

УДК 351.862:004.056:614.8
DOI <https://doi.org/10.32782/2709-9261-2026-2-18-8>

Хондак Інна Іванівна,
кандидат технічних наук, доцент
(Харківський національний університет радіоелектроніки, м. Харків)
ORCID: <https://orcid.org/0000-0001-6644-9968>



Невлюдов Ігор Шакирович,
доктор технічних наук, професор
(Харківський національний університет радіоелектроніки, м. Харків)
ORCID: <https://orcid.org/0000-0002-9837-2309>



Мамонтов Олександр Вікторович,
кандидат технічних наук, доцент
(Харківський національний університет радіоелектроніки, м. Харків)
ORCID: <https://orcid.org/0000-0003-1464-8644>



Стиценко Тетяна Євгенівна,
кандидат технічних наук, доцент
(Харківський національний університет радіоелектроніки, м. Харків)
ORCID: <https://orcid.org/0000-0003-4530-0253>



Пронюк Ганна Валеріївна,
кандидат технічних наук, доцент
(Харківський національний університет радіоелектроніки, м. Харків)
ORCID: <https://orcid.org/0000-0001-7648-0360>



ІНФОРМАЦІЙНЕ ЗАБРУДНЕННЯ ЯК ФАКТОР РИЗИКУ ДЛЯ СИСТЕМИ ЦИВІЛЬНОГО ЗАХИСТУ В УМОВАХ ВОЄННОГО СТАНУ

У статті досліджено вплив інформаційного забруднення на функціонування системи цивільного захисту України в умовах воєнного стану. Запропоновано класифікацію інформаційних загроз, проаналізовано динаміку медіаграмотності населення та кіберінцидентів, а також розроблено модель інформаційного забруднення. Обґрунтовано напрями підвищення стійкості системи цивільного захисту до сучасних інформаційних загроз.

Ключові слова: цивільний захист, інформаційне забруднення, інформаційна безпека, надзвичайні ситуації, дезінформація, воєнний стан, інформаційний простір.

Постановка проблеми. Війна в Україні докорінно змінила характер сучасних загроз. Поряд із традиційними природними, техногенними та соціальними небезпеками суттєво зросла роль інформаційних факторів, здатних впливати на безпеку населення. Інформація перетворилася не лише на ресурс управління, але й на інструмент ведення війни.

Система цивільного захисту нині функціонує в умовах постійного інформаційного навантаження. Населення щоденно отримує значний обсяг повідомлень із різних джерел: офіційних державних органів, соціальних мереж, месенджерів, засобів масової інформації та приватних каналів комунікації. Значна частина цих повідомлень містить недостовірну або суперечливу інформацію, що створює явище інформаційного забруднення.

На відміну від класичних екологічних видів забруднення, а саме матеріального й енергетичного, інформаційне забруднення не має матеріальної форми, проте його наслідки можуть бути не менш небезпечними [1]. Воно здатне змінювати поведінку людей, формувати панічні настрої, знижувати довіру до органів державної влади та перешкоджати проведенню заходів цивільного захисту.

Інформаційне забруднення нині є не лише проблемою інформаційної безпеки, а й чинником виникнення надзвичайних ситуацій, який безпосередньо впливає на ефективність цивільного захисту населення.

Актуальність дослідження зумовлена тим, що в умовах повномасштабної війни інформаційний простір став одним із ключових середовищ ведення гібридного протистояння. Поширення дезінформації, фейкових повідомлень, маніпулятивного контенту, інформаційно-психологічних операцій та кіберінцидентів суттєво впливає на ефективність функціонування системи цивільного захисту, ускладнює процес прийняття управлінських рішень, спричиняє панічні настрої серед населення та знижує результативність реагування на надзвичайні ситуації. Незважаючи на значну кількість досліджень у сфері інформаційної та кібернетичної безпеки, інформаційне забруднення як самостійний фактор ризику для системи цивільного захисту досліджено не досить. Це зумовлює необхідність комплексного аналізу його впливу та розроблення практичних підходів до підвищення стійкості системи цивільного захисту до сучасних інформаційних загроз.

Аналіз останніх досліджень та публікацій. Проблеми інформаційної безпеки, протидії дезінформації та забезпечення стійкого функціонування системи цивільного захисту останніми роками набули особливої актуальності. Значний внесок у дослідження інформаційних війн, інформаційно-психологічних операцій та механізмів інформаційного впливу зробив Г. Почепцов [2]. Інформаційна війна, що нині є основою протистояння [3, с. 151], спрямована на маніпуляцію свідомістю аудиторії.

Питання протидії негативним інформаційним впливам досліджував В. Пальчук, розглядає механізми поширення дезінформації, неправдивого та маніпулятивного

контенту в глобальному й національному інформаційних просторах [4].

Б. Гривнак досліджував дезінформацію як одну з ключових загроз національній безпеці України в умовах російсько-української війни, особливу увагу приділив необхідності формування ефективних механізмів протидії дезінформації та зміцнення інформаційної безпеки України. Дезінформація як явище потребує юридичного визначення в українському законодавстві. Для ефективної протидії цьому явищу потрібне релевантне законодавство, що визначатиме чіткі механізми боротьби, відповідальність за поширення дезінформації, порядок притягнення до неї [5].

Проблеми дезінформації та забезпечення інформаційної безпеки держави висвітлено також у працях О. Пугачова [6], Д. Лободи, Н. Прямухіної [7], О. Бровко, О. Курбан [8] та інших учених.

Як зазначає український науковець М. Захаревиц, інформаційна війна постає як складна система комунікативних практик, яка не лише формує громадську думку, а й активно впливає на когнітивні структури, визначаючи сприйняття реальності та стратегічні пріоритети [9].

Теоретичні та практичні засади функціонування системи цивільного захисту, управління ризиками, кризового реагування та державного управління у цій сфері розкрито у роботі М. Андрієнка. Нині розвиток системи ЦЗ є важливим складником розвитку всієї системи забезпечення національної безпеки, а тому вимагає постійного доктринального дослідження та методологічного забезпечення [10].

Разом із тим аналіз наукових публікацій свідчить, що більшість досліджень присвячено окремим аспектам інформаційної або кібернетичної безпеки, тоді як інформаційне забруднення як самостійний фактор ризику для системи цивільного захисту практично не розглядається. Не досить дослідженими залишаються питання його впливу на процеси управління надзвичайними ситуаціями, поведінку населення під час кризових подій та ефективність функціонування органів цивільного захисту. Це зумовило необхідність проведення цього дослідження.

Метою статті є дослідження впливу інформаційного забруднення на функціонування системи цивільного захисту в умовах воєнного стану, систематизація інформаційних загроз, аналіз сучасних тенденцій їх розвитку та розроблення практичних заходів щодо підвищення стійкості органів управління і населення до інформаційних впливів.

Виклад основного матеріалу. Інформаційне забруднення можна визначити як сукупність негативних інформаційних впливів, що порушують процеси сприйняття, аналізу та використання інформації людиною або системою управління.

До основних складників інформаційного забруднення належать:

- поширення фейкових повідомлень;
- дезінформація;
- інформаційний шум;
- маніпулятивні повідомлення;

– пропаганда;
– масове дублювання неперевіраних повідомлень;
– кіберінциденти, що призводять до спотворення інформації.

Особливо небезпечним є поєднання інформаційного забруднення із фізичними надзвичайними ситуаціями. Всі інформаційні загрози у сфері цивільного захисту представлені у таблиці 1.

Таблиця 1

Класифікація інформаційних загроз у системі цивільного захисту

Класифікаційна ознака	Види інформаційних загроз	Характеристика	Можливі наслідки для цивільного захисту
За джерелом походження	Зовнішні	Інформаційний вплив з боку іноземних держав, спецслужб, міжнародних хакерських угруповань	Дестабілізація роботи органів влади, паніка серед населення
	Внутрішні	Недостовірні інформація від громадян, посадових осіб, медіа, помилки операторів	Помилкові управлінські рішення, зниження довіри до офіційних повідомлень
За способом поширення	Соціальні мережі	Facebook, Instagram, TikTok тощо	Масове поширення дезінформації
	Месенджери	Telegram, Viber, WhatsApp, Signal	Швидке розповсюдження чуток та фейків
	Засоби масової інформації	Телебачення, радіо, друковані та інтернет-ЗМІ	Формування громадської думки
	Усні повідомлення	Чутки, «сарафанне радіо»	Поширення панічних настроїв
За характером впливу	Дезінформація	Свідоме поширення неправдивих відомостей	Введення населення в оману
	Фейки	Повністю вигадані повідомлення	Паніка, хаотична поведінка
	Маніпуляція	Використання правдивої інформації з викривленням змісту	Формування хибного сприйняття ситуації
	Інформаційний шум	Надлишок повідомлень, що ускладнює пошук достовірної інформації	Перевантаження інформаційного простору
	Пропаганда	Систематичний психологічний вплив	Зміна суспільних настроїв
За технічним способом реалізації	Кібератаки	Злом інформаційних систем	Порушення роботи інформаційних ресурсів
	Фішинг	Викрадення персональних даних	Компрометація інформаційних систем
	Deepfake	Підроблені відео, фото та аудіо	Дискредитація органів влади
	Бот-мережі	Автоматизоване поширення повідомлень	Штучне формування громадської думки
За об'єктом впливу	Населення	Психологічний вплив на громадян	Паніка, недовіра, порушення громадського порядку
	Органи державної влади	Інформаційний вплив на процес управління	Прийняття помилкових рішень
	Підрозділи цивільного захисту	Поширення неправдивої оперативної інформації	Зниження ефективності реагування
	Критична інфраструктура	Інформаційний вплив на системи управління	Порушення функціонування об'єктів
За масштабом поширення	Локальні	Обмежена територія або окремих об'єкт	Локальна дестабілізація
	Регіональні	Окрема область або кілька громад	Порушення роботи регіональних служб
	Загальнодержавні	Уся територія країни	Масова паніка, порушення функціонування державних структур
	Глобальні	Міжнародний інформаційний простір	Транскордонні інформаційні кризи
За тривалістю впливу	Короточасні	Одноразові інформаційні атаки	Тимчасова дестабілізація
	Довготривалі	Систематичний інформаційний вплив	Формування стійких хибних переконань
За наслідками	Психологічні	Страх, паніка, стрес	Масова дезорганізація населення
	Організаційні	Порушення управління	Затримка реагування на надзвичайні ситуації
	Соціальні	Втрата довіри до державних інституцій	Соціальна напруга
	Економічні	Збитки підприємств та держави	Порушення роботи економіки
	Безпекові	Підвищення ризику для життя людей	Зростання кількості постраждалих

[складено авторами]

Запропонована авторами класифікація демонструє, що інформаційні загрози мають комплексний характер і можуть класифікуватися за різними ознаками: джерелом виникнення, способом поширення, характером впливу, технічними механізмами реалізації, об'єктом ураження, масштабом, тривалістю та наслідками. Такий підхід дозволяє більш точно оцінювати рівень ризику інформаційного забруднення та обґрунтовувати заходи щодо підвищення стійкості системи цивільного захисту в умовах надзвичайних ситуацій і воєнного стану. Ця таблиця може слугувати основою для подальшого аналізу та розроблення моделей оцінювання інформаційних ризиків.

Наскільки населення стало більш стійким до інформаційного забруднення проаналізовано за допомогою індексу медіаграмотності. Індекс медіаграмотності оцінює, наскільки люди розуміють роботу медіа, як вони споживають інформацію, чи здатні перевіряти її достовірність, а також наскільки добре володіють цифровими інструментами.

Динаміка рівня медіаграмотності українців (2020–2025) показана на рисунку 1 [11; 12]. Індекс медіаграмотності використовується як інтегральний показник оцінювання інформаційної компетентності населення. Він враховує рівень розуміння принципів роботи медіа, особливості споживання інформації, уміння перевіряти її достовірність, розпізнавати маніпулятивний контент, а також рівень цифрової компетентності користувачів. Аналіз результатів дослідження демонструє позитивну динаміку цього показника після 2022 року, тоді і відбулося його різке зростання (українці почали значно активніше перевіряти інформацію і користуватися різними джерелами новин). За результатами дослідження 2025 року середній індекс медіаграмотності українців досяг 5,2 бала із 10 можливих, що характеризує достатній рівень інформаційної стійкості населення в умовах посилення інформаційних загроз [12].

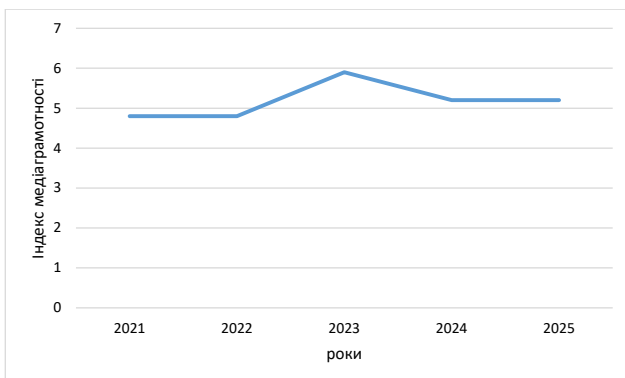


Рис. 1. Динаміка рівня медіаграмотності українців

Одним із проявів інформаційного забруднення є зростання кількості кібератак, які використовуються для порушення роботи інформаційних систем, поширення дезінформації та дестабілізації діяльності державних органів і об'єктів критичної інфраструктури. Динаміка кіберінцидентів є важливим індикатором рівня інформаційних загроз і характеризує інтенсивність протистояння у кіберпросторі.

На рисунку 2 наведено динаміку кількості кіберінцидентів, зареєстрованих Державним центром кіберзахисту України протягом 2021–2025 років [13; 14; 15].

У 2025 році було зареєстровано 3018 кіберінцидентів у I півріччі та 2909 – у II півріччі, що свідчить про збе-

реження високого рівня кіберзагроз протягом року [15]. Водночас, незважаючи на незначне збільшення кількості розсилок шкідливого програмного забезпечення, фактична кількість випадків інфікування комп'ютерів зменшилася. Така тенденція пояснюється підвищенням рівня кіберстійкості українських організацій, ефективною роботою команд реагування на кіберінциденти, оперативним виявленням і блокуванням шкідливої активності, а також зростанням обізнаності користувачів щодо дотримання основ кібергігієни.

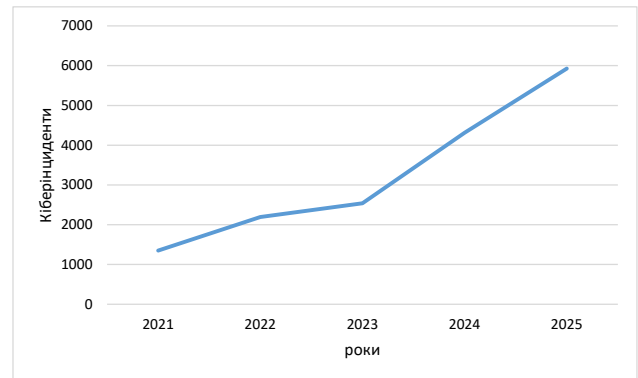


Рис. 2. Динаміка рівня зареєстрованих кіберінцидентів

Аналіз рис. 2 показує стійку тенденцію до зростання кількості зареєстрованих кіберінцидентів в Україні протягом 2021–2025 років. Якщо у 2021 році було зафіксовано 1350 кіберінцидентів, то у 2022 році їхня кількість збільшилася до 2194, що становить приріст 62,5%. Таке зростання безпосередньо пов'язане з початком повномасштабної збройної агресії Російської Федерації, під час якої кіберпростір став одним із ключових напрямів ведення гібридної війни.

У наступні роки тенденція до збільшення кількості кіберінцидентів зберігалася. У 2023 році Державним центром кіберзахисту було зареєстровано 2541 інцидент, що на 15,8% більше порівняно з попереднім роком. Найбільш стрімке зростання спостерігалось у 2024 році, коли кількість кіберінцидентів досягла 4315, тобто збільшилася майже на 70%. У 2025 році цей показник зріс до 5927 випадків, що на 37,4% перевищує рівень 2024 року.

Загалом за досліджуваний період кількість зареєстрованих кіберінцидентів збільшилася більш ніж у 4,4 раза, що свідчить про істотне посилення інформаційних і кібернетичних загроз для державних органів, об'єктів критичної інфраструктури та суспільства загалом. Отримані результати підтверджують, що кіберпростір став одним із головних театрів сучасного протистояння, а інформаційне забруднення, дезінформація та кібератаки дедалі частіше використовуються комплексно як елементи гібридної війни.

Зазначена динаміка підкреслює необхідність подальшого розвитку системи цивільного захисту шляхом удосконалення механізмів кіберзахисту, впровадження сучасних систем моніторингу інформаційного простору, підвищення рівня медіаграмотності населення та зміцнення міжвідомчої взаємодії у сфері інформаційної безпеки.

Авторами побудовано модель інформаційного забруднення та його впливу на систему цивільного захисту з метою систематизації основних джерел, механізмів поширення, наслідків інформаційних загроз і визначення ефективних напрямів їх попередження та мінімізації (рис. 3).

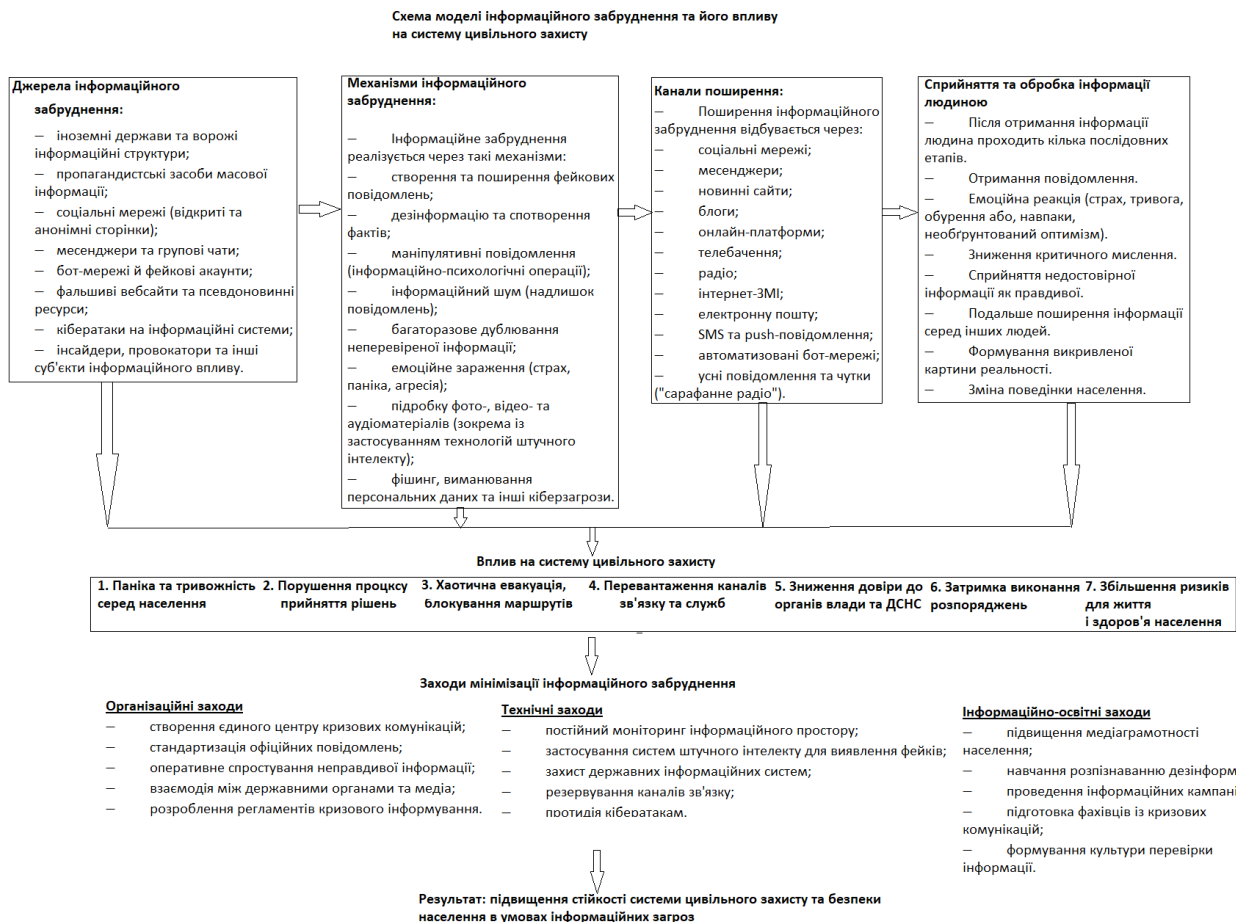


Рис. 3. Схема моделі інформаційного забруднення та його впливу на систему цивільного захисту

Запропонована авторами модель узагальнює взаємозв'язок між джерелами інформаційного забруднення, механізмами його поширення, каналами передачі інформації, наслідками для населення та системи цивільного захисту, а також комплексом заходів щодо їх мінімізації. На відміну від наявних підходів, модель розглядає інформаційне забруднення як самостійний фактор ризику, що впливає на ефективність управління надзвичайними ситуаціями в умовах воєнного стану та може бути використаний як основа для вдосконалення інформаційно-аналітичного забезпечення органів цивільного захисту.

Інформаційне забруднення негативно впливає практично на всі етапи функціонування системи цивільного захисту.

На етапі прогнозування ризиків воно ускладнює отримання достовірної інформації про обстановку.

Під час реагування на надзвичайні ситуації інформаційне забруднення може спричиняти:

- паніку серед населення;
- хаотичну евакуацію;
- блокування транспортних маршрутів;
- перевантаження телефонних мереж;
- недовіру до офіційних повідомлень;
- затримку виконання розпоряджень органів влади.

У процесі ліквідації наслідків надзвичайних ситуацій поширення неправдивих повідомлень здатне створювати додаткові ризики для рятувальників та населення.

В умовах війни особливого значення набувають інформаційно-психологічні операції противника, які поєднуються з ракетними ударами, кібератаками та диверсійною діяльністю.

Висновки. Проведене дослідження підтвердило, що в умовах воєнного стану інформаційне забруднення перетворилося на один із вагомих факторів ризику для системи цивільного захисту. Його негативний вплив проявляється у поширенні дезінформації, виникненні панічних настроїв, порушенні процесів управління надзвичайними ситуаціями, зниженні ефективності кризових комунікацій та ускладненні роботи органів цивільного захисту.

У роботі запропоновано класифікацію інформаційних загроз, що дозволяє систематизувати їх за джерелами виникнення, способами поширення, характером впливу, технічними механізмами реалізації, об'єктами ураження та можливими наслідками. На основі аналізу статистичних даних встановлено стійку тенденцію до зростання кількості кіберінцидентів упродовж 2021–2025 років, що свідчить про посилення інформаційних і кібернетичних загроз у період повномасштабної війни. Водночас позитивна динаміка індексу медіаграмотності населення свідчить про поступове підвищення стійкості суспільства до інформаційних впливів.

Науковою новизною дослідження є запропонована авторами модель впливу інформаційного забруднення на систему цивільного захисту, яка відображає взаємозв'язок між джерелами інформаційних загроз, механізмами їх поширення, наслідками та комплексом заходів щодо їх мінімізації. Практичне значення одержаних результатів полягає у можливості використання запропонованих підходів під час удосконалення інформаційно-аналітичного забезпечення органів цивільного захисту, розвитку кризових комунікацій, підвищення рівня медіаграмотності населення та розроблення заходів щодо зміцнення інформаційної стійкості держави.

Список використаних джерел

1. Хондак І. І. Підвищення безпеки праці при інформаційному забрудненні. *Наука і техніка сьогодні. Серія «Техніка»*. 2024. № 2(30). С. 931–944. [https://doi.org/10.52058/2786-6025-2024-2\(30\)-931-944](https://doi.org/10.52058/2786-6025-2024-2(30)-931-944)
2. Почепцов Г. Г. Смыслові та інформаційні війни. *Інформаційне суспільство*. 2013. Вип. 18. С. 21–27.
3. Бадер А. В., Вовк С. О. Прийоми та засоби інформаційної війни. Переосмислення проблеми. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2024. Вип. 54. С. 145–153. DOI: <https://doi.org/10.30970/PPS.2024.54.17>
4. Пальчук В. Особливості протидії негативним інформаційним впливам. *Наукові праці Національної бібліотеки України ім. В. І. Вернадського*. 2022. Вип. 64. С. 469–483. DOI: <https://doi.org/10.15407/np.64.469>
5. Гривнак Б., Лопушинський І., Сапіжак І. Дезінформація як загроза національній безпеці України в умовах неоголошеної російсько-української війни. *Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування»*. 2024. Вип. 1. С. 53–63. DOI: <https://doi.org/10.32782/2786-5681-2024-1.07>
6. Пугачов О. І. Проблеми забезпечення інформаційної безпеки України в сучасних умовах. *Проблеми сучасних трансформацій. Серія : Право, державне управління та адміністрування*. 2024. № 12. DOI: <https://doi.org/10.54929/2786-5746-2024-12-02-15>
7. Лобода Д. О., Прямухіна Н. В. Боротьба з дезінформацією як частина інформаційної безпеки держави. *Прикладні аспекти сучасних міждисциплінарних досліджень : матеріали II міжнар. наук.-практ. конф., м. Вінниця, січень 2024 р. Вінниця : ДонНУ імені Василя Стуса*, 2024. С. 95–96. URL: <https://jpasmd.donnu.edu.ua/article/view/14777>
8. Інформаційно-комунікаційна безпека: сучасні тренди : монографія / Бровко О. О. та ін. ; за заг. ред.: Курбан О. В., Лісневська А. Л. Київ : Київ. ун-т ім. Б. Грінченка, 2022. 392 с. URL: https://www.researchgate.net/profile/alina-lisnevskaya-2/publication/378316003_informacijno-komunikacijna_bezpeka/links/65d486e21141586f3f51393c/informacijno-komunikacijna-bezpeka.pdf
9. Захаревич М. Протидія російській дезінформації та кіберзагрозам у підготовці майбутніх учителів «Захисту України». *Вісник Черкаського національного університету імені Богдана Хмельницького. Серія «Педагогічні науки»*. 2025. № 3. С. 67–74. DOI: <https://doi.org/10.31651/2524-2660-2025-3-67-74>
10. Андрієнко М. В., Гаман П. І., Гордєєв П. М. Особливості становлення цивільного захисту України в контексті безпекової функції. *Сучасний науковий журнал*. 2023. № 1(1). С. 72–83. DOI: <https://doi.org/10.36994/2786-9008-2023-1-10>
11. Індекс медіаграмотності українців – 2025 : вебсайт. URL: <https://www.undp.org/uk/ukraine/publications/indeks-mediahramotnosti-ukrayintsiv-2025> (дата звернення 14.07.2026).
12. Кричківська Г. Рівень медіаграмотності українців стабільний, кількість користувачів ІІІ зросла до 49%: дослідження. URL: <https://osvitoria.media/news/riven-mediahramotnosti-ukrayintsiv-stabilnyj-kilkist-korystuvachiv-shi-zroslo-do-49-doslidzhennya/> (дата звернення: 14.07.2026).
13. У 2022 році кількість зареєстрованих кіберінцидентів виросла майже втричі – звіт. URL: <https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zarejestrovanih-kiberincidentiv-viroslo-maizhe-vtrichi-zvit> (дата звернення: 14.07.2026).
14. CERT-UA минулого року опрацювала 4315 кіберінцидентів. URL: <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv> (дата звернення: 14.07.2026).
15. Зростання кількості кіберінцидентів припинилося, але інтенсивність атак ворога залишається високою – звіт CERT-UA за II півріччя 2025 року. URL: <https://cip.gov.ua/ua/news/zrostantnya-kilkosti-kiberincidentiv-pripinilosya-ale-intensivnist-atak-voroga-zalishayetsya-visokoyu-zvit-cert-ua-za-ii-pivrichchya-2025-roku> (дата звернення: 14.07.2026).

References

1. Khondak, I. I. (2024). Pidvishchennya bezpeki pratsi pri informatsiinomu zabrudnenni [Improving occupational safety in the event of information pollution]. *Nauka i tekhnika sodayni. Seriya «Tekhnika» – Science and Technology Today. Series “Technology”*, 2(30), 931–944. DOI: [https://doi.org/10.52058/2786-6025-2024-2\(30\)-931-944](https://doi.org/10.52058/2786-6025-2024-2(30)-931-944) [in Ukrainian].
2. Pocheptsov, G. G. (2013). Smislovi ta informatsiini viini [Semantic and information wars]. *Informatsiine suspilstvo – Information society*, 18, 21–27 [in Ukrainian].
3. Bader, A. V., & Vovk, S. O. (2024). Priiomi ta zasobi informatsiinoi viini [Techniques and means of information warfare]. *Pereosmislennya problemi. Visnik Lvivskogo universitetu. Seriya filos.-politolog. studiyi – Rethinking the problem. Bulletin of Lviv University. Series of philosophical and political science studies*, 54, 145–153. DOI: <https://doi.org/10.30970/PPS.2024.54.17> [in Ukrainian].
4. Palchuk, V. (2022). Osoblivosti protidiyi negativnim informatsiinim vplivam [Features of countering negative information influences]. *Naukovi pratsi Natsionalnoi biblioteki Ukrayini im. V. I. Vernadskogo – Scientific works of the National Library of Ukraine named after V. I. Vernadsky*, 64, 469–483. DOI: <https://doi.org/10.15407/np.64.469> [in Ukrainian].
5. Grivnak, B., Lopushinskii, I., & Sapizhak, I. (2024). Dezinformatsiya yak zagroza natsionalnii bezpetsi Ukraini v umovakh neogoloshenoi rosiisko-ukraynskoyi viini [Disinformation as a threat to the national security of Ukraine in the context of the undeclared Russian-Ukrainian war]. *Naukovii visnik Vinnitskoyi akademiyi bezperervnoyi osviti. Seriya «Ekologiya. Publichne upravlinnya ta administruvannya» – Scientific Bulletin of the Vinnytsia Academy of Continuing Education. Series “Ecology. Public Management and Administration”*, 1, 3–63. DOI: <https://doi.org/10.32782/2786-5681-2024-1.07> [in Ukrainian].
6. Pugachov, O. I. (2024). Problemi zabezpechennya informatsiynoyi bezpeki Ukrayini v suchasniy umovah [Problems of Ensuring Information Security of Ukraine in Modern Conditions]. *Problemi suchasniy transformacij. Seriya: Pravo, derzhavne upravlinnya ta administruvannya – Problems of Modern Transformations. Series: Law, Public Management and Administration*, 12. DOI: <https://doi.org/10.54929/2786-5746-2024-12-02-15> [in Ukrainian].
7. Loboda, D. O., & Pryamukhina, N. V. (2024). Borotba z dezinformatsieyu yak chastina informatsiynoyi bezpeki derzhavi [Combating disinformation as part of the state’s information security]. *Proceedings from II Mizhnarodna naukovo-praktychna konferentsiya «Prikladni aspekti suchasniy mizhdisziplinarniy doslidzhen» – The second International Scientific and Practical Conference “Applied Aspects of Modern Interdisciplinary Research”*. (pp. 95–96). Vinnytsia: Vasyl Stus Donetsk National University. Retrieved from <https://jpasmd.donnu.edu.ua/article/view/14777> [in Ukrainian].

8. Brovko, O. O. (2022). Informatsiino-komunikatsiina bezpeka: suchasni trendi [Information and communication security: current trends]. Kyiv. B. Grinchenko University. Retrieved from https://www.researchgate.net/profile/alina-lisnevskya-2/publication/378316003_informacijno-komunikacijna_bezpeka/links/65d486e21141586f3f51393c/informacijno-komunikacijna-bezpeka.pdf [in Ukrainian].
9. Zakharevich, M. (2025) Protidiya rosiiskii dezinformatsiyi ta kiberzagrozam u pidgotovtsi maibutnikh uchiteliv «Zakhistu Ukraini» [Countering Russian disinformation and cyber threats in the training of future teachers of the “Defense of Ukraine”]. *Visnik Cherkaskogo natsionalnogo universitetu imeni Bogdana Khmelnytskogo. Seriya «Pedagogichni nauki» – Bulletin of the Bohdan Khmelnytskyi Cherkasy National University. Series “Pedagogical Sciences”*, 3, 67–74. DOI: <https://doi.org/10.31651/2524-2660-2025-3-67-74> [in Ukrainian].
10. Andriienko, M. V., Gaman, P. I., & Gordeev, P. M. (2023). Osoblivosti stanovlennya tsivilnogo zakhistu Ukraini v konteksti bezpekovoï funktsiyi [Peculiarities of the formation of civil defense in Ukraine in the context of the security function]. *Suchasni naukovii zhurnal – Modern scientific journal*, 1(1), 72–83. DOI: <https://doi.org/10.36994/2786-9008-2023-1-10> [in Ukrainian].
11. Indeks mediahramotnosti ukraintsiv – 2025 [Ukrainian Media Literacy Index – 2025]. (2026). Retrieved from <https://www.undp.org/uk/ukraine/publications/index-mediahramotnosti-ukrayintsiv-2025> [in Ukrainian].
12. Krichkovska, G. Riven mediagramotnosti ukrayintsiv stabilnii, kilkist koristuvachiv ShI zroslo do 49%: doslidzhennya [The level of media literacy of Ukrainians is stable, the number of AI users has increased to 49%: study]. Retrieved from <https://osvitoria.media/news/riven-mediagramotnosti-ukrayintsiv-stabilnyj-kilkist-korystuvachiv-shi-zroslo-do-49-doslidzhennya/> [in Ukrainian].
13. U 2022 roci kilkist zareyestrovanih kiberincidentiv viroslo majzhe vtrichi – zvit [The number of registered cyber incidents almost tripled in 2022 – report]. Retrieved from <https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanih-kiberincidentiv-viroslo-majzhe-vtrichi-zvit> [in Ukrainian].
14. CERT-UA minulogo roku opracyuvala 4315 kiberincidentiv [CERT-UA processed 4.315 cyber incidents last year]. Retrieved from <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv> [in Ukrainian].
15. Zrostantnya kilkosti kiberincidentiv pripinilosya, ale intensivnist atak voroga zalishayetsya visokoyu – zvit CERT-UA za II pivrichchya 2025 roku [The growth in the number of cyber incidents has stopped, but the intensity of enemy attacks remains high – CERT-UA report for the second half of 2025]. Retrieved from <https://cip.gov.ua/ua/news/zrostantnya-kilkosti-kiberincidentiv-pripinilosya-ale-intensivnist-atak-voroga-zalishayetsya-visokoyu-zvit-cert-ua-za-ii-pivrichchya-2025-roku> [in Ukrainian].

Khondak Inna,

Candidate of Technical Sciences, Associate Professor
(Kharkiv National University of Radioelectronics, Kharkiv)
ORCID: <https://orcid.org/0000-0001-6644-9968>

Nevliudov Igor,

Doctor of Technical Sciences, Professor
(Kharkiv National University of Radioelectronics, Kharkiv)
ORCID: <https://orcid.org/0000-0002-9837-2309>

Mamontov Oleksandr,

Candidate of Technical Sciences, Associate Professor
(Kharkiv National University of Radioelectronics, Kharkiv)
ORCID: <https://orcid.org/0000-0003-1464-8644>

Stytsenko Tetiana,

Candidate of Technical Sciences, Associate Professor
(Kharkiv National University of Radioelectronics, Kharkiv)
ORCID: <https://orcid.org/0000-0003-4530-0253>

Proniuk Ganna,

Candidate of Technical Sciences, Associate Professor
(Kharkiv National University of Radioelectronics, Kharkiv)
ORCID: <https://orcid.org/0000-0001-7648-0360>

INFORMATION POLLUTION AS A RISK FACTOR FOR THE CIVIL PROTECTION SYSTEM UNDER MARTIAL LAW

The article examines information pollution as a significant modern risk factor affecting the functioning of the civil protection system of Ukraine under martial law. The study is based on the understanding that information space has become one of the key environments of hybrid warfare, where disinformation, fake messages, manipulative content, information noise, cyber incidents, and psychological influence operations can substantially affect public safety, crisis management, and emergency response effectiveness.

The purpose of the study is to determine the impact of information pollution on the civil protection system, to classify the main information threats, and to develop practical measures aimed at increasing the resilience of public authorities and the population to destructive information influences. The research applies methods of analysis, comparison, systematization, and interpretation of statistical data related to media literacy and cyber incidents in Ukraine during 2021–2025.

The paper proposes an author's classification of information threats according to their source, dissemination channel, nature of influence, technical implementation mechanism, object of impact, scale, duration, and consequences for civil protection. Special attention is paid to the relationship between information pollution and cyber threats. Statistical analysis demonstrates a steady increase in the number of registered cyber incidents, which confirms the growing intensity of information and cyber risks in the conditions of full-scale war.

In addition, the study analyzes the dynamics of the media literacy index of the Ukrainian population, which reached 5.2 points out of 10 in 2025, indicating a gradual increase in society's ability to critically evaluate information and resist manipulative influences. An author's model of information pollution and its impact on the civil protection system is developed, reflecting the interconnection between sources of information threats, dissemination mechanisms, consequences for the population and authorities, and measures for their prevention and minimization.

The practical significance of the research lies in substantiating organizational, technical, and educational measures aimed at strengthening crisis communications, improving information and analytical support, implementing monitoring systems for the information space, enhancing cyber protection, and increasing the level of media literacy and cyber hygiene of the population. The proposed approaches can be used to improve the resilience of the civil protection system to modern information threats under martial law.

Key words: civil protection, information pollution, information security, emergencies, disinformation, martial law, information space.

Дата першого надходження статті до видання: 16.07.2026
Дата прийняття статті до друку після рецензування: 17.08.2026
Дата публікації (оприлюднення) статті: 14.10.2026