохетапну синергетичну модель ідентифікації маніпулятивного контенту: лінгвістичний скринінг, екстракція цифрових артефактів, глибокий OSINT-аналіз, атрибуція загрози. Впровадження цієї моделі дозволить правоохоронним органам та фахівцям з кібербезпеки діяти проактивно: своєчасно виявляти маніпулятивні мережі на етапі їх розгортання та ініціювати блокування всієї шкідливої інфраструктури.

Перспективи подальших наукових розвідок у цьому напрямі доцільно зосередити на питаннях автоматизації запропонованого алгоритму, зокрема шляхом інтеграції великих мовних моделей та алгоритмів штучного інтелекту для потокового лінгво-семантичного скринінгу цифрових комунікацій у режимі реального часу.

Література:

1. Відкрита розвідка (OSINT) у протидії інформаційним війнам. *Аналітично-порівняльне правознавство*. 2024. URL: https://app-journal.in.ua/wp-content/uploads/2025/12/45-1.pdf (дата звернення: 28.03.2026).

2. OSINT & AI: як оптимізувати своє розслідування. *Molfar*. 2024. URL: https://molfar.com/blog/osint-ai-yak-optymizuvaty-svoe-rozsliduvannya-u-2024-roci (дата звернення: 25.03.2026).

3. Георгієвська В. В. Розвінчення російських ІПСО на базі медіаплатформи (кваліфікаційне дослідження). Київ : Київський столичний університет імені Бориса Грінченка, 2025. URL: https://elibrary.kubg.edu.ua/id/eprint/55475/ (дата звернення: 22.03.2026).

4. Лунгол О. М., Габорець О. А. Інноваційні методи та цифрові технології в оперативно-розшуковій діяльності. *Актуальні питання у сучасній науці*. 2023. № 11 (17). С. 602–615.

5. Габорець О. А., Лунгол О. М. Соціальна інженерія як феномен інформаційного впливу в цифровому середовищі. *Національні інтереси України*. 2025. № 11 (16). С. 95–104. URL: https://surl.li/dathod (дата звернення: 20.03.2026).

6. Лунгол О. М. Методологічні засади атрибуції суб'єктів гібридної агресії в національному кіберпросторі. *Кібербезпека: освіта, наука, техніка*. 2025. № 2 (30). С. 374–382. URL: https://surl.li/tekobp (дата звернення: 28.03.2026).

7. Іванова К. І., Гудзь Т. І. OSINT як інструмент протидії дезінформації та deepfake-технологіям у системі інформаційної безпеки України. *Національна безпека України: виклики та реалії сьогодення* : тези доп. учасників кругл. столу (м. Вінниця, 31 жовт. 2025 р.) : у 2-х ч. Вінниця : ХНУВС, 2025. Ч. 2. С. 32–33.

8. Главацька А., Ангельська О., Опірський І. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. *Кібербезпека: освіта, наука, техніка*. 2024. № 1 (25). С. 19–50.

9. Джулій В., Муляр І., Філюк Є. Метод верифікації відкритих джерел та виявлення дезінформації за допомогою OSINT-інструментів. Measuring and Computing Devices in Technological Processes. 2025. № 84 (4). С. 107–121. DOI: https://doi.org/10.31891/2219-9365-2025-84-13

References:

1. Vidkryta rozvidka (OSINT) u protydii informatsiinym viinam [Open-source intelligence (OSINT) in countering information wars]. (2024). *Analitychno-porivnialne pravoznavstvo – Analytical and Comparative Jurisprudence*. Retrieved from https://app-journal.in.ua/wp-content/uploads/2025/12/45-1.pdf [in Ukrainian].

2. OSINT & AI: yak optymizuvaty svoie rozsliduvannia [OSINT & AI: how to optimize your investigation]. (2024). *Molfar*. Retrieved from https://molfar.com/blog/osint-ai-yak-optymizuvaty-svoe-rozsliduvannya-u-2024-roci [in Ukrainian].

3. Heorhiievska, V. V. (2025). Rozvinchennia rosiiskykh IPSO na bazi mediaplatformy (kvalifikatsiine doslidzhennia) [Debunking Russian psychological operations based on a media platform (qualification research)]. Kyiv: Kyivskyi stolychnyi universytet imeni Borysa Hrinchenka. Retrieved from https://elibrary.kubg.edu.ua/id/eprint/55475/ [in Ukrainian].

4. Lunhol, O. M., & Haborets, O. A. (2023). Innovatsiini metody ta tsyfrovi tekhnolohii v operatyvno-rozshukovii diialnosti [Innovative methods and digital technologies in operational-search activities]. *Aktualni pytannia u suchasnii nautsi – Current issues in modern science*, 11 (17), 602–615 [in Ukrainian].

5. Haborets, O. A., & Lunhol, O. M. (2025). Sotsialna inzheneriia yak fenomen informatsiinoho vplyvu v tsyfrovomu seredovyshchi [Social engineering as a phenomenon of information influence in the digital environment]. *Natsionalni interesy Ukrainy – National Interests of Ukraine*, 11 (16), 95–104. Retrieved from https://surl.li/dathod [in Ukrainian].

6. Lunhol, O. M. (2025). Metodolohichni zasady atributsii subiektiv hibridnoi ahresii v natsionalnomu kiberprostori [Methodological principles of attribution of subjects of hybrid aggression in the national cyberspace]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technique*, 2 (30), 374–382. Retrieved from https://surl.li/tekobp [in Ukrainian].

7. Ivanova, K. I., & Hudz, T. I. (2025). OSINT yak instrument protydii dezinformatsii ta deepfake-tekhnolohiiam u systemi informatsiinoi bezpeky Ukrainy [OSINT as a tool for countering disinformation and deepfake technologies in the information security system of Ukraine]. *Proceedings from Natsionalna bezpeka Ukrainy: vyklyky ta realii sohodennia: tezy dop. uchasnykiv kruhl. stolu – National Security of Ukraine: Challenges and Realities of Today: Abstracts of the Round Table*. (Part 2), (pp. 32–33). Vinnytsia: KhNUVS [in Ukrainian].

8. Hlavatska, A., Anhelska, O., & Opirskyi, I. (2024). Doslidzhennia tekhnolohii vykorystannia OSINT yak novoi zahrozy z deanonimizatsii osoby v internet prostori [Research on the technology of using OSINT as a new threat to person's deanonymization in the Internet space]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technique*, 1 (25), 19–50 [in Ukrainian].

9. Dzhulii, V., Muliar, I., & Filiuk, Ye. (2025). Metod veryfikatsii vidkrytykh dzherel ta vyiavlennia dezinformatsii za dopomohoiu OSINT-instrumentiv [Method of open source verification and detection of disinformation using OSINT tools]. Measuring and Computing Devices in Technological Processes, 84 (4), 107–121. https://doi.org/10.31891/2219-9365-2025-84-13 [in Ukrainian].

Дата першого надходження статті до видання: 10.03.2026
Дата прийняття статті до друку після рецензування: 25.03.2026