НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет цивільної та господарської юстиції
Кафедра приватного права
Кафедра права інтелектуальної власності та патентної юстиції

ІТ-ПРАВО, КІБЕРБЕЗПЕКА ТА ШІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

МАТЕРІАЛИ
Всеукраїнської наукової конференції

28 березня 2026 р.

Одеса
Фенікс
2026

УДК 342.95:343.32 (477):351.863
І-92

За загальною редакцією
доктора юридичних наук, професора **Є. О. Харитонова**,
докторки юридичних наук, професорки **І. В. Давидової**

Упорядники-укладачі:

Давидова І. В. – доктор юридичних наук, професор, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Калітенко О. М. – кандидат юридичних наук, доцент, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Бобейко Н. І. – лаборантка кафедри приватного права Національного університету «Одеська юридична академія».

І-92 **ІТ-право, кібербезпека та ШІ в умовах гібридної війни** : мате-ріали Всеукр. наук. конф. (Одеса, 28 берез. 2026 р.) / за заг. ред.: д-ра юрид. наук, проф. Є. О. Харитонова, д-ра юрид наук, проф. І. В. Давидової. Одеса : Фенікс, 2026. 300 с. DOI: https://doi.org/10.32837/11300.33701

ISBN 978-617-8763-22-0

Збірник містить матеріали доповідей, присвячені актуальним проблемам ІТ-права, кібербезпеки, цифрової трансформації суспільних відносин, правового регулювання штучного інтелекту та захисту інформації в умовах гібридної війни, які були оприлюднені на Всеукраїнській науковій конференції 26 березня 2026 року в Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення науковців, викладачів, здобувачів освіти, практикуючих юристів, фахівців у сфері інформаційних технологій і кібербезпеки з результатами сучасних досліджень щодо правових, організаційних і технологічних аспектів функціонування цифрового середовища в умовах сучасних викликів. Матеріали видання можуть бути використані в науковій, освітній і практичній діяльності, а також під час подальшого вдосконалення правового регулювання цифрових відносин і забезпечення кібербезпеки України.

342.95 : 343.32 (477) : 351.863

Матеріали видано за авторською редакцією.
Повну відповідальність за достовірність і якість поданого матеріалу несуть учасники Всеукраїнської наукової конференції, їхні наукові керівники, рецензенти і структурні підрозділи вищих навчальних закладів та установ, які рекомендували ці матеріали до друку.

ISBN 978-617-8763-22-0

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ
Всеукраїнської наукової конференції

Харитонов Є. О. – завідувач кафедри приватного права Національного університету «Одеська юридична академія», д-р юрид. наук, проф. (голова);

Федотов О. П. – начальник науково- дослідної частини, професор кафедри морського, митного та інформаційного права, д-р юрид. наук, проф. (заступник голови);

Харитонова О. І. – завідувачка кафедри права інтелектуальної власності і патентної юстиції, д-р юрид. наук, проф.;

Галупова Л. І. – доцентка кафедри права інтелектуальної власності і патентної юстиції, канд. юрид. наук, доц.;

Зубар В. М. – професор кафедри приватного права, канд. юрид. наук, проф.;

Калітенко О. М. – професорка кафедри приватного права, канд. юрид. наук, доц.;

Кривенко Ю. В. – доцентка кафедри приватного права, канд.юрид. наук, доц.;

Токарева В. О. – доцентка кафедри приватного права, д-р юрид. наук,доц.;

Бобейко Н. І. – лаборантка кафедри приватного права.

. ,

Савенко Дмитро Олександрович
магістр, спеціальність «Системний аналіз»
Одеського державного університету внутрішніх справ

ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ТА ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

OSINT (Open Source Intelligence) – це методологія збору, систематизації та аналізу інформації з відкритих джерел, таких як соціальні мережі, агрегатори новин, сервіси геолокації, відкриті державні реєстри та бази даних. На відміну від традиційних розвідувальних дисциплін, інструменти та засоби OSINT є юридично прозорими та забезпечують відтворюваність результатів, тому ця дисципліна також чудово підходить для перевірки інформації у публічному просторі та використання як доказів у судових процесах.

В умовах стрімкого розвитку інформаційних технологій OSINT залишається одним із найбільш перспективних та багатосторонніх інструментів у сфері кібербезпеки. Інформація отримана за допомогою розвідки у відкритих джерелах може одночасно використовуватись як інструмент протидії загрозам національній безпеці України, так і як інструмент для їх розповсюдження, як, наприклад, розповсюдження інформації про об'єкти критичної інфраструктури, військові об'єкти та інші чутливі підприємства [1, с. 169].

Окремим видом загрози, який становить гібридна війна, є розповсюдження дезінформації та фейків, що в свою чергу може сприяти зміні соціальних настроїв та спонуканню населення країни до певних діянь, які можуть становити загрозу для національної безпеки. Тобто, збір відкритої інформації, включно з аналізом соціальних мереж, супутникових знімків, повідомлень у ЗМІ та даних із різних онлайн-ресурсів, є важливим елементом боротьби проти дезінформації [2, с. 283].

Особливу увагу слід приділити взаємодії OSINT з технологіями штучного інтелекту (ШІ) у боротьбі з дезінформацією.

Сучасні рішення на основі ШІ, такі як автоматизовані системи перевірки фактів, виявлення контенту типу «діпфейк» на основі нейронних мереж та алгоритми кластеризації скоординованих інформаційних кампаній, значно посилюють аналітичний потенціал OSINT. Інтеграція розвідки з відкритих джерел та машинного навчання створює нову парадигму боротьби з гібридними інформаційними загрозами та вимагає відповідної правової кодифікації у національному законодавстві та міжнародних угодах, що стосуються кіберпростору.

Станом на сьогоднішній день існує досить велика кількість інструментів які доцільно використовувати під час перевірки новин та протидії дезінформації як працівникам державних структур, так і приватним підприємствам:

Ще за часів окупації Криму та Донбасу росія почала систематично використовувати дезінформацію як складову доктрини «інформаційно-психологічної війни», що вже було відображено в її військових доктринах. Ключовими механізмами є: фабрикація псевдодоказів (жертви обстрілів, які стали «жертвами українських злочинів»), спотворення наративу (зображення збройної агресії як «захисту мирного населення»), а також інформаційне перевантаження – коли медіапростір навмисно розширюється настільки, щоб вмістити таку кількість суперечливих повідомлень про подію, що звичайний споживач інформації не зможе відрізнити правду від брехні. Дослідники називають цей ефект «туманом неправди».

У зв'язку із повномасштабним вторгненням російської федерації на територію України в лютому 2022 значущість та використання OSINT-інструментів різко збільшилося. Розвідка з відкритих джерел почала активно використовуватися з обох сторін конфлікту: розповсюдження дезінформації, пошук інформації про дислокацію та кількість особового складу збройних сил на певній території, моніторинг переміщення військової техніки та іншої розвідувальної інформації. Також із розвитком технологій різко збільшилось використання штучного інтелекту, особливо в контексті OSINT-інструментів.

Таблиця

Порівняння технічних можливостей OSINT інструментів

№ п/п	Назва	Технічні можливості OSINT-інструменту
1.	Hive AI	Виявляє чи використовувався ШІ під час створення аудіо-, відео- та фотоматеріалів.
2.	Decopy AI	Виявляє чи використовувався ШІ під час створення фотоматеріалів та написання тексту.
3.	TinEye	Реверсивний пошук схожих фотознімків, додатково є можливість більш розширеного пошуку з можливістю виявлення «цифрового втручання» у фотоматеріали (чи редагувався фотознімок у Фотошопі та іншому аналогічному програмному забезпеченні).
4.	InVID-WeVerify	Мультизадачний інструмент для ідентифікації фейкових новин (аналіз відео-, аудіозаписів та фотознімків, перевірки першоджерела інформації, та багато іншого функціоналу).
5.	Deepware scanner	Виявляє чи використовувався ШІ для створення відеофайлів. В наявності 4 різних моделі перевірки.
6.	AI voice detector	Виявляє чи не використовувася ШІ для створення аудіоматеріалів.
7.	Let`s Data	Дуже потужний інструмент який за допомогою ШІ-аналітики в реальному часі виявляє дезінформаційні компанії в соціальних мережах, новинних та інших ресурсах.
8.	EU vs Disinfo database	Офіційна датабаза Європейського Союзу в якій зібрано фейкові новини з проросійськими наративами з різних джерел та ресурсів.
9.	Pangram	Перевіряє чи не використовувався ШІ під час генерації тексту. Існує можливість перевірки 20+ мовами.

Таким чином, сучасний OSINT-інструментарій є ефективним засобом верифікації інформації та виявлення дезінформаційних кампаній в умовах гібридної війни в Україні. Подальший розвиток цієї галузі потребує комплексного підходу, що включає в себе як технологічне вдосконалення методів збору та аналізу даних, так і формування належної правової бази, яка б забезпечувала законність застосування відповідних інструментів та захист прав експертів, які займаються розвідкою у відкритих джерелах інформації.

ЛІТЕРАТУРА:

1. Івкова В., Опірський І. (2025). OSINT-технології як загроза кібербезпеці держави. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 3(27). С. 165-179.

2. Величко Т. (2024). Протидія російській інформаційній агресії за допомогою OSINT. *Матеріали Всеукраїнської науково-практичної конференції представників сектору безпеки і оборони України, наукових та науково-педагогічних працівників, здобувачів освіти та інших зацікавлених осіб* (м. Київ). № 1. С. 283–284.

Самойленко Георгій Валерійович
доктор юридичних наук, професор,
професор кафедри цивільного права
Запорізький національний університет

ВІДШКОДУВАННЯ ШКОДИ, ЗАВДАНОЇ ТЕРИТОРІАЛЬНІЙ ГРОМАДІ ЗБРОЙНОЮ АГРЕСІЄЮ РФ

В контексті вирішення завдання визначення особливостей відшкодування шкоди, завданої збройною агресією РФ територіальним громадам визначимо наступні аспекти. По-перше, суб'єктом, який потребує захисту порушених майнових прав у вигляді відшкодування шкоди, завданої збройною агресією РФ (позивачем) є територіальна громада, від імені якої діє орган місцевого самоврядування (місцева рада); по-друге, судова практика визнає відповідачем у різних справах РФ як державу [1], міністерство оборони, міністерство юстиції, генеральну прокуратуру РФ. Оскіль-