КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1255
УДК 355.40:004.056]:323(477)

Носов Віталій Вікторович
кандидат технічних наук, доцент, професор кафедри протидії кіберзлочинності
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID:0000-0002-7848-6448
vitnos.g@gmail.com

Манжай Олександр Володимирович
кандидат юридичних наук, професор, завідувач кафедри протидії кіберзлочинності
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID:0000-0001-5435-5921
sofist@ukr.net

Лучик Світлана Дмитрівна
доктор економічних наук, професор, професор кафедри інформаційних систем і технологій
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID:0000-0003-0757-1140
luchiksvitlana@gmail.com

Стецик Роман Мирославович
курсант Навчально-наукового інституту №4
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID:0009-0009-1263-184X
romanstetsyk06@gmail.com

Садовий Костянтин Віталійович
кандидат технічних наук, доцент, начальник кафедри озброєння радіотехнічних військ
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна
ORCID:0000-0003-2703-9696
971sadovyi@gmail.com

ДЕЗІНФОРМАЦІЙНІ КАМПАНІЇ В УКРАЇНІ: МЕТОДОЛОГІЯ СТРУКТУРИЗАЦІІ НА ОСНОВІ ФРЕЙМВОРКУ DISARM ТА ПЛАТФОРМИ OPENCTI

Анотація. З початком повномасштабної російської агресії в Україні агресивне використання цифрового середовища ворогом еволюціонувало від розрізнених пропагандистських актів до моделювання потужних дезінформаційних кампаній. Це обумовлює необхідність розробки і впровадження стандартизованих методологій структуризації даних, що базуються на інструментарії розвідки загроз, зокрема. на фреймворку DISARM та платформі OpenCTI. Метою статті є розробка та наукове обґрунтування методології структуризації дезінформаційних кампаній через призму тактик і технік DISARM із використанням графів знань платформи OpenCTI, на основі аналізу експериментальних даних щодо внутрішньої дестабілізації суспільства та дискредитації військовослужбовців України.

Під час дослідження використано: загальнонаукові теоретичні методи, такі як системний аналіз і абстрактно-логічний метод для здійснення теоретичних узагальнень та формулювання висновків і рекомендацій стосовно структуризації дезінформаційних кампаній; метод кластеризації – для виділення найбільш потужних у першій половині 2025 року дезінформаційних кампаній, графовий метод – для візуалізації та аналізу структури мережі дезінформаційних інцидентів.

Застосування графового методу для побудови структурних графів дезінформаційних кампаній дозволило авторам побудувати архітектуру, топологію та динаміку поширення дезінформації в інформаційному просторі України, а STIX Visualizer забезпечило можливість перегляду побудованих графів онлайн. Для виділених дезінформаційних кампаній визначені найбільш поширені канали та веб ресурси, які систематично виступали джерелами або ключовими вузлами розповсюдження дезінформаційних повідомлень. Використання програмного інструменту Gephi забезпечило можливість візуалізувати

результати аналізу графів, дослідити архітектури поширення дезінформаційних повідомлень. Порівняно із застосуванням систем на базі штучного інтелекту Gephi дозволяє досліднику більш зручно намічати шляхи подальшого дослідження та виключає галюцинаційні помилки, що можуть бути допущені інструментами на базі штучного інтелекту.

Ключові слова: дезінформаційна кампанія; методологія; структуризація; фреймворк; відкрита платформа; графовий метод; великі дані; візуалізація; штучний інтелект.

ВСТУП

З початком повномасштабної російської агресії інформаційне протистояння в Україні характеризується докорінною трансформацією стратегій дезінформаційного впливу. Агресивне використання цифрового середовища ворогом еволюціонувало від розрізнених пропагандистських актів до моделювання потужних дезінформаційних кампаній. Це обумовлює необхідність впровадження стандартизованих методологій структуризації даних, що базуються на інструментарії розвідки загроз (Threat Intelligence), зокрема на фреймворку DISARM (Disinformation Analysis and Response Measures) та платформі OpenCTI (Open Cyber Threat Intelligence).

Постановка проблеми. Незважаючи на інтенсивний розвиток засобів стратегічних комунікацій, у сфері інформаційної безпеки України зберігається суттєва науково-практична проблема, що полягає у відсутності уніфікованих алгоритмів функціональної структуризації дезінформаційних операцій. Дана проблема детермінована низкою критичних аспектів:

1. Методологічна інваріантність аналізу. Існуючі підходи часто ігнорують функціональну специфіку кампаній різної спрямованості. Експериментальні дані 2025-2026 рр. демонструють, що ДК з дестабілізації суспільства та ДК з дискредитації військовослужбовців мають принципово відмінні топологічні характеристики та набори тактик, технік і процедур (TTPs), що потребує диференційованого підходу до їх структурування.
2. Технологічна складність систематизації великих даних. Величезний обсяг неструктурованої інформації в месенджерах та соціальних мережах унеможливлює ручну обробку індикаторів впливу. Проблема полягає у відсутності формалізованого переходу від сирих даних до об’єктно-орієнтованих моделей у форматі STIX 2.1, що дозволило б автоматизувати процес виявлення ворожих кампаній на ранніх стадіях.
3. Брак когерентності у візуалізації загроз. Традиційні методи представлення результатів аналізу (текстові звіти, статичні таблиці) не відображають динаміку мутації наративів та зв’язків між суб’єктами впливу. Використання графів знань у OpenCTI є критично необхідним для вирішення проблеми візуалізації «інформаційних каскадів», проте методика такої інтеграції для потреб ІПСО ще не набула належного наукового опису.

Отже, розробка методології структуризації дезінформаційних кампаній на основі фреймворку DISARM та платформи OpenCTI є нагальною науковою задачею, вирішення якої дозволить підвищити точність атрибуції інформаційних атак та ефективність прийняття управлінських рішень у сфері національної безпеки.

Аналіз останніх досліджень і публікацій. Питання ідентифікації та класифікації дезінформації розглядалися у працях багатьох вітчизняних та закордонних дослідників. Багато наукових праць присвячені переважно змістовному наповненню поняття «дезінформації» та процесу формування дезінформаційних кампаній. При цьому дослідники часто обмежувалися наративним аналізом або дескриптивними моделями. Наприклад, A. Bârgăoanu і M. Pană у своєму дослідженні [1] якісно аналізують шляхом зіставлення структури аналізу (традиційні методи) та управління ризиками дезінформації (DISARM) з доказами, зібраними за допомогою інструментів розвідки з відкритим кодом (OSINT), після інноваційного аналізу, структурованого відповідно до моделі цілей, дій, результатів та методів (PART). Автори показали, що застосування структури DISARM до кібероперацій може бути корисним для прогнозування та реагування на загрози FIMI, навіть коли такі операції, здається, не мають конкретної, одразу ідентифікованої мети.

На відміну від статичних моделей, DISARM часто називають стандартом, який дозволяє різним відомствам розмовляти однією мовою. M. Prysiazhniuk порівнює фреймворк із періодичною таблицею елементів Менделєєва [2]. Це дозволяє не просто класифікувати інцидент, а й прогнозувати розвиток кампанії. Якщо визначається техніка "створення підробних експертних профілів", то вже відомо, які наступні кроки за протоколом DISARM очікувати від агресора. González F. S., Pastor-Galindo J., Ruipérez-Valiente J. A. спробували інтегрувати дезінформаційні загрози в екосистему CTI з використанням її стандартів CTI (зокрема формату STIX2) для моделювання дезінформації через DISARM [3].

Інтеграцію DISARM-тегування в аналітичні платформи типу OpenCTI розглядали в своєму дослідженні T. S. Niven and C.-T. Li [4]. Автори розробили та протестували інноваційну систему автоматичного тегування інцидентів іноземного інформаційного маніпулювання (FIMI), яка базується на архітектурі DISARM (аналог MITRE ATT&CK для інформаційних загроз). загроз. Дослідження підкреслює, що автоматизація за допомогою великих мовних моделей (LLMs) у поєднанні з фреймворком DISARM дозволяє виявляти закономірності, які раніше залишалися непомітними для людей-модераторів. Інтеграція DISARM-тегування в аналітичні платформи типу OpenCTI перетворює моніторинг на проактивну систему кіберрозвідки. Подібні дослідження провели K. Tseng, J. C. Toledano, Dukach B. De C. Yu., які представили систему DISARM-Agent − автономну архітектуру на основі багатоагентних LLM (великих мовних моделей), спеціально розроблену для розслідування інцидентів FIMI (іноземного інформаційного маніпулювання) у соціальних мережах. Автори акцентують на тому, що результати роботи агентів легко експортуються у форматі STIX 2.1, що робить їх ідеальними для миттєвого завантаження в платформи на кшталт OpenCTI [5].

Проте, попри наявність ґрунтовних теоретичних розробок, практичне застосування таксономій типу DISARM для аналізу повномасштабного воєнного конфлікту 2025-2026 рр. залишається недостатньо висвітленим у науковій літературі. Також спостерігається дефіцит досліджень, присвячених алгоритмізації процесів візуалізації та управління знаннями про інформаційні загрози в межах спеціалізованих платформ, таких як OpenCTI.

Метою статті є розробка та наукове обґрунтування методології структуризації дезінформаційних кампаній через призму тактик і технік DISARM із використанням графів знань платформи OpenCTI, на основі аналізу експериментальних даних щодо внутрішньої дестабілізації суспільства та дискредитації військовослужбовців України.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У сучасному інформаційному середовищі дезінформаційні інциденти характеризуються високою складністю, багаторівневістю та швидкістю поширення, що ускладнює їх своєчасне виявлення, аналіз і протидію. Для ефективного дослідження, класифікації та прогнозування подібних атак необхідна уніфікована система опису їхньої структури та взаємозв'язків. Таку функцію виконує система DISARM, яка забезпечує стандартизовану модель опису дезінформаційних кампаній, дозволяючи систематизувати їхні етапи, тактики, методи та цілі.

Для обміну структурованими даними між різними організаціями та аналітичними системами застосовується формат STIX, що забезпечує сумісність, точність і машинозчитуваність описів загроз. Він дозволяє ефективно «транспортувати» результати аналізу DISARM між платформами кіберрозвідки, зберігаючи логічні зв'язки між елементами кампанії.

Для візуалізації, управління та глибокого аналітичного опрацювання отриманої інформації використовуються спеціалізовані платформи, серед яких OpenCTI (Open Cyber Threat Intelligence Platform, Відкрита платформа розвідданих про кіберзагрози). Вона забезпечує інтеграцію даних у форматі STIX, відображення взаємозв'язків між суб'єктами дезінформації, тактиками і каналами поширення, а також може використовуватися як для візуалізації, так і для безпосереднього створення та редагування структур загроз. Водночас існують рішення, орієнтовані насамперед на онлайн-візуалізацію даних без подальшої їх модифікації, серед яких сайт STIX Visualizer.

DISARM – це спеціалізована система, створена для опису, класифікації та розуміння інцидентів, пов'язаних із дезінформацією. Вона розроблена як адаптація підходів і практик інформаційної безпеки до сфери інформаційних впливів, зокрема до боротьби з дезінформацією, маніпуляціями та іншими формами інформаційної шкоди і використовується для їх опису: упорядковує процес від створення фейкового повідомлення до його поширення, посилення та закріплення в свідомості аудиторії. Її застосування дозволяє «оцифрувати» дезінформаційну операцію, представляючи її у вигляді структурованої послідовності фаз, дій, залучених акторів і застосованих тактик. DISARM надає аналітикам, дослідникам і фахівцям із комунікацій єдину методологічну основу для відстеження, опису, аналізу та нейтралізації дезінформаційних операцій, і тим самим забезпечує єдиний формат документування інформаційних атак, що унеможливлює дублювання даних і полегшує координацію між суб'єктами, які протидіють дезінформації.

На основі аналізу останніх звітів, зокрема Antagonistic Information Threats, 2026 [6] та результатів роботи ШІ-агентів, можна виділити групу технік DISARM, які стали "робочими конячками" дезінформаційних кампаній в Україні у 2025-2026 роках. Ворожі операції змістилися від простого поширення фейків до складної імітації внутрішньоукраїнського дискурсу. До ключових DISARM-технік останніх років слід віднести наступні.

1. Фаза планування та підготовки (Resource Planning):

T0143: Create Inauthentic Profiles (Створення неавтентичних профілів. У 2025 році зафіксовано перехід до "глибоких профілів" – ботів, які роками ведуть звичайні соцмережі, постять фото котів і репостять меми, щоб у критичний момент вкинути дезінформацію.

T0158: Acquire/Create Infrastructure (Придбання/створення інфраструктури). Масове створення мереж "сплячих" Telegram-каналів, які мімікрують під локальні медіа невеликих міст України.

2. Фаза виконання (Execution):

T0083: Create Cross-Platform Content (Створення крос-платформного контенту). Кампанія запускається одночасно в TikTok (відео), Telegram (текст) та Facebook (обговорення), створюючи ілюзію "повсюдності" певної проблеми;

T0140: Impersonate Legitimate Entities (Імітація легітимних організацій). Створення клонів сайтів державних органів (Дія, МОУ) або відомих медіа для публікації фейкових наказів чи новин, що провокують паніку.

3. Фаза поширення (Dissemination):

T0040: Micro-target Audience (Мікротаргетинг аудиторії). Використання викрадених або куплених баз даних для таргетованої реклами на конкретні професійні чи соціальні групи (наприклад, дружин військовослужбовців або мешканців прифронтових громад);

T0041: Use Automated Tools/Bots (Використання автоматизованих інструментів). Масована атака коментарями під постами лідерів думок для створення ілюзії "народного гніву".

4. Фаза впливу (Impact):

T0103: Flooding the Information Space (Затоплення інформаційного простору). Техніка "пожежного шлангу", коли продукується така кількість суперечливих версій події, що пересічний громадянин просто втомлюється шукати правду і вимикає критичне мислення.

Отже, фреймворк DISARM виступає як концептуальна основа, що забезпечує систематизацію тактик, технік і процедур (TTPs), характерних для дезінформаційних операцій. Його використання дозволяє декомпозувати складні інформаційні впливи на структурні компоненти та виявити типові патерни поведінки суб'єктів інформаційного протиборства.

Водночас, концептуального опису недостатньо для проведення повноцінного аналізу, особливо в умовах великих обсягів даних та необхідності автоматизації процесів обробки інформації. Це зумовлює потребу у використанні стандартизованих моделей представлення даних. Одним із таких підходів є мова структурованого опису кіберзагроз STIX, яка забезпечує уніфіковане подання об'єктів, їх атрибутів та зв'язків між ними. STIX дозволяє формалізувати елементи дезінформаційних кампаній (актори, інфраструктура, контент, події) у вигляді взаємопов'язаних сутностей, що є критично важливим для подальшого машинного аналізу. Це дозволяє дескриптивні моделі дезінформації трансформувати в об'єктно-орієнтовані структури, придатні для автоматизованої обробки в OpenCTI.

STIX визначає такі основні об'єкти, які описують різні аспекти кіберзагроз: Attack Pattern – шаблон атаки (описує, як зловмисник намагається скомпрометувати ціль); Campaign – кампанія (сукупність дій або хвиль атак, спрямованих на певні цілі); Course of Action – можливі дії у відповідь або рекомендації; Grouping – об'єднання STIX-об'єктів, що мають спільний контекст; Identity – інформація про осіб, організації або групи, пов'язані з інцидентом; Indicator – індикатор, який використовується для виявлення підозрілої активності; Infrastructure – системи, сервіси або ресурси, що підтримують атаки (наприклад, сервери C2); Intrusion Set – набір технік і поведінки, що приписуються певній групі зловмисників; Location – географічне розташування, пов'язане з інцидентом; Malware – шкідливе програмне забезпечення (код, скрипт, вірус тощо); Malware Analysis – результати аналізу конкретного зразка шкідливого ПЗ; Note – текстові пояснення або додаткова контекстна інформація; Observed Data – фактичні дані, зібрані під час спостереження (наприклад, IP, файли, мережеві артефакти); Opinion – оцінка достовірності або коректності інформації; Report – звіт, що об'єднує об'єкти STIX у логічну аналітичну публікацію; Threat Actor – загроза (індивід, група або організація, що діє зі злим наміром); Tool – легітимне програмне забезпечення, яке може бути використане зловмисниками;Vulnerability – вразливість у програмному забезпеченні, яку можна експлуатувати для атаки. STIX 2 також визначає два об'єкти зв'язків: Relationship – використовується для пов'язування двох об'єктів; Sighting – позначає факт спостереження певного об'єкта.

Отже, DISARM може бути інтегрований із STIX, оскільки обидва побудовані за принципом структурованого представлення даних. Це дозволяє описувати дезінформаційні інциденти у форматі STIX, пов'язуючи їх із кіберзагрозами, кампаніями та акторами та оперативно обмінюватися інформацією. Завдяки такій сумісності дані з DISARM можуть використовуватись у платформах, що підтримують STIX. Таким чином, DISARM визначає що саме необхідно аналізувати (таксономія дезінформаційних дій), тоді як STIX визначає яким чином це має бути структуровано у вигляді

формалізованих даних. Наступним логічним кроком є використання програмних платформ, здатних оперувати такими даними, забезпечуючи їх накопичення, кореляцію та аналітичну обробку.

У цьому контексті доцільним є застосування платформи OpenCTI, яка реалізує концепцію управління кіберрозвідувальною інформацією (Cyber Threat Intelligence, CTI) на основі стандарту STIX. OpenCTI забезпечує інтеграцію різнорідних джерел даних, побудову графових моделей взаємозв'язків та візуалізацію складних структур інформаційних операцій.

З позиції дослідження дезінформаційних кампаній, OpenCTI виконує роль інструментального середовища, у якому:

реалізується імпорт та нормалізація даних відповідно до STIX;

здійснюється моделювання елементів дезінформаційних кампаній згідно з таксономією DISARM;

формується графова структура зв'язків між акторами, каналами поширення, контентом і подіями;

забезпечується можливість виявлення прихованих залежностей і сценаріїв інформаційного впливу.

OpenCTI підтримує кілька способів розгортання, що забезпечує її гнучкість та адаптивність до різних інфраструктурних умов. Платформу можна запустити як на локальному комп'ютері, так і на віддаленому сервері. Одним із методів інсталяції є використання контейнеризації через Docker, що спрощує процес налаштування середовища та керування залежностями. Водночас існує можливість традиційного встановлення за допомогою ручної конфігурації компонентів (Node.js, Elasticsearch, Redis, RabbitMQ тощо), що надає користувачеві повніший контроль над архітектурою системи.

Отже, інтеграція фреймворку DISARM, стандарту STIX та платформи OpenCTI формує цілісну методологічну основу дослідження, яка поєднує:

1. концептуальну класифікацію дезінформаційних процесів;
2. формалізоване подання даних;
3. інструментальні засоби аналітичної обробки.

Це, у свою чергу, дозволяє перейти від описового аналізу дезінформаційних кампаній до їх системного моделювання та автоматизованого виявлення структурних закономірностей.

Для виявлення та аналізу актуальних інформаційних загроз у другому півріччі 2025 року було проведено моніторинг масивів даних українських фактчекінгових проєктів, зокрема Gwara Media, StopFake, VoxUkraine та «Детектор медіа».

У результаті аналізу ідентифіковано 418 унікальних дезінформаційних інцидентів [7]. За тематичною спрямованістю та спільними наративними лініями ці інциденти були кластеризовані у наступні дезінформаційні кампанії:

- Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії – 145 інцидентів;
- Дискредитація військовослужбовців України – 130 інцидентів;
- Дискредитація України на міжнародній арені – 35 інцидентів;
- Кросплатформне залучення аудиторії – 32 інциденти.

Перші дві з виділених дезінформаційних кампаній виберемо для подальшого дослідження.

Кампанія «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» характеризується чіткою подвійною спрямованістю. З одного боку, вона націлена на українське населення з метою провокування паніки, відчуття соціально-економічної безвиході та загальної деморалізації суспільства. З іншого боку, ці ж наративи активно використовуються пропагандою на внутрішньому російському ринку для конструювання штучного образу хаотичної та приреченої України. Така стратегія дозволяє ворогу дегуманізувати українців в очах власних громадян, виправдовувати продовження збройної агресії та підтримувати лояльність російського населення до дій свого державного і військового керівництва.

Кампанія «Дискредитація військовослужбовців України» є цілеспрямованою стратегією підриву довіри до Збройних сил як ключового інституту національного спротиву. Вона орієнтована одночасно на українське суспільство та міжнародну спільноту. Головна мета кампанії полягає у системному конструюванні негативного образу українського військового – маргіналізованого, схильного до жорстоких злочинів, недисциплінованого чи покинутого командуванням. Для внутрішньої аудиторії такі маніпуляції покликані стимулювати паніку, зірвати мобілізаційні процеси та спровокувати штучний розкол між армією і цивільним населенням. На зовнішньому рівні ця тактика застосовується для дискредитації держави перед західними партнерами з метою створення образу неконтрольованої сили, що має стати хибним обґрунтуванням для скорочення або повного припинення військової та фінансової допомоги.

Інтеграція зібраних даних до середовища OpenCTI дозволила структурувати елементи дезінформаційних кампаній у вигляді комплексної мережі взаємопов'язаних об'єктів. Архітектура цих зв'язків вибудовувалася поетапно. Спочатку до бази вносилися джерела загроз: анонімні інформаційні

канали та вебресурси реєструвалися як групові суб'єкти загроз (Threat actors – groups), тоді як ідентифіковані особи фіксувалися як індивідуальні суб'єкти загроз (Threat actors – individuals). Далі масив даних був доповнений просторовим контекстом (регіонами, країнами та адміністративними одиницями).

Для точного опису механізмів атаки з офіційного GitHub-репозиторію OpenCTI було імпортовано повний перелік технік (Attack patterns). Цей інструментарій розширений ключовими наративами (Narratives) та доступними заходами нейтралізації (Courses of action). Фактична доказова база формувалася шляхом реєстрації цифрових слідів (Observables) – прямих URL-посилань на ворожі публікації та матеріали фактчекерів із їхнім спростуванням. Після внесення назв конкретних подій через модуль інцидентів (Incidents), усі згенеровані компоненти були додані в єдиний підсумковий звіт.

Послідовність формування зв'язків між об'єктами реалізовувалася за чітко визначеною логікою. На першому етапі URL-адреси виявлених дезінформаційних публікацій поєднувалися з відповідними суб'єктами загроз за допомогою зв'язку related to (пов'язано з), що формалізувало належність маніпулятивного контенту конкретному автору чи каналу поширення (рис. 1).

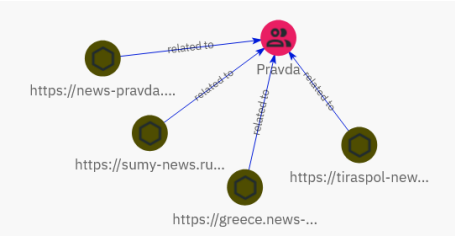

Рис. 1. Зв'язок між суб'єктами загроз та їх публікаціями

Завдяки такій структуризації сформувалася аналітична база для відстеження активності одних і тих самих акторів у межах різних скоординованих кампаній.

Коли під час інциденту фіксувалася каскадна модель поширення фейку, між вторинними публікаціями та оригіналом встановлювався зв'язок derived from (походить від), який візуалізував послідовність поширення дезінформації. При цьому перше повідомлення, визначене як першоджерело маніпуляції, безпосередньо інтегрувалося в загальну структуру інциденту через базовий атрибут related to (рис. .2).

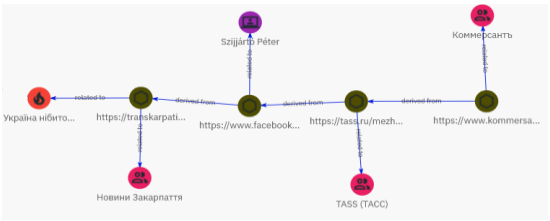

Рис. 2. Візуалізація послідовності поширення дезінформації

У випадках, коли достовірно відтворити хронологічний ланцюжок поширення контенту було неможливо, застосовувався прямий підхід: усі виявлені URL-адреси безпосередньо прив'язувалися до відповідного інциденту через зв'язок related to (рис. 3).

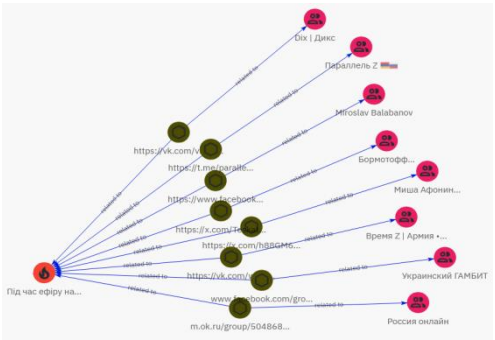

Рис 3. Прив'язка URL до інциденту за відсутності простежуваної послідовності поширення дезінформації

URL-посилання на пости, що містили спростування фейків, поєднувалися з інцидентами (типом зв'язка related to), а також із відповідним контрзаходом (типом зв'язка related to) (рис. 4).

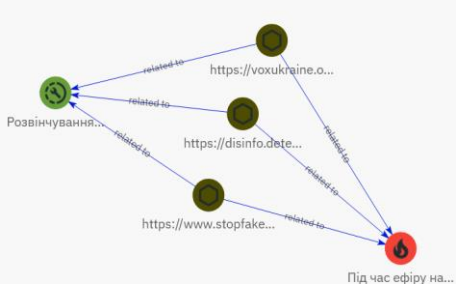

Рис. 4. Зв'язування URL-посилань на спростування фейків з інцидентами та відповідним контрзаходом

На наступному етапі дослідження основна увага зосереджувалася на аналізі інцидентів та технік. Більшість технік була безпосередньо пов'язана з інцидентами через зв'язок типу *uses*, що відображав застосування конкретної техніки в рамках відповідного інциденту (рис. 5).

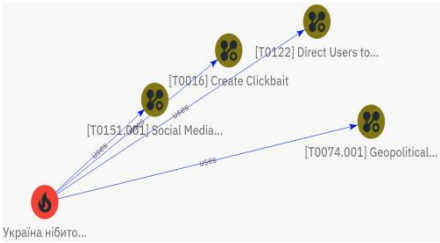

Рис. 5. Зв'язування технік з інцидентами

Для технік, таких як Technique T0003: Leverage Existing Narratives та Technique T0118: Amplify Existing Narrative, використовувалася опосередкована схема побудови зв'язків: спершу інцидент пов'язувався з наративом через зв'язок типу *uses*, що вказує на його застосування інцидентом, а вже наратив був пов'язаний із відповідною технікою через зв'язок типу *related to*, який визначає належність наративу до конкретної техніки (рис. 6).

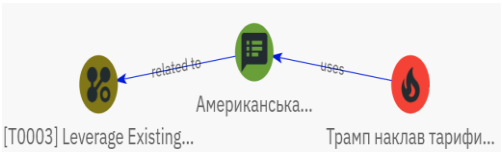

Рис. 6. Опосередковане зв'язування інцидентів з техніками через наративи

Аналогічний підхід застосовувався для техніки Technique T0072.001: Geographic Segmentation: техніка була пов'язана з регіонами, на які спрямовувалася дезінформація, через зв'язок типу related to, тоді як самі регіони виступали як цілі інцидентів і фіксувалися через зв'язок типу targets (рис. 7).

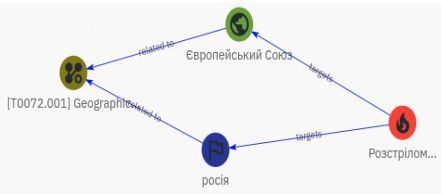

Рис. 7. Опосередковане зв'язування інцидентів з техніками через регіони

За результатами системного аналізу обох дезінформаційних кампаній встановлено, що попри стабільність їхньої загальної архітектури, ключова різноманітність зосереджена у площині інструментарію створення та легітимізації контенту. Найчастіше динамічних змін зазнавали техніки фази підготовки, зокрема щодо переосмислення контексту реальних подій (T0023.001: Reframe Context) та використання «ядра правди» (T0042: Seed Kernel of Truth) для вибудовування видимої достовірності (TA16: Establish Legitimacy). Це дозволяло зловмисникам ефективно адаптувати наративи під специфічні

вразливості цільових аудиторій (TA13: Target Audience Analysis), перетворюючи поодинокі інциденти на масштабні та скоординовані хвилі впливу.

Автори дослідження Носов В. В., Стецик Р.М. систематизували результати аналізу для кампанії "Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії" у вигляді окремого дата сету [8], Аналогічним чином опрацьовано кампанію «Дискредитація військовослужбовців України» [9].

Після інтеграції даних у платформу OpenCTI побудовано структурні графи дезінформаційних кампаній та експортовано відповідні STIX файли: «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» (рис. 8) [10] та «Дискредитація військовослужбовців України» [11]. Для можливості перегляду графів онлайн використано STIX Visualizer, вихідний код якого було частково модифіковано з метою досягнення максимальної відповідності вигляду та структури графів тим, що відображаються в платформі OpenCTI. Після модифікації вихідного коду створено відповідні репозиторії на GitHub та розгорнуто вебсайти («Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» – https://tinyurl.com/mufkvhx8, «Дискредитація військовослужбовців України» – https://tinyurl.com/yc5wfuzw).

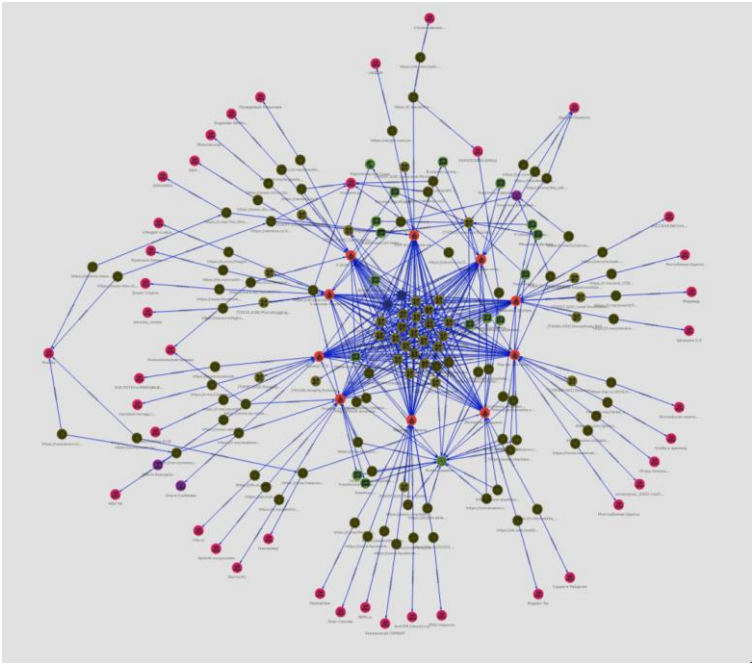

Рис. 8. Граф дезінформаційної кампанії «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії»

Для проведення аналізу граф було конвертовано у табличний формат та приведено до структури, сумісної з програмним забезпеченням Gephi. Крім того, за допомогою табличного редактора було додано нові поля, необхідні для дослідження, зокрема поле *URL_Role*, що дозволяє розділяти фактчекінгові платформи та дезінформаційні пости. Також було створено додаткові вершини типу *platforms* та відповідні зв'язки, що забезпечило коректне відображення структури взаємодій у графі.

Імпорт підготовлених даних до Gephi та подальше застосування методів обробки і узагальнення інформації дали змогу отримати аналітичні показники, які відображають ступінь участі різних платформ у розповсюдженні дезінформації. У результаті було встановлено перелік платформ, що характеризуються найвищими показниками кількості дезінформаційних публікацій.

ISSN 2663 – 4023

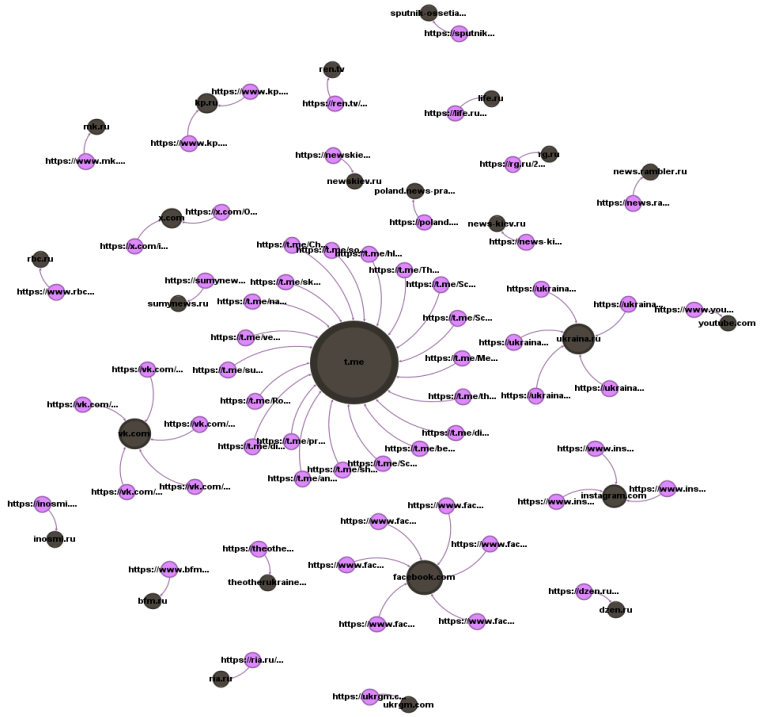

Рис. 9. Розподіл дезінформаційних постів за онлайн-платформами у межах графа «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» (– онлайн-платформа; – дезінформаційний пост)

Результати аналізу (рис. 9) [12] демонструють, що в межах графа «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» для поширення дезінформації найактивніше використовувалися платформи Telegram та Facebook, які перевищували інші платформи за кількістю зафіксованих публікацій.

Натомість аналіз графа «Дискредитація військовослужбовців України» [13] вказує на відмінну структуру залучених платформ, де найчастіше застосовувалися Telegram та Вконтакте.

З метою поглиблення мережевого аналізу було здійснено оцінювання участі онлайн-платформ у поширенні дезінформації не лише за кількістю публікацій, але й за кількістю унікальних інцидентів, у межах яких відповідна платформа виступала каналом розповсюдження. Згідно з отриманими результатами, у межах графа «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» [14] найчастіше в різних випадках фігурували платформи Telegram та Facebook. Окрім цього, було визначено інформаційні приводи, що охоплювали найбільшу кількість різних платформ. До них належать: «90% вступників на бакалаврат в Україні – дівчата», «Україна «закрила доступ ЗМІ» до прифронтових областей, намагаючись приховати катастрофу».

Аналіз графа «Дискредитація військовослужбовців України» [15] показав, що серед платформ, найчастіше задіяних у різних випадках, домінують Telegram та Вконтакте. Найбільше платформ для поширення дезінформації в цьому графі було використано в таких інформаційних приводах: «Військові 95-ї ОШБр розстріляли трьох людей на Сумщині – Нацполіція», «Нетверезий військовий 80-ї ОДШБр на смерть збив 17-річну дівчину» та «Український військовий загинув під Лиманом через відсутність підкріплення», причому останні два характеризуються однаковим рівнем охоплення платформ.

На наступному етапі дослідження було визначено випадки, що характеризувалися найвищим рівнем поширення в мережі, та ідентифіковано первинні джерела (URL), які виконували роль початкових вузлів у процесі розповсюдження відповідних інформаційних повідомлень, відповідно до результатів аналізу, у межах графа «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» [16] до найбільш поширених належать такі інформаційні кейси: «90% вступників на бакалаврат в Україні – дівчата», «Під час обстрілу кияни в метро кричали «Зеленський, спускайся до нас»» та «Україна «закрила доступ ЗМІ», останні два з яких однакові за рівнем поширення.

Водночас результати аналізу графа «Дискредитація військовослужбовців України» [17] показали, що найширше поширення отримав інцидент «У ЗСУ служить оператором БПЛА людина з синдромом Дауна», тоді як інциденти «Нетверезий військовий 80-ї ОДШБр на смерть збив 17-річну дівчину», «Військовий ЗСУ вбив свого побратима за крадіжку» та «Військові 95-ї ОШБр розстріляли трьох людей на Сумщині – Нацполіція» демонструють однаковий, трохи нижчий рівень поширення.

Окремо було здійснено аналіз спільної участі онлайн-платформ у дезінформаційних кейсах, що дав змогу виявити платформи, які найчастіше співфігурували в межах одних і тих самих інформаційних сюжетів, відповідно до отриманих результатів, у межах кампанії «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» [18] найчастіше в одних і тих самих дезінформаційних кейсах спільно фігурували пари платформ ВКонтакте і Telegram, Facebook і Telegram, а також сайт ukraina.ru разом із Telegram.

Натомість аналіз графа «Дискредитація військовослужбовців України» [19] показав, що найтиповішими комбінаціями платформ у межах тих самих інформаційних кейсів є пари Telegram і ВКонтакте, Telegram і X.

Окремо в межах графового аналізу було визначено найбільш поширені канали та вебресурси, які систематично виступали джерелами або ключовими вузлами розповсюдження дезінформаційних повідомлень. У межах кампанії «Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії» [20] найбільш активними у поширенні дезінформаційних повідомлень були ресурси Pravda та «Украина.ру». Водночас для кампанії «Дискредитація військовослужбовців України» [21] найбільш залученими джерелами виступали Pravda та «Другая Украина».

У згаданому контексті доречно навести приклад повторного аналізу вже опрацьованих даних із використанням інструменту Claude (Sonnet 4.6) як засобу незалежної верифікації обчислень, виконаних у Gephi. До системи було завантажено JSON-файл із даними двох інформаційних кампаній («Дискредитація військовослужбовців України» та «Дискредитація України на міжнародній арені»). Після завантаження даних моделі було поставлено уніфікований запит, який задавав інтерпретаційні правила (зокрема, трактування платформи як домену) та вимоги до вихідного формату (структурований звіт і рейтинги строго з чотирьох позицій).

Текст запиту до моделі:

“Я надам тобі граф під назвою «Дискредитація військовослужбовців України», що відображає поширення дезінформаційних повідомлень.

Твоя місія – провести комплексний аналітичний розбір і визначити такі характеристики.

Під онлайн-платформами слід розуміти окремі домени. Тобто:

Кожен унікальний домен (наприклад: telegram.org, t.me, facebook.com, vk.com, twitter.com, x.com, конкретні новинні сайти тощо) вважається окремою платформою але Gwara Media, StopFake, VoxUkraine та Детектор медіа не враховувати.

Різні сайти або канали в межах одного домену враховуються як одна платформа.

1. *Платформи з найбільшою кількістю дезінформаційних публікацій*

Визнач платформи, на яких зафіксовано найбільшу кількість дезінформаційних постів. Подай лише топ-2 платформи у вигляді рейтингу (від більшої до меншої кількості).

2. *Частота залучення платформ до інцидентів*

Проаналізуй не лише кількість публікацій, а й кількість різних дезінформаційних інцидентів, у межах яких кожна платформа фігурувала як канал поширення. Визнач платформи, які найчастіше були залучені до різних інформаційних кейсів. Подай лише топ-2 платформи за цим показником у вигляді рейтингу.

3. *Інциденти з найбільшою кількістю залучених платформ*

Визнач дезінформаційні інциденти, у яких було задіяно найбільшу кількість різних онлайн-платформ. Подай лише топ-2 інциденти у порядку спадання кількості залучених платформ.

4. *Інциденти з найбільшим рівнем поширення*

Визнач дезінформаційні інциденти, які характеризувалися найвищим рівнем поширення в мережі (з урахуванням кількості публікацій, врахуй шо у графі не всі посилання повязані напряму з інцидентом). Подай лише топ-2 інциденти.

5. *Спільна участь платформ (ко-участь)*

Проаналізуй, які онлайн-платформи найчастіше фігурують разом у межах одних і тих самих дезінформаційних інцидентів. Подай топ-2 пари платформ (Наприклад: Вконтакте та Telegram, Telegram та X, Facebook та Telegram).

6. *Найбільш впливові канали та сайти*

Подай лише топ-2 Thread Actrors за рівнем впливовості (враховуючи кількість постів які вони поширили).

Формат відповіді:

Чітка структурована аналітична доповідь із підзаголовками, без додаткових пояснень, конкретна відповідь.

У кожному рейтингу – строго 2 позиції (не більше)".

З першої спроби система сформувала звіт відповідно до заданих критеріїв. Нижче наведено результати у скороченому вигляді як дослівні фрагменти відповіді Claude (Sonnet 4.6).

1. Інформаційна кампанія Дестабілізація громадянського суспільства України та формування внутрішньої підтримки війни серед російської аудиторії.

Таблиця 1
Платформи з найбільшою кількістю дезінформаційних публікацій

№ з/п	Платформа	Кількість публікацій
1	t.me (Telegram)	20
2	facebook.com (Facebook)	6

Таблиця 2
Частота залучення платформ до інцидентів

№ з/п	Платформа	Кількість інцидентів
1	t.me (Telegram)	10 із 10
2	facebook.com / ukraina.ru	5 із 10

Таблиця 3
Інциденти з найбільшою кількістю залучених платформ

№ з/п	Інцидент	Кількість платформ
1 (ex aequo)	«Україна закрила доступ ЗМІ до прифронтових областей»	6
1 (ex aequo)	«Під час обстрілу кияни в метро кричали "Зеленський, спускайся до нас"»	6

Таблиця 4
Інциденти з найбільшим рівнем поширення

№ з/п	Інцидент	Кількість публікацій
1	«Під час обстрілу кияни в метро кричали "Зеленський, спускайся до нас"»	7
2 (ex aequo)	«У 2026 році в України закінчаться гроші на зарплати військовим»	6
2 (ex aequo)	«У школах Кривого Рогу карають дітей, чиї батьки-військові самовільно залишили місце служби»	6

Таблиця 5
Спільна участь платформ (ко-участь)

№ з/п	Пара платформ	Кількість спільних інцидентів
1	Facebook + Telegram	5
2	Telegram + Ukraina.ru	5

Таблиця 6
Найбільш впливові Thread Actors

№ з/п	Актор	Тип	Кількість поширених публікацій
1	Украина.ру	Медіагрупа	6
2	Pravda	Медіагрупа	4

2. Інформаційна кампанія "Дискредитація військовосужбовців України"

1. Платформи з найбільшою кількістю дезінформаційних публікацій:

– *t.me (Telegram) 30 публікацій;*
– *vk.com (ВКонтакте) 5 публікацій.*

2. Частота залучення платформ до інцидентів:

– *t.me (Telegram) 10 інцидентів;*
– *vk.com (ВКонтакте) 4 інциденти.*

3. Інциденти з найбільшою кількістю залучених платформ:

– *«Військові 95-ї ОШБр розстріляли трьох людей на Сумщині – Нацполіція»;*
– *t.me, vk.com, dzen.ru, kp.ru, ren.tv, theotherukraine.info 6 платформ;*
– *«Нетверезий військовий 80-ї ОДШБр на смерть збив 17-річну дівчину» t.me, vk.com, ukrgm.com, mk.ru 4 платформи.*

4. Інциденти з найбільшим рівнем поширення:

– *«У ЗСУ служить оператором БПЛА людина з синдромом Дауна» 10 публікацій;*
– *«Військові 95-ї ОШБр розстріляли трьох людей на Сумщині – Нацполіція» 6 публікацій.*

5. Спільна участь платформ (ко-участь):
– *Telegram & ВКонтакте 4 інциденти;*
– *Telegram & theotherukraine.info 2 інциденти.*

6. Найбільш впливові канали (Threat Actors):
– *«Другая Украина» 6 постів;*
– *Pravda 5 постів".*

За результатами зіставлення відповідей, отриманих у Gephi, з аналітичними підрахунками, виконаними Claude (Sonnet 4.6), встановлено, що переважна більшість показників і ранжувань збігається або відтворюється на рівні тієї самої загальної структури. Виявлені поодинокі розбіжності доцільно трактувати як наслідок відмінностей у процедурі обробки даних: штучний інтелект міг інакше інтерпретувати окремі елементи запиту (зокрема правила нормалізації доменів, критерії включення "непрямих" URL через зв'язки derived-from тощо) і, відповідно, застосувати альтернативну обробку метрик. Це могло призвести до незначних змін у підрахунках або перестановок на межі рейтингових позицій без суттєвого впливу на загальні висновки. Водночас узгодженість результатів у цілому дозволяє зробити висновок про коректність і відтворюваність виконаних процедур аналізу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, для ефективного дослідження, класифікації та прогнозування інформаційних атак необхідна уніфікована система опису їхньої структури та взаємозв'язків. Таку функцію виконує система DISARM, яка визначається як концептуальна основа, що забезпечує систематизацію тактик, технік і процедур (TTPs), характерних для дезінформаційних операцій. ЇЇ інтеграція зі стандартом STIX та платформою OpenCTI створює цілісну методологічну основу дослідження, яка поєднує концептуальну класифікацію дезінформаційних процесів, формалізоване подання даних та інструментальні засоби аналітичної обробки.

Застосування графового методу для побудови структурних графів дезінформаційних кампаній дозволяє побудувати архітектуру, топологію та динаміку поширення дезінформації в інформаційному просторі, а STIX Visualizer надає можливість перегляду графів онлайн. Знання того, як саме збудований граф (наприклад, чи це централізована «зірка», чи децентралізована мережа ізольованих кластерів), визначає стратегію комунікації у відповідь. Також з'являється можливість визначити найбільш поширені канали та вебресурси, які систематично виступали джерелами або ключовими вузлами розповсюдження дезінформаційних повідомлень. Це переводить протидію загрозам із площини «гасіння пожеж» у площину стратегічного керування інцидентами та проактивного захисту інформаційного простору через широку публікацію виявленої структури і каналів поширення дезінформаційних кампаній.

Програмний інструмент Gephi є ефективним та методологічно доречним інструментом для опрацювання великих масивів даних, візуалізації та аналізу складних мереж і графів. Саме Gephi переводить аналіз із площини вивчення змісту фейків у площину дослідження архітектури їх поширення. Він робить видимими приховані мережеві зв'язки, перетворюючи хаотичні масиви цифрових логів та метаданих на чіткі структурні карти. Порівняно із застосуванням систем на базі штучного інтелекту Gephi дає візуальне представлення результатів мережевого аналізу, що дозволяє досліднику більш зручно намічати шляхи подальшого дослідження та виключає галюцинаційні помилки, що можуть бути допущені інструментами на базі штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bârgăoanu, A., & Pană, M. (2024). Cyber influence defense: Applying the DISARM framework to a cognitive hacking case from the Romanian digital space. Applied Cybersecurity & Internet Governance, 3(1), 91-121. https://doi.org/10.60097/ACIG/190196
2. Prysiazhniuk, M. (n.d.). DISARM framework – "Mendeleev's table" of information operations and campaigns. ATHENA. https://project-athena.eu/disarm-framework-mendeleevs-table-of-information-operations-and-campaigns/
3. González, F. S., Pastor-Galindo, J., & Ruipérez-Valiente, J. A. (2025). Toward interoperable representation and sharing of disinformation incidents in cyber threat intelligence (arXiv:2502.20997). arXiv. https://doi.org/10.48550/arXiv.2502.20997

4. Niven, T. S., & Li, C.-T. (2026). Automatic tagging of foreign information manipulation and interference incidents with DISARM tactics, techniques, and procedures. IEEE Access, 14, 6364-6377. https://ieeexplore.ieee.org/document/11343758
5. Tseng, K., Toledano, J. C., & Dukach, B. De C. Yu. (2026). An agentic operationalization of DISARM for FIMI investigation on social media (arXiv:2601.15109). arXiv. https://arxiv.org/abs/2601.15109
6. Antagonistic information threats: Lessons from Ukraine. (2026, March 16). Policy Brief. https://freepolicybriefs.org/2026/03/16/antagonistic-information-threats/
7. Nosov, V., & Stetsyk, R. (2026). Cases of disinformation about Ukraine detected in the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19355384
8. Nosov, V., & Stetsyk, R. (2026). Systematised results of the analysis of the campaign "Destabilisation of Ukrainian civil society and the formation of internal support for the war among Russian audiences" for the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19355791
9. Nosov, V., & Stetsyk, R. (2026). Systematised results of the analysis of the campaign "Discrediting Ukrainian military personnel" for the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19356201
10. Nosov, V., & Stetsyk, R. (2026). STIX file of the disinformation campaign "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" for the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19906835
11. Nosov, V., & Stetsyk, R. (2026). STIX file of the disinformation campaign "Discrediting Ukrainian military personnel" for the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19906470
12. Stetsyk, R., & Nosov, V. (2026). Distribution of disinformation posts across online platforms within the graph dataset "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19907720
13. Stetsyk, R., & Nosov, V. (2026). Distribution of disinformation posts across online platforms within the graph dataset "Discrediting Ukrainian military personnel" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19664075
14. Stetsyk, R., & Nosov, V. (2026). Frequency of involvement of online platforms in the dissemination of disinformation by the number of incidents within the graph "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19896612
15. Stetsyk, R., & Nosov, V. (2026). Frequency of involvement of online platforms in the dissemination of disinformation by the number of incidents within the graph "Discrediting Ukrainian military personnel" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19886629
16. Stetsyk, R., & Nosov, V. (2026). Most disseminated disinformation incidents and their primary sources (URL) within the graph "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19898023
17. Stetsyk, R., & Nosov, V. (2026). Most disseminated disinformation incidents and their primary sources (URL) within the graph "Discrediting Ukrainian military personnel" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19888831
18. Stetsyk, R., & Nosov, V. (2026). Shared participation of online platforms in disinformation incidents within the graph "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19898257
19. Stetsyk, R., & Nosov, V. (2026). Shared participation of online platforms in disinformation incidents within the graph "Discrediting Ukraine in the international arena" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19894895
20. Stetsyk, S., & Nosov, V. (2026). Most common disinformation channels and websites within the graph "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19905646
21. Stetsyk, S., & Nosov, V. (2026). Most common disinformation channels and websites within the graph "Discrediting Ukrainian military personnel" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19895231

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Vitalii Nosov
Candidate of Technical Sciences, Associate Professor, Professor of the Department of Combating Cybercrime
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID:0000-0002-7848-6448
vitnos.g@gmail.com

Oleksandr Manzhai
Candidate of Juridical Sciences, Professor, Head of the Department Combating Cybercrime
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID:0000-0001-5435-5921
sofist@ukr.net

Svitlana Luchyk
Doctor of Economic Sciences, Professor, Professor of the Department of Information Systems and Technologies
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID:0000-0003-0757-1140
luchiksvitlana@gmail.com

Roman Stetsyk
Cadet of Educational and Scientific Institute No. 4
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID:0009-0009-1263-184X
romanstetsyk06@gmail.com

Sadovyi Kostiantyn
Candidate of Technical Sciences, Associate Professor, Head of the department of radiotechnical troops armament
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID:0000-0003-2703-9696
971sadovyi@gmail.com

DISINFORMATION CAMPAIGNS IN UKRAINE: A STRUCTURING METHODOLOGY BASED ON THE DISARM FRAMEWORK AND THE OPENCTI PLATFORM

Abstract. With the onset of full-scale Russian aggression in Ukraine, the enemy's aggressive use of the digital environment has evolved from isolated propaganda acts to the orchestration of powerful disinformation campaigns. This necessitates the development and implementation of standardized data structuring methodologies based on threat intelligence tools, specifically the DISARM framework and the OpenCTI platform. The aim of this article is to develop and scientifically substantiate a methodology for structuring disinformation campaigns through the lens of DISARM tactics and techniques, utilizing the knowledge graphs of the OpenCTI platform, based on an analysis of experimental data regarding the internal destabilization of society and the discrediting of Ukrainian military personnel.

The study utilized: general scientific theoretical methods, such as systems analysis and the abstract-logical method, to make theoretical generalizations and formulate conclusions and recommendations regarding the structuring of disinformation campaigns; the clustering method – to identify the most powerful disinformation campaigns in the first half of 2025; and the graph method – to visualize and analyze the structure of the network of disinformation incidents.

The application of graph theory to construct structural graphs of disinformation campaigns enabled the authors to map the architecture, topology, and dynamics of disinformation dissemination in Ukraine's information space, while STIX Visualizer provided the ability to view the constructed graphs online. For the identified disinformation campaigns, the most common channels and web resources that systematically served as sources or key nodes for the dissemination of disinformation messages were identified. The use of the Gephi software tool made it possible to visualize the results of the graph analysis and investigate the architectures of disinformation message dissemination. Compared to the use of AI-based systems, Gephi allows researchers to more conveniently map out paths for further research and eliminates the hallucination errors that can be made by AI-based tools.

Keywords: disinformation campaign; methodology; structuring; framework; open platform; graph method; big data; visualization; artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bârgăoanu, A., & Pană, M. (2024). Cyber influence defense: Applying the DISARM framework to a cognitive hacking case from the Romanian digital space. Applied Cybersecurity & Internet Governance, 3(1), 91-121. https://doi.org/10.60097/ACIG/190196
2. Prysiazhniuk, M. (n.d.). DISARM framework – "Mendeleev's table" of information operations and campaigns. ATHENA. https://project-athena.eu/disarm-framework-mendeleevs-table-of-information-operations-and-campaigns/
3. González, F. S., Pastor-Galindo, J., & Ruipérez-Valiente, J. A. (2025). Toward interoperable representation and sharing of disinformation incidents in cyber threat intelligence (arXiv:2502.20997). arXiv. https://doi.org/10.48550/arXiv.2502.20997
4. Niven, T. S., & Li, C.-T. (2026). Automatic tagging of foreign information manipulation and interference incidents with DISARM tactics, techniques, and procedures. IEEE Access, 14, 6364-6377. https://ieeexplore.ieee.org/document/11343758
5. Tseng, K., Toledano, J. C., & Dukach, B. De C. Yu. (2026). An agentic operationalization of DISARM for FIMI investigation on social media (arXiv:2601.15109). arXiv. https://arxiv.org/abs/2601.15109
6. Antagonistic information threats: Lessons from Ukraine. (2026, March 16). Policy Brief. https://freepolicybriefs.org/2026/03/16/antagonistic-information-threats/
7. Nosov, V., & Stetsyk, R. (2026). Cases of disinformation about Ukraine detected in the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19355384
8. Nosov, V., & Stetsyk, R. (2026). Systematised results of the analysis of the campaign "Destabilisation of Ukrainian civil society and the formation of internal support for the war among Russian audiences" for the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19355791
9. Nosov, V., & Stetsyk, R. (2026). Systematised results of the analysis of the campaign "Discrediting Ukrainian military personnel" for the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19356201
10. Nosov, V., & Stetsyk, R. (2026). STIX file of the disinformation campaign "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" for the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19906835
11. Nosov, V., & Stetsyk, R. (2026). STIX file of the disinformation campaign "Discrediting Ukrainian military personnel" for the second half of 2025 [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19906470
12. Stetsyk, R., & Nosov, V. (2026). Distribution of disinformation posts across online platforms within the graph dataset "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19907720
13. Stetsyk, R., & Nosov, V. (2026). Distribution of disinformation posts across online platforms within the graph dataset "Discrediting Ukrainian military personnel" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19664075
14. Stetsyk, R., & Nosov, V. (2026). Frequency of involvement of online platforms in the dissemination of disinformation by the number of incidents within the graph "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19896612
15. Stetsyk, R., & Nosov, V. (2026). Frequency of involvement of online platforms in the dissemination of disinformation by the number of incidents within the graph "Discrediting Ukrainian military personnel" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19886629
16. Stetsyk, R., & Nosov, V. (2026). Most disseminated disinformation incidents and their primary sources (URL) within the graph "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19898023
17. Stetsyk, R., & Nosov, V. (2026). Most disseminated disinformation incidents and their primary sources (URL) within the graph "Discrediting Ukrainian military personnel" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19888831
18. Stetsyk, R., & Nosov, V. (2026). Shared participation of online platforms in disinformation incidents within the graph "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19898257

19. Stetsyk, R., & Nosov, V. (2026). Shared participation of online platforms in disinformation incidents within the graph "Discrediting Ukraine in the international arena" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19894895
20. Stetsyk, S., & Nosov, V. (2026). Most common disinformation channels and websites within the graph "Destabilization of Ukrainian civil society and the development of internal support for the war among the Russian audience" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19905646
21. Stetsyk, S., & Nosov, V. (2026). Most common disinformation channels and websites within the graph "Discrediting Ukrainian military personnel" (second half of 2025) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.19895231

Отримано редакцією журналу / Received: 24.01.26
Прорецензовано / Revised: 06.02.26
Схвалено до друку / Accepted: 24.09.26