



Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Інститут цифровізації освіти НАПН України
Національний технічний університет України
«Київський політехнічний інститут» ім. І. Сікорського
Вінницький національний технічний університет
Житомирський військовий інститут імені С.П. Корольова
Тернопільський національний технічний університет імені Івана Пулюя
Харківський національний університет радіоелектроніки
Уманський державний педагогічний університет імені Павла Тичини
Національний університет біоресурсів і природокористування України
Інститут геохімії навколишнього середовища НАН України
Черкаський державний технологічний університет
Державний університет «Київський авіаційний інститут»

Комп'ютерні технології: інновації, проблеми, рішення

***Тези доповідей VIII Всеукраїнської
науково-технічної конференції***

м. Житомир, 02-03 грудня 2025 р.

УДК 327.56:004.056.5

*Ціфринець В.М., здобувач,
Ткачук Р.Л., д.т.н., професор,
Івануса А.І., к.т.н., доцент*

Львівський державний університет безпеки життєдіяльності

ВПЛИВ ДЕЗІНФОРМАЦІЇ НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

Розповсюдження недостовірної інформації стало критичним викликом сучасного інформаційного суспільства, впливаючи на громадську думку та процеси прийняття рішень.

Наслідки дезінформації включають політичні конфлікти, погіршення стану громадського здоров'я та загрозу національній безпеці. В умовах гібридної агресії проти України дезінформація застосовується як традиційний метод ведення війни, спрямований на дестабілізацію суспільства та послаблення державних структур.

Одночасно Україна використовує власні інформаційні інструменти для захисту населення від маніпуляцій та підтримки демократичних принципів, зберігаючи баланс між свободою слова та інформаційною безпекою. Ефективна протидія дезінформації потребує комплексного підходу, що поєднує технологічні, правові та просвітницькі заходи.

Проведений аналіз засвідчує, що дезінформація є одним із ключових чинників, які істотно впливають на внутрішню та зовнішню стабільність функціонування держави. Її поширення генерує комплекс загроз, що проявляються у соціальній, політичній, інформаційній та безпековій сферах. Серед основних негативних наслідків виявлено:

1. *Вплив дезінформації на внутрішню стабільність держави, які зводяться до:* провокування штучних конфліктів і загострення наявних поділів; активізації стереотипів і поширення атмосфери ворожнечі; зростанні емоційної напруги, що може викликати протести; поглиблення дезорієнтації та недовіри між групами; посилення політичної й етнічної поляризації; формування образу «ворога» та соціальної фрагментації; підриву довіри до влади й інститутів, зниженні легітимності; негативного впливу на психологічний стан суспільства.

2. *Вплив дезінформації на зовнішню стабільність держави, які зводяться до:* зниження довіри союзників; ускладнення дипломатичної взаємодії; формування негативного міжнародного іміджу; зростання ризиків напруги й конфліктів; провокування суперечок і регіональної дестабілізації; використання як інструменту зовнішнього тиску.

Проведене дослідження підтверджує, що дезінформація є системною загрозою, яка одночасно підриває внутрішню стійкість

держави та її зовнішньополітичні позиції. У цьому контексті визначено ключові напрями підвищення ефективності протидії дезінформаційним впливам. Насамперед необхідно вдосконалити законодавчу базу, чітко визначивши поняття, критерії та процедури виявлення дезінформації й механізми відповідальності. Важливо також посилити міжвідомчу координацію структур безпеки, медіарегуляторів і аналітичних центрів для оперативного обміну інформацією. Значну роль відіграє розвиток національних систем моніторингу на основі штучного інтелекту та аналізу великих даних. Потребує інституційної підтримки діяльність фактчекінгових ініціатив та впровадження механізмів швидкого спростування фейків. Підвищення медіаграмотності через освітні програми й суспільні кампанії посилює стійкість населення. Важливим є також розширення міжнародної співпраці з партнерами ЄС і НАТО та впровадження найкращих практик. Підвищення відкритості державних органів сприяє зменшенню впливу маніпуляцій і відновленню суспільної довіри.

Список використаних джерел:

1. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу : проблеми та підходи Історико-політичні проблеми сучасного світу : Збірник наукових статей. 2021, № 43. С. 30–39.
2. Про рішення Ради національної безпеки і оборони України від 15.10.2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>
3. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України. від 16.02.2022 року № 56/2022. URL: <https://zakon.rada.gov.ua/laws/show/56/2022#Text>
4. Крикун В., Бауліна Т. Дезінформація як засіб гібридної війни : сутність і наслідки. Вісник Київського національного університету імені Тараса Шевченка. Філософія. 2022, Вип. 2. С. 30–33. URL : http://nbuv.gov.ua/UJRN/VKNUF_2022_2_7
5. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали III Міжнародної науково-практичної конференції (Хмельницьк, 21 листопада 2024 р.). Хмельницький: НАДПСУ, 2024. С. 1136–1138.

Черкас С. А., Ящук В. І., Пановик У. П.	Інтеграція технологій безпеки для підвищення захищеності IoT-систем у побутовому середовищі	93
Щерб'як М. Т., Ящук В. І., Шклярський Р. А.	Розроблення концептуальної моделі системи захисту корпоративної мережі ТОВ «Інфо Простір Плюс» від несанкціонованого доступу на основі багаторівневої архітектури безпеки	95
Маруняк С. Т., Кирик М. І.	Інтерпретований аналіз ознак для підвищення точності класифікації аномалій BGP	97
Бень Д. Ю., Ткачук Р. Л., Ящук В. І.	Адміністративно-правові механізми забезпечення кібербезпеки держави	99
Зеленчук А. Р., Ткачук Р. Л., Федина Б. І.	Інформаційна безпека в системі національної безпеки держави	101
Кривий Р. А., Ткачук Р. Л., Балацька В. С.	Кібербезпека банківського сектору: сучасні загрози та роль ШІ у протидії	103
Панченко Н. А., Ткачук Р. Л., Полотай О. І.	Кібертероризм, дезінформація та інформаційні обмеження як загрози держбезпеці	105
Ціфринєць В. М., Ткачук Р. Л., Івануса А. І.	Вплив дезінформації на національну безпеку України	107
Шелуха О. О., Овсянніков Д. В.	Методи та технології організації захищеного доступу корпоративної мереж	109
Ретивих К. О., Колошук М. С.	Моніторинг і візуалізація мережевого трафіку за допомогою Zenarmor Dashboard	111
Ференз А. Р., Фальковський І. Г.	Огляд мережевих протоколів, що використовуються для моніторингу	113

Янчук Е. А., Нікітчук Т. М., Коренівська О. Л.	Інтерфейси мозок-комп'ютер: сучасні тенденції розвитку	443
Дудка В. Р.	Сучасні інформаційні технології у біомедицині	445