КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1178
УДК 343.9:004.056:004.738.5

Габорець Ольга Андріївна
доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки
Донецький державний університет внутрішніх справ, Кропивницький, Україна
ORCID: 0000-0001-7791-6795
olga-gaborets@ukr.net

АНАЛІЗ ДЕСТРУКТИВНИХ ІНФОРМАЦІЙНИХ НАРАТИВІВ У ЦИФРОВОМУ ПРОСТОРІ ЯК СКЛАДОВА КРИМІНАЛЬНОГО АНАЛІЗУ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Анотація. У статті досліджено деструктивні інформаційні наративи у цифровому просторі як самостійний об’єкт кримінального аналізу інформаційних загроз. Обґрунтовано, що в умовах цифровізації суспільних відносин, зростання ролі платформених комунікацій та трансформації сучасних безпекових викликів інформаційний простір набуває ознак середовища, у якому реалізуються системні маніпулятивні впливи, дезінформаційні кампанії та інформаційно-психологічні операції, здатні впливати на стан громадської безпеки, рівень довіри до державних інституцій і стійкість суспільних процесів.

Визначено, що деструктивний інформаційний наратив доцільно розглядати не лише як комунікативний або пропагандистський феномен, а й як аналітичну категорію, що характеризується змістовою цілісністю, повторюваністю, адаптивністю до актуального інформаційного контексту, багатоканальністю поширення та потенціалом формування негативних когнітивних, емоційних і поведінкових ефектів. Такий підхід дає змогу інтегрувати дослідження деструктивних наративів у систему кримінального аналізу, орієнтованого на виявлення патернів, тенденцій, джерел, механізмів поширення та ризикових наслідків інформаційного впливу. Теоретико-методологічною основою такого підходу визначено концепцію Intelligence-Led Policing, яка передбачає проактивний, превентивний і ризик-орієнтований характер правоохоронної діяльності, заснованої на використанні аналітичної розвідки, достовірних даних та аналітичних продуктів для підтримки управлінських рішень.

У результаті опрацювання аналітичних матеріалів встановлено, що в цифровому просторі системно функціонують кілька основних груп деструктивних інформаційних наративів, зокрема наративи дискредитації державного управління, дестабілізації через поширення страху та невизначеності, підриву міжнародної суб’єктності України, маніпуляцій навколо мобілізаційних і безпекових тем, а також технологічно посилені наративи з використанням AI-згенерованого контенту. Доведено, що зазначені наративи мають структурований характер, відзначаються повторюваністю, мережевою реплікативністю та високим потенціалом впливу на інформаційне середовище й суспільні настрої.

Обґрунтовано, що кримінальний аналіз деструктивних інформаційних наративів має здійснюватися із застосуванням комплексу взаємодоповнювальних методів, зокрема контент-аналізу, аналізу інформаційних потоків, OSINT-аналізу, аналізу соціальних мереж, а також темпорального й ризик-орієнтованого аналізу. Використання такого інструментарію дає змогу не лише фіксувати зміст окремих інформаційних повідомлень, а й виявляти закономірності поширення наративів, їхні мережеві зв’язки, часову динаміку активізації та потенційні ризики для безпекового середовища.

Зроблено висновок, що деструктивні інформаційні наративи у цифровому просторі слід розглядати як повноцінний об’єкт кримінального аналізу інформаційних загроз. Їх системне виявлення, структуризація, класифікація та аналітичне оцінювання є важливою умовою підвищення ефективності правоохоронної діяльності у сфері запобігання та протидії сучасним інформаційним загрозам.

Ключові слова: кримінальний аналіз; інформаційні загрози; деструктивні інформаційні наративи; цифровий простір; дезінформація; аналітична розвідка; OSINT; аналіз соціальних мереж; Intelligence-Led Policing.

ВСТУП

Постановка проблеми. Сучасний етап розвитку інформаційного суспільства характеризується інтенсивною цифровізацією комунікаційних процесів, що зумовлює зростання ролі інформаційних потоків у формуванні суспільної думки, політичних орієнтацій та поведінкових моделей. Розвиток соціальних мереж, цифрових медіа та платформених сервісів суттєво підвищив швидкість і масштаб поширення інформації, трансформувавши інформаційний простір у середовище активного впливу на соціальні процеси.

Водночас зазначені трансформації створили сприятливі умови для системного поширення деструктивних інформаційних впливів, зокрема у формі стійких наративних конструкцій, спрямованих на викривлення сприйняття соціально значущих подій, підрив довіри до державних інституцій та дестабілізацію суспільних процесів. Такі наративи функціонують як відтворювані смислові моделі, здатні адаптуватися до змін інформаційного контексту та поширюватися через різні сегменти цифрового середовища.

Особливої актуальності ця проблематика набуває в умовах гібридного протистояння та воєнного стану, коли інформаційний вплив використовується як інструмент досягнення стратегічних цілей. У цифровому просторі системно циркулюють наративи, спрямовані на дискредитацію державного управління, делегітимацію української державності, маніпуляції у сфері мобілізаційних процесів та формування кризових очікувань у суспільстві. Додатковим фактором ускладнення є використання синтетичного медіаконтенту, зокрема AI-згенерованих матеріалів, що підвищують переконливість дезінформаційних повідомлень. За таких умов деструктивні інформаційні наративи доцільно розглядати як специфічний об’єкт аналітичного дослідження, оскільки вони характеризуються структурованістю, повторюваністю та потенційним впливом на безпекове середовище. Це обумовлює необхідність їх інтеграції у систему кримінального аналізу інформаційних загроз, який орієнтований на виявлення патернів, тенденцій та факторів ризику. Сучасні підходи до правоохоронної діяльності, зокрема концепція Intelligence-Led Policing, передбачають проактивний і ризик-орієнтований характер аналізу, спрямованого на попередження загроз. У цьому контексті дослідження деструктивних інформаційних наративів як відтворюваних інформаційних патернів створює підґрунтя для підвищення ефективності аналітичної діяльності у сфері забезпечення громадської безпеки.

Отже, актуальність дослідження зумовлена необхідністю теоретичного обґрунтування деструктивних інформаційних наративів як об’єкта кримінального аналізу інформаційних загроз та визначення підходів до їх системного виявлення й оцінювання у цифровому середовищі.

Аналіз останніх досліджень і публікацій. Проблематика інформаційних загроз та деструктивних інформаційних впливів у цифровому середовищі в останні роки стала предметом активних наукових досліджень у межах різних галузей знань, зокрема інформаційного права, кримінології, кібербезпеки, медіакомунікацій та безпекових студій. Це зумовлено як стрімким розвитком інформаційно-комунікаційних технологій, так і трансформацією сучасних загроз національній безпеці, які дедалі частіше реалізуються через цифрові платформи, соціальні мережі та інші канали електронної комунікації.

У науковій літературі значну увагу приділено дослідженню сутності та механізмів деструктивного інформаційного впливу. Зокрема, Р. Черниш розглядає деструктивний інформаційний вплив як елемент інформаційної війни та наголошує, що в умовах зовнішньої збройної агресії він становить реальну загрозу державному суверенітету й територіальній цілісності України. Автор підкреслює, що деструктивний інформаційний вплив спрямовується на тиск на державні інституції, поляризацію суспільства, підрив довіри до органів влади, Збройних Сил України, правоохоронних і спеціальних органів, а також може використовуватися для дестабілізації суспільно-політичної ситуації та впливу на громадську думку [1].

Значну увагу дослідженню маніпулятивних інформаційних впливів у цифровому медіасередовищі приділяє В. Шевченко. У своїй роботі авторка аналізує різновиди маніпуляцій в онлайн-медіа та соціальних мережах і підкреслює, що маніпуляція є цілеспрямованим психологічним та інформаційним впливом на свідомість аудиторії з метою формування необхідних оцінок і моделей поведінки. Дослідниця виокремлює такі форми маніпулятивної інформації, як дезінформація, малінформація, місінформація, пропаганда та фейки, які активно використовуються для впливу на суспільну думку, поширення викривлених наративів і формування емоційно забарвленого сприйняття подій у цифровому просторі [5].

У сучасних дослідженнях цифрового середовища значна увага приділяється також наративним формам представлення інформації. Зокрема, C. Lambert та співавтори зазначають, що цифрове сторітелінг (digital storytelling) є наративною практикою, яка дозволяє транслювати індивідуальний

досвід за допомогою цифрових медіа та формувати нові інтерпретаційні рамки сприйняття соціальних явищ. Використання цифрових історій створює можливість впливати на суспільні уявлення та формувати альтернативні інтерпретації подій у цифровому просторі [7].

Актуальність дослідження деструктивних інформаційних наративів підтверджується також сучасними аналітичними звітами у сфері безпеки. Зокрема, у звіті Homeland Threat Assessment 2025 Міністерства внутрішньої безпеки США зазначається, що державні актори активно використовують дезінформацію, соціальні мережі, мережі ботів та інші цифрові інструменти для поширення маніпулятивного контенту, підриву довіри до державних інституцій та загострення суспільних протиріч [6]. Як зазначає М. Баран, забезпечення інформаційної безпеки в Україні має комплексний адміністративно-правовий характер і спрямоване на захист інформації, а також особи, суспільства і держави від деструктивного інформаційного впливу. Важливим елементом цього процесу є діяльність органів публічної влади щодо регулювання інформаційних відносин та запобігання поширенню протиправної інформації [2].

У контексті трансформації безпекового середовища значну увагу приділяють дослідженням ролі правоохоронних органів у протидії сучасним інформаційним загрозам. Зокрема, В. Василенко у своїх працях підкреслює, що цифрова трансформація правоохоронних органів є необхідною умовою ефективної протидії новим формам загроз, які виникають у цифровому середовищі. Автор зазначає, що сучасні інформаційні загрози дедалі частіше мають нематеріальний характер і реалізуються через електронні комунікаційні канали, соціальні мережі та цифрові платформи, що потребує розвитку аналітичних та інформаційно-технологічних можливостей правоохоронних органів [3-4].

Крім того, у сучасних дослідженнях підкреслюється важливість формування інформаційної культури та цифрової грамотності як елементів забезпечення стійкості суспільства до інформаційних загроз. Зокрема, у роботах, присвячених питанням цифрової безпеки та взаємодії громад із правоохоронними органами, наголошується на необхідності формування партнерських моделей співпраці між державними інституціями та громадянським суспільством у сфері моніторингу інформаційного простору, виявлення дезінформаційних кампаній та протидії поширенню маніпулятивного контенту.

Разом із тим аналіз наукових джерел [1-7] свідчить, що попри значну кількість досліджень, присвячених проблемам дезінформації, інформаційно-психологічних операцій та забезпечення інформаційної безпеки, питання дослідження деструктивних інформаційних наративів у цифровому просторі саме у контексті кримінального аналізу інформаційних загроз залишається недостатньо розробленим. У більшості наукових праць деструктивні інформаційні наративи розглядаються як явище інформаційної війни або елемент медійної комунікації, тоді як їх системне дослідження у межах кримінального аналізу, спрямованого на виявлення закономірностей поширення, джерел формування та потенційних ризиків для безпеки, потребує подальшого наукового обґрунтування.

Отже, наявні наукові дослідження створюють теоретичне підґрунтя для осмислення деструктивних інформаційних впливів у цифровому просторі, однак проблема дослідження деструктивних інформаційних наративів як об’єкта кримінального аналізу інформаційних загроз потребує подальшого наукового опрацювання, що і зумовлює актуальність цієї статті.

Метою статті є теоретичне обґрунтування деструктивних інформаційних наративів у цифровому просторі як специфічного об’єкта кримінального аналізу інформаційних загроз, а також дослідження закономірностей їх формування, поширення та впливу на безпекове середовище в умовах цифрової трансформації суспільства.

Наукова новизна дослідження полягає в обґрунтуванні деструктивних інформаційних наративів у цифровому просторі як самостійного об’єкта кримінального аналізу інформаційних загроз. У роботі уточнено наукові підходи до розуміння деструктивного інформаційного наративу шляхом визначення його структурних характеристик, механізмів формування та закономірностей поширення у цифровому середовищі. Обґрунтовано доцільність застосування кримінально-аналітичного підходу до дослідження деструктивних інформаційних наративів, що передбачає їх розгляд як повторюваних інформаційних патернів, аналіз структури поширення, тематичної стабільності та потенційного впливу на безпекове середовище.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасна цифрова трансформація суспільства істотно змінила не лише способи комунікації, а й саму природу інформаційних загроз. Якщо у традиційному інформаційному середовищі деструктивний вплив здебільшого мав лінійний характер і реалізовувався через відносно обмежене коло засобів масової інформації, то в цифровому просторі він набув ознак багатоканальності, високої швидкості

масштабування, адаптивності та мережевої реплікативності. Зазначені характеристики створюють умови для системного поширення деструктивних інформаційних наративів, які вже трансформуються у складний аналітичний об'єкт, що потребує дослідження у межах кримінального аналізу. У сучасних умовах вони виступають специфічною формою інформаційного впливу, що має власну структуру, динаміку поширення, набір тематичних домінант, цільові аудиторії та потенціал до дестабілізаційного впливу на громадську безпеку.

У теоретичному плані деструктивний інформаційний наратив доцільно розуміти як системно відтворювану смислову конструкцію, що поєднує серію взаємопов'язаних повідомлень, інтерпретацій, оціночних суджень і візуально-текстових маркерів, спрямованих на формування у цільової аудиторії певного когнітивного шаблону сприйняття соціально значущих подій. Його принципова відмінність від окремого фейкового повідомлення полягає в тому, що наратив не існує як ізольований інформаційний акт. Він функціонує як більш стійка, повторювана й адаптивна модель пояснення дійсності, здатна відтворюватися у різних форматах і на різних цифрових платформах. Саме тому наратив має значно вищий потенціал впливу, ніж одноразова дезінформаційна публікація, оскільки працює не лише на рівні інформування чи дезінформування, а передусім на рівні тривалого конструювання способу мислення, інтерпретації подій та оцінювання діяльності інституцій [5].

Такий підхід узгоджується з напрацьованими у статті теоретичними положеннями, відповідно до яких деструктивні інформаційні наративи характеризуються змістовою цілісністю, повторюваністю, адаптивністю до динаміки інформаційного середовища, багатоканальністю поширення та потенціалом формування негативних когнітивних, емоційних і поведінкових ефектів. У цьому контексті деструктивний інформаційний наратив доцільно розглядати як аналітичну категорію, а не лише як інформаційний продукт, оскільки саме аналітичний підхід дає змогу виявляти його внутрішню структуру, джерела формування, моделі поширення та потенційні ризикові наслідки для безпекового середовища [1].

У прикладному вимірі це означає, що деструктивні наративи у цифровому просторі мають бути включені до предметного поля кримінального аналізу інформаційних загроз. Такий висновок ґрунтується на сучасному розумінні кримінального аналізу, що вже не обмежується дослідженням лише факту вчиненого кримінального правопорушення, а охоплює виявлення тенденцій, патернів, факторів ризику, механізмів формування загроз і прогнозування їхнього розвитку. У межах концепції Intelligence-Led Policing кримінальний аналіз виконує проактивну функцію, оскільки орієнтований на раннє виявлення загроз, аналітичну підтримку управлінських рішень, встановлення закономірностей поширення ризиків та визначення пріоритетних напрямів реагування. Саме тому деструктивні інформаційні наративи, що характеризуються системністю, повторюваністю та потенційним впливом на безпекове середовище, можуть розглядатися як самостійний об'єкт кримінального аналізу інформаційних загроз [3-4].

Формування деструктивних інформаційних наративів у цифровому просторі є складним багаторівневим процесом, що поєднує комунікаційні, психологічні та технологічні компоненти. На відміну від поодиноких інформаційних повідомлень або ізольованих дезінформаційних публікацій, деструктивні наративи створюються як системні смислові конструкції, які формуються, підтримуються та поширюються в межах певної інформаційної стратегії [5]. У сучасному цифровому середовищі процес формування деструктивного наративу зазвичай відбувається у кілька взаємопов'язаних етапів.

Першим етапом є конструювання смислового ядра наративу, тобто формування ключової інтерпретаційної тези, яка визначає загальну логіку пояснення певної події або процесу. Така теза, як правило, формулюється у вигляді узагальненого повідомлення, здатного легко відтворюватися у різних інформаційних контекстах.

Другим етапом є інтерпретаційне розширення наративу, під час якого базова теза наповнюється додатковими аргументами, прикладами та інформаційними повідомленнями. У цей період створюються різні варіації повідомлень, які підтримують основну смислову модель і адаптуються до змін інформаційного середовища.

Третім етапом є масштабування наративу в цифровому середовищі, що здійснюється через соціальні мережі, онлайн-медіа, месенджери та інші цифрові платформи. Завдяки мережевій природі цифрових комунікацій такі повідомлення можуть швидко поширюватися серед значної кількості користувачів.

Четвертим етапом є адаптація наративу до інформаційного контексту, коли зміст окремих повідомлень змінюється залежно від актуальних подій, однак базова смислова конструкція залишається незмінною.

Не менш важливим є й те, що деструктивні наративи у цифровому просторі мають виразно емпірично фіксовану структуру. Їх можна виявити через повторюваність ключових тез, стабільність тематичних домінант, наявність однакових інтерпретаційних схем, синхронізацію появи схожих

повідомлень у різних сегментах цифрового простору, а також через використання подібних емоційних тригерів, візуальних елементів і риторичних засобів. Це означає, що такий наратив піддається не лише якісному опису, а й кількісному вимірюванню та статистичній інтерпретації, що особливо важливо для кримінального аналізу як прикладної аналітичної діяльності.

У цьому зв'язку особливо показовими є дані інформаційно-аналітичних матеріалів Центру протидії дезінформації (ЦПД), які можуть бути використані як емпірична база для дослідження деструктивних інформаційних наративів у цифровому просторі за кількома часовими зрізами, зокрема за періоди 20-26 вересня 2025 року, 6-12 грудня 2025 року та 28 лютого - 6 березня 2026 року [8-10]. Використання саме такого підходу дає змогу перейти від фрагментарного опису окремих інформаційних інцидентів до виявлення стійких закономірностей функціонування деструктивних наративів, їх тематичної стабільності, інтенсивності поширення та адаптації до поточного безпекового контексту.

Порівняльний аналіз зазначених періодів свідчить про збереження стабільно високого рівня інформаційної активності у досліджуваному сегменті цифрового простору. Так, у період 20-26 вересня 2025 року було зафіксовано 136 інформаційних загроз, у період 6-12 грудня 2025 року – 124, а у період 28 лютого – 6 березня 2026 року – 128 [8-10]. Уже сама ця динаміка дає підстави стверджувати, що деструктивний інформаційний вплив не має епізодичного характеру, а функціонує як системне й відносно стабільне явище, здатне відтворюватися у різних часових інтервалах із незначними коливаннями інтенсивності. При цьому зміна абсолютних показників не свідчить про зникнення загрози, а, навпаки, демонструє її постійну присутність у цифровому середовищі та здатність адаптуватися до актуального інформаційного порядку денного.

Не менш важливим є порівняння структури виявлених загроз. У вересневому періоді 2025 року маніпуляції становили 47 %, чутливі інформаційні теми – 21 %, дезінформація – 14 %, інші види загроз – 18 %. У грудневому періоді 2025 року частка маніпуляцій навіть зросла до 50 %, чутливих тем – до 26 %, тоді як дезінформація залишилася на рівні 14 %, а інші види загроз зменшилися до 11 %. Натомість у період 28 лютого – 6 березня 2026 року структура змінилася в бік ще більш вираженого домінування маніпулятивного контенту: його частка становила 60 %, чутливих інформаційних тем – 19 %, дезінформації – 12 %, інших загроз – 8 %. Така динаміка дозволяє зробити принципово важливий висновок: у сучасному цифровому просторі переважає не стільки відверта фальсифікація фактів, скільки маніпулятивне конструювання смислів, тобто технологічно складніші форми інформаційного впливу, спрямовані на поступове зміщення інтерпретаційних рамок сприйняття подій.

Кількісний аналіз ключових деструктивних наративів також виявляє стійке тематичне ядро, яке зберігається в різні часові періоди. У період 20-26 вересня 2025 року домінували наративи «українська влада некомпетентна» – 9 випадків, «Україна примусово мобілізує всіх підряд» – 6, «Україна – держава-терорист» – 6, «Захід проводить агресивну політику відносно росії» – 6, «влада бреше українському суспільству» – 5, а також «українці – нацисти» та «Україна – маріонетка США / НАТО» – по 4. У період 6-12 грудня 2025 року тематичне ядро дещо модифікується, але залишається концептуально близьким: найбільш поширеними стають наративи «Україна – корумпована держава» – 11, «Захід – політично слабкий» – 9, «українська влада некомпетентна» – 8, «на Україну чекає енергетична криза» – 8, «Україна примусово мобілізує всіх підряд» – 7, «Україна має йти на переговори» – 7, «українська армія слабка / некомпетентна» – 7, «Захід проводить агресивну політику відносно росії» – 7. У період 28 лютого – 6 березня 2026 року знову зберігається домінування наративу «українська влада некомпетентна» – 12 випадків, а також активізуються наративи «Україна шантажує Захід» – 8, «Україна – маріонетка США / НАТО» – 7, «Україну чекає енергетична криза» – 6, «Захід зрадив Україну» – 6, «Україна примусово мобілізує всіх підряд» – 6. Отже, попри зміну формулювань і тематичних акцентів, у всі три періоди зберігаються кілька домінантних змістових осей: дискредитація державного управління, делегітимація української державності, маніпуляції навколо мобілізаційних процесів, формування кризових очікувань і підрив міжнародної підтримки України.

Принципово важливим є те, що зазначені наративи не лише повторюються, а й адаптуються до конкретного безпекового контексту. У вересні 2025 року помітним є акцент на дискредитації влади, мобілізаційних процесів і формуванні образу України як джерела загрози. У грудні 2025 року на перший план виходять теми можливих переговорів, «критичної» ситуації для України, корумпованості держави та слабкості Заходу. У період кінця лютого – початку березня 2026 року посилюються наративи, пов'язані з енергетичною кризою, нібито «втомою Заходу» від України та спробами перекласти відповідальність за продовження війни на українську сторону. Така динаміка свідчить, що деструктивні інформаційні наративи функціонують як гнучкі смислові конструкції, здатні змінювати конкретні тематичні маркери залежно від подійного фону, але при цьому зберігати незмінним своє стратегічне призначення – підрив довіри, посилення тривожності, стимулювання поляризації та делегітимацію державних і міжнародних інституцій.

Окремий аналітичний інтерес становить сегментація деструктивних впливів залежно від інформаційного простору. У матеріалах ЦПД за вересень і грудень 2025 року чітко виокремлено український, міжнародний та російський інформаційні сегменти. В українському сегменті домінують наративи, спрямовані на дискредитацію діяльності державних органів, підрив довіри до мобілізаційних заходів, поширення тез про енергетичний колапс і кризовий стан на фронті. У міжнародному сегменті переважають повідомлення, покликані сформувати уявлення про небажання союзників підтримувати Україну, необхідність територіальних поступок, неефективність українського керівництва та безперспективність подальшого спротиву. У російському сегменті найбільш агресивно відтворюються наративи, пов'язані з дискредитацією України як суб'єкта міжнародних відносин, виправданням агресії та поширенням дезінформації про нібито злочини української сторони. Така сегментація підтверджує, що йдеться не про спонтанний інформаційний шум, а про координовану багаторівневу систему інформаційного впливу, яка адаптується до різних аудиторій та використовує різні аргументаційні моделі залежно від очікуваного ефекту.

У кримінально-аналітичному сенсі наведені дані дають підстави розглядати деструктивні інформаційні наративи як стійкі інформаційні патерни, що мають чітко фіксовані кількісні та якісні характеристики. Їх повторюваність у різні часові періоди, відносна стабільність тематичного ядра, адаптивність до змін інформаційного контексту, а також сегментованість за цільовими аудиторіями свідчать про те, що деструктивні наративи можуть і повинні бути предметом системного кримінального аналізу. Вони підлягають не лише описовій фіксації, а й класифікації, темпоральному аналізу, оцінці інтенсивності поширення, виявленню мережевих зв'язків та прогнозуванню потенційного впливу на безпекове середовище. Саме тому емпіричне опрацювання трьох часових зрізів підтверджує, що деструктивні інформаційні наративи у цифровому просторі є не епізодичним комунікативним явищем, а повноцінним об'єктом кримінального аналізу інформаційних загроз.

З метою узагальнення отриманих результатів та систематизації основних груп деструктивних інформаційних наративів доцільно представити їх типологію у вигляді узагальнюючої таблиці (Табл. 1).

Таблиця 1

Типологія деструктивних інформаційних наративів у цифровому просторі

Тип деструктивного наративу	Основна змістова теза	Ціль інформаційного впливу
Делегітимаційні наративи	Українська влада є некомпетентною, корумпованою або неспроможною ефективно керувати державою	Підрив довіри до державних інституцій, дискредитація державного управління
Дестабілізаційні наративи	Україну очікує енергетична, економічна або соціальна криза	Формування страху, невизначеності та соціальної напруженості
Мобілізаційно-маніпулятивні наративи	Україна здійснює примусову мобілізацію або порушує права громадян	Стимулювання протестних настроїв, посилення соціальної поляризації
Геополітичні наративи	Україна є маріонеткою Заходу або втратила міжнародну підтримку	Делегітимація міжнародної суб'єктності України
Делегітимізаційно-пропагандистські наративи	Україна є агресором, терористичною державою або загрозою для інших держав	Формування негативного міжнародного іміджу України

Додатково аналітичні матеріали [8-10] дозволяють встановити тематичну диференціацію деструктивних впливів залежно від інформаційного сегмента. У документах чітко виокремлено український, міжнародний та російський інформаційні простори, що має принципове методологічне значення для кримінального аналізу інформаційних загроз.

В українському сегменті домінують наративи, спрямовані на дестабілізацію внутрішньополітичної ситуації, формування уявлення про неминучий енергетичний колапс, дискредитацію діяльності територіальних центрів комплектування та соціальної підтримки, а також підрив довіри до військово-політичного керівництва держави. У міжнародному інформаційному сегменті переважають повідомлення, спрямовані на формування уявлення про нібито незацікавленість України у завершенні війни, неефективність або некомпетентність європейських партнерів, а також корумпованість українського керівництва. У російському сегменті інформаційного простору деструктивні наративи мають найбільш агресивний характер і спрямовані на виправдання збройної агресії, делегітимацію України як суб'єкта міжнародних відносин, поширення звинувачень українських військових у злочинах

та формування тез про відсутність необхідності мирного врегулювання через нібито позицію української сторони.

Така сегментація підтверджує, що деструктивні інформаційні наративи не лише відтворюються у різних часових періодах, але й адаптуються до специфіки цільових аудиторій, що є ключовою ознакою координованого та керованого інформаційного впливу. Окремої уваги заслуговує використання AI-згенерованого контенту як інструменту підсилення деструктивних наративів. В аналітичних матеріалах зафіксовано поширення відео, згенерованих за допомогою штучного інтелекту, спрямованих на дискредитацію Сил оборони України. У кримінально-аналітичному вимірі цей факт є надзвичайно важливим, оскільки демонструє технологічну еволюцію інформаційних загроз. Синтетичний медіаконтент знижує ефективність традиційних способів перевірки достовірності, підвищує емоційний вплив повідомлень та створює ілюзію візуальної правдивості. Отже, предмет кримінального аналізу у сфері інформаційних загроз уже не обмежується текстовими або класичними медійними формами, а повинен охоплювати мультимедійні продукти з високим рівнем технологічної мімікрії [6].

З огляду на це кримінальний аналіз деструктивних інформаційних наративів повинен спиратися на комплекс взаємодоповнювальних методів. Насамперед ідеться про контент-аналіз, який дозволяє виявляти повторювані смислові конструкції, ключові тези, оцінні характеристики та емоційні маркери. Однак сам по собі контент-аналіз є недостатнім, оскільки він фіксує переважно змістове ядро, але не дає цілісного уявлення про механізми поширення. Саме тому він повинен поєднуватися з аналізом інформаційних потоків, що дозволяє простежити частоту появи повідомлень, динаміку їх розповсюдження та інтенсивність активізації у певні часові відрізки. Важливе значення має також OSINT-аналіз, який дає можливість виявляти джерела публікацій, повтори на різних майданчиках, зв’язки між акаунтами та цифрові сліди поширення контенту. Нарешті, аналіз соціальних мереж дозволяє виявити мережеву архітектуру поширення наративів, включаючи вузлові акаунти, точки прискорення охоплення, кластери та ознаки координованої інформаційної активності. Саме сукупність цих методів перетворює дослідження деструктивних наративів із загального спостереження за контентом на повноцінний кримінально-аналітичний процес [3].

У цьому контексті доцільно запропонувати таку логіку кримінально-аналітичного дослідження деструктивного наративу. На першому етапі здійснюється ідентифікація смислового ядра наративу, тобто визначення ключової тези, що лежить в основі серії повідомлень. На другому етапі формується масив джерел і повідомлень, у яких цей наратив відтворюється. На третьому етапі здійснюється контентне й темпоральне структурування: встановлюється, як саме варіюються формулювання, з якою частотою з’являється наратив, які події слугують тригером для його актуалізації. На четвертому етапі проводиться мережевий аналіз, який дозволяє простежити архітектуру поширення. На п’ятому етапі здійснюється ризик-оцінювання, тобто визначення потенційного впливу наративу на громадську безпеку, довіру до інституцій, емоційний стан населення, поляризацію суспільства та інші значущі безпекові параметри. Саме така процедура дозволяє розглядати деструктивний інформаційний наратив як повноцінний об’єкт кримінального аналізу інформаційних загроз, а не лише як інформаційний феномен.

Таким чином, проведений аналіз свідчить, що деструктивні інформаційні наративи у цифровому просторі мають усі ознаки самостійного кримінально-аналітичного об’єкта. Вони характеризуються повторюваністю, тематичною стабільністю, адаптивністю, сегментованістю залежно від аудиторії, технологічною еволюцією форм поширення та високим потенціалом впливу на безпекове середовище. Їх статистично фіксована присутність у цифровому просторі, відносна стабільність упродовж досліджуваних періодів та структурна організованість підтверджують, що йдеться не про хаотичний інформаційний шум, а про системне явище, яке підлягає професійному аналітичному дослідженню. Саме тому інтеграція аналізу деструктивних інформаційних наративів у систему кримінального аналізу інформаційних загроз є не лише теоретично виправданою, а й практично необхідною умовою підвищення ефективності правоохоронної діяльності в умовах сучасного цифрового та гібридного протистояння.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження дозволило встановити, що в умовах цифровізації суспільних комунікацій інформаційний простір трансформується у складне багаторівневе середовище формування сучасних безпекових загроз. У цьому середовищі деструктивні інформаційні наративи виступають не випадковими інформаційними проявами, а системно організованими смисловими конструкціями, здатними впливати на суспільні настрої, інтерпретацію подій та рівень довіри до державних інституцій.

У ході дослідження обґрунтовано, що деструктивні інформаційні наративи доцільно розглядати як відтворювані інформаційні патерни, які мають внутрішню структурованість і включають смислове ядро,

інтерпретаційні рамки, повторювані аргументаційні моделі та емоційні тригери. Їх функціонування у цифровому середовищі характеризується здатністю до адаптації, варіативністю форм подачі та збереженням змістової стабільності, що забезпечує їх тривалий і кумулятивний вплив.

На основі аналізу інформаційно-аналітичних матеріалів встановлено, що у цифровому просторі функціонує відносно стабільне тематичне ядро деструктивних інформаційних наративів. Найбільш поширеними є наративи, спрямовані на дискредитацію державного управління, делегітимацію української державності, маніпуляції у сфері мобілізаційних процесів, формування кризових очікувань та підрив міжнародної суб'єктності України. Виявлено, що зазначені наративи демонструють високу повторюваність і адаптацію до різних сегментів інформаційного простору, що свідчить про їх координований і системний характер.

Доведено, що у кримінально-аналітичному вимірі деструктивні інформаційні наративи можуть розглядатися як індикатори формування інформаційних загроз, оскільки вони відображають закономірності інформаційної поведінки, динаміку поширення та потенційні напрями дестабілізаційного впливу. Їх аналіз дозволяє переходити від фіксації окремих інформаційних повідомлень до виявлення стійких патернів і тенденцій.

Обґрунтовано, що ефективне дослідження деструктивних інформаційних наративів у межах кримінального аналізу потребує застосування комплексу взаємодоповнювальних методів, зокрема контент-аналізу, аналізу інформаційних потоків, OSINT-аналізу, аналізу соціальних мереж, темпорального аналізу та ризик-орієнтованого оцінювання. Їх інтегроване використання забезпечує можливість виявлення джерел формування наративів, механізмів їх поширення та оцінювання потенційного впливу на безпекове середовище.

Практичне значення отриманих результатів полягає у можливості їх використання у діяльності правоохоронних органів для підвищення ефективності аналітичної роботи у сфері протидії інформаційним загрозам. Зокрема, інтеграція аналізу деструктивних наративів у систему кримінального аналізу, що функціонує відповідно до принципів Intelligence-Led Policing, сприятиме своєчасному виявленню ризиків, прогнозуванню розвитку інформаційних впливів та прийняттю обґрунтованих управлінських рішень.

Перспективи подальших наукових досліджень полягають у розробленні методів кількісного вимірювання впливу деструктивних інформаційних наративів, створенні автоматизованих інструментів їх виявлення у цифровому просторі, а також у дослідженні ролі технологій штучного інтелекту у трансформації механізмів інформаційного впливу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Черниш, Р. Ф. (2023). Деструктивний інформаційний вплив в умовах гібридної війни: Сутність та загрози для національної безпеки України. *Вісник кримінального судочинства*, (3-4), 202-211.
2. Баран, М. В. (2022). *Адміністративно-правове забезпечення інформаційної безпеки в Україні* (Дисертація доктора філософії, Львівський державний університет внутрішніх справ).
3. Василенко, В. М. (2024). Цифрова трансформація правоохоронних органів: Ризики в умовах гібридних загроз та шляхи їх подолання. *Вісник Кримінологічної асоціації України*, 2(32), 945-958.
4. Василенко, В. М. (2024). Роль громад у забезпеченні цифрової безпеки: Партнерство з поліцією в умовах гібридних загроз. *Вісник Кримінологічної асоціації України*, 3(33), 782-793.
5. Шевченко, В. (2025). Різновиди маніпуляцій в онлайн-медіа і соцмережах. *Образ*, 1(47), 6-18. https://doi.org/10.21272/Obraz.2025.1(47)-6-18
6. U.S. Department of Homeland Security. (2025). *Homeland threat assessment 2025*. Office of Intelligence and Analysis. https://www.dhs.gov
7. Lambert, C., Egan, R., Turner, S., Milton, M., Khalu, M., Lobo, R., & Douglas, J. (2023). The Digital Bytes Project: Digital storytelling as a tool for challenging stigma and making connections in a forensic mental health setting. *International Journal of Environmental Research and Public Health, 20*, Article 6268. https://doi.org/10.3390/ijerph20136268
8. Центр протидії дезінформації.(2026). *Моніторинг інформаційних загроз (20-26 вересня 2025 року)*. Київ.
9. Центр протидії дезінформації. (2026). *Моніторинг інформаційних загроз (6-12 грудня 2025 року)*. Київ.
10. Центр протидії дезінформації. (2026). *Моніторинг інформаційних загроз (28 лютого - 6 березня 2026 року)*. Київ.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Olha Haborets
PhD, Associate Professor, Associate Professor of the Department of Operational and Investigative Activities and Information Security, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine
ORCID: 0000-0001-7791-6795
olga-gaborets@ukr.net

ANALYSIS OF DESTRUCTIVE INFORMATION NARRATIVES IN THE DIGITAL SPACE AS A COMPONENT OF CRIMINAL ANALYSIS OF INFORMATION THREATS

Abstract. The article examines destructive information narratives in the digital space as an independent object of criminal analysis of information threats. It is substantiated that under the conditions of the digitalization of social relations, the growing role of platform-based communications, and the transformation of contemporary security challenges, the information space acquires the characteristics of an environment in which systemic manipulative influences, disinformation campaigns, and information-psychological operations are implemented. These phenomena are capable of affecting the state of public security, the level of trust in state institutions, and the stability of social processes.

It is determined that a destructive information narrative should be considered not only as a communicative or propagandistic phenomenon but also as an analytical category characterized by semantic integrity, recurrence, adaptability to the current information agenda, multichannel dissemination, and the potential to generate negative cognitive, emotional, and behavioral effects. Such an approach enables the integration of the study of destructive narratives into the system of criminal analysis aimed at identifying patterns, trends, sources, mechanisms of dissemination, and the risk-related consequences of informational influence. The theoretical and methodological foundation of this approach is the concept of Intelligence-Led Policing, which implies a proactive, preventive, and risk-oriented model of law enforcement activity based on the use of analytical intelligence, reliable data, and analytical products to support managerial decision-making.

Based on the analysis of analytical materials, it has been established that several key groups of destructive information narratives systematically function within the digital space. These include narratives aimed at discrediting public administration, destabilizing the information environment through the dissemination of fear and uncertainty, undermining Ukraine's international subjectivity, manipulating mobilization and security-related topics, as well as technologically enhanced narratives involving AI-generated content. It is demonstrated that these narratives possess a structured nature, are characterized by recurrence, network replicability, and a high potential to influence the information environment and public sentiment.

It is substantiated that the criminal analysis of destructive information narratives should be conducted through the application of a set of complementary analytical methods, including content analysis, information flow analysis, OSINT analysis, social network analysis, as well as temporal and risk-oriented analysis. The use of such an analytical toolkit makes it possible not only to record the content of individual information messages but also to identify patterns in narrative dissemination, their network connections, the temporal dynamics of their activation, and potential risks to the security environment.

It is concluded that destructive information narratives in the digital space should be considered a full-fledged object of criminal analysis of information threats. Their systematic identification, structuring, classification, and analytical assessment constitute an important prerequisite for enhancing the effectiveness of law enforcement activities in the field of prevention and counteraction to contemporary information threats.

Keywords: criminal analysis; information threats; destructive information narratives; digital space; disinformation; analytical intelligence; OSINT; social network analysis; Intelligence-Led Policing.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Chernysh, R. F. (2023). Destructive information influence in conditions of hybrid war: Essence and threats to national security of Ukraine. *Bulletin of Criminal Proceedings*, (3–4), 202–211.

2. Baran, M. V. (2022). Administrative and legal support of information security in Ukraine (Doctoral dissertation, Lviv State University of Internal Affairs).
3. Vasylenko, V. M. (2024). Digital transformation of law enforcement agencies: Risks in conditions of hybrid threats and ways to overcome them. *Bulletin of the Criminological Association of Ukraine, 2*(32), 945–958.
4. Vasylenko, V. M. (2024). The role of communities in ensuring digital security: Partnership with police in conditions of hybrid threats. *Bulletin of the Criminological Association of Ukraine, 3*(33), 782–793.
5. Shevchenko, V. (2025). Types of manipulation in online media and social networks. *Obraz, 1*(47), 6–18. https://doi.org/10.21272/Obraz.2025.1(47)-6-18
6. U.S. Department of Homeland Security. (2025). *Homeland threat assessment 2025*. Office of Intelligence and Analysis. https://www.dhs.gov
7. Lambert, C., Egan, R., Turner, S., Milton, M., Khalu, M., Lobo, R., & Douglas, J. (2023). The Digital Bytes Project: Digital storytelling as a tool for challenging stigma and making connections in a forensic mental health setting. *International Journal of Environmental Research and Public Health, 20*, Article 6268. https://doi.org/10.3390/ijerph20136268
8. Center for Countering Disinformation. (2026). *Monitoring of information threats (September 20–26, 2025)*. Kyiv.
9. Center for Countering Disinformation. (2026). *Monitoring of information threats (December 6–12, 2025)*. Kyiv.
10. Center for Countering Disinformation. (2026). *Monitoring of information threats (February 28 – March 6, 2026)*. Kyiv.

Отримано редакцією журналу / Received: 12.02.26
Прорецензовано / Revised: 25.02.26
Схвалено до друку / Accepted: 25.06.26