

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ЗАКЛАД «ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ К. Д. УШИНСЬКОГО»

КАФЕДРА ПОЛІТИЧНИХ НАУК І ПРАВА
ЦЕНТР СОЦІАЛЬНО-ПОЛІТИЧНИХ ДОСЛІДЖЕНЬ «POLITICUS»

ІХ ВСЕУКРАЇНСЬКА НАУКОВО - ПРАКТИЧНА КОНФЕРЕНЦІЯ

«СУЧАСНА УКРАЇНСЬКА ДЕРЖАВА: ВЕКТОРИ РОЗВИТКУ ТА
ШЛЯХИ МОБІЛІЗАЦІЇ РЕСУРСІВ»



30 квітня 2025 року

Одеса

УДК 321(477)(063)

С91

Рекомендовано до друку рішенням Вченої ради
ДЗ «Південноукраїнський національний
педагогічний університет імені К. Д. Ушинського»
(№ 17 від 26 червня 2025 року)

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Музиченко Г. В. – доктор політичних наук, професор, професор кафедри політичних наук і права ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»;

Наумкіна С. М. – доктор політичних наук, професор, завідувач кафедри політичних наук і права ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»;

Гедікова Н. П. – доктор політичних наук, професор, професор кафедри політичних наук і права ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»;

Долженков О. Ф. – доктор юридичних наук, професор, професор кафедри політичних наук і права ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»;

Каменчук Т.О. – кандидат політичних наук, доцент, доцент кафедри політичних наук і права ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»

Проноза І.І. – кандидат політичних наук, доцент, доцент кафедри політичних наук і права ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»;

Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів : матеріали IX Всеукраїнської науково-практичної конференції, м. Одеса 30 квітня 2025 року. Одеса ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», центр соціально-політичних досліджень «POLITICUS», 2025. 253с.

УДК 321(477)(063)

С91

© ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», 2025

© Центр соціально-політичних досліджень «POLITICUS», 2025

14. Каменчук Т. О. ІНФОРМАЦІЙНА СФЕРА УКРАЇНИ. НАЦІОНАЛЬНІ ІНТЕРЕСИ ТА ПРІОРИТЕТИ ДЕРЖАВНОЇ ПОЛІТИКИ. 67
15. Карагіоз Р. С. ЗМІЦНЕННЯ ПОЛІТИКО ПРАВОВИХ ОСНОВ УКРАЇНСЬКОЇ ДЕРЖАВНОСТІ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ 72
16. Коваль О. А., Проноза І. І. ПОЛІТИЧНЕ ЛІДЕРСТВО ЯК КЛЮЧОВИЙ РЕСУРС МОДЕРНІЗАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ 77
17. Козловська Л. В., Уцеховський М. Ю. ПОЛІТИЧНА КУЛЬТУРА МІГРАНТІВ-БІЖЕНЦІВ ВІД ВІЙНИ З УКРАЇНИ В УМОВАХ АГРЕСІЇ РФ ТА ЇЇ АДАПТАЦІЯ ДО ЛОКАЛЬНИХ ДЕМОКРАТИЧНИХ СТРАТЕГІЙ ПРИЙМАЮЧИХ КРАЇН ЄС 2022-2025 РР 81
18. Кокорев О. В. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ ТА ГІБРИДНОЇ АГРЕСІЇ: ЛАНДШАФТ ІНФОРМАЦІЙНИХ ЗАГРОЗ ДЛЯ УКРАЇНИ 86
19. Краснопольська Т. М. УЧАСТЬ МОЛОДІ У ФОРМУВАННІ ІНСТИТУТУ ПАРЛАМЕНТАРИЗМУ ЯК УМОВА ДЕМОКРАТИЧНОГО РОЗВИТКУ 92
20. Крікуненко С. В. СУЧАСНИЙ УКРАЇНСЬКИЙ МАЛЬОПИС ЯК ІСТОРИКО-КУЛЬТУРНИЙ АРТЕФАКТ 98
21. Кропівко В. В. ПОЛІТИЧНА РЕКЛАМА У ЦИФРОВОМУ СУСПІЛЬСТВІ: СКАСУВАТИ НЕ МОЖНА РЕГУЛЮВАТИ 102
22. Лагутін М. Р. ДИСКУРС НОВИХ МЕДІА ЩОДО НАЦІОНАЛЬНОГО ІНТЕРЕСУ 106
23. Левченко Я. В. ЦИФРОВА ПОЛІТИЧНА КОМУНІКАЦІЯ: ТРАНСФОРМАЦІЯ ТА ВИКЛИКИ 112
24. Лісовська О. В. Скриль С. А., МІЖНАРОДНЕ ГУМАНІТАРНЕ ПРАВО ТА ЗБРОЙНІ КОНФЛІКТИ СУЧАСНОСТІ 117
25. Макарець С. В. ФЕНОМЕН УКРАЇНСЬКОЇ МОДЕРНІЗАЦІЇ: ВІД НЕЗАВЕРШЕНИХ ПРОЕКТІВ МИНУЛОГО ДО СТРАТЕГІЇ МАЙБУТНЬОГО (ІСТОРИКО-ФІЛОСОФСЬКИЙ ТА ПОЛІТОЛОГІЧНИЙ АНАЛІЗ 121
26. Малишенко Л. О. ПУЛЬС СПРОТИВУ ТА ВІДРОДЖЕННЯ: УКРАЇНСЬКЕ ГРОМАДСЬКЕ СУСПІЛЬСТВО В ДОБУ ВІЙНИ 129

Список використаних джерел

1. Вебер М. Соціологія. Загальноісторичні аналізи. Політика / Пер. з нім. Олександр Погорілий. Київ: Основи, 1998. 34 с. (173)
2. Лібанова Е., Позняк О., Цимбал О. Масштаби та наслідки вимушеної міграції населення України внаслідок збройної агресії Російської Федерації. Демографія та соціальна економіка. 2022. № 2(48). С. 37-57. URL: <http://jnas.nbu.gov.ua/article/UJRN-0001339377>
3. Almond G., Verba S. *The Civic Culture. Political Attitudes and Democracy in Five Countries*. Princeton, 1963. P. 514.
4. Duszyk, M., Kaczmarek, P. *Wojna na Ukrainie i migracja do Polski: Outlook and Challenges*. *Intereconomics*. 2022. 57(3), p. 164-170. URL: <https://www.intereconomics.eu/contents/year/2022/number/3/article/the-war-in-ukraine-and-migration-to-poland-outlook-and-challenges.html>

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ ТА ГІБРИДНОЇ АГРЕСІЇ, ЛАНДШАФТ ІНФОРМАЦІЙНИХ ЗАГРОЗ ДЛЯ УКРАЇНИ

Кокорєв Олексій Вікторович,
д. політ.н., доцент,
в.о. завідувача кафедри журналістики,
соціальних комунікацій і ІТ-права
Державного університету
Інтелектуальних технологій і зв'язку
м. Одеса

В епоху глобальної цифровізації та стрімкого розвитку інформаційних технологій, інформаційна безпека перетворилася на один із наріжних каменів національної безпеки будь-якої держави. Для України, яка з 2014 року, і особливо інтенсивно після повномасштабного вторгнення Російської Федерації у 2022 році, перебуває в стані

безперервної гібридної війни, забезпечення інформаційної безпеки набуло екзистенційного значення. Інформаційний простір став не просто середовищем для комунікації, а повноцінним театром воєнних дій, де ворог активно застосовує дезінформацію, пропаганду, кібератаки та психологічні операції з метою підриву суверенітету, територіальної цілісності, обороноздатності та суспільної стійкості України [1].

Сучасне розуміння інформаційної безпеки охоплює захист інформаційних ресурсів, критичної інформаційної інфраструктури, протидію інформаційним загрозам та забезпечення сталого розвитку інформаційного суспільства на засадах захисту прав людини на інформацію та свободу слова, водночас мінімізуючи ризики від шкідливих інформаційних впливів [2, с. 15-18]. Нормативно-правову основу цієї сфери в Україні формують, зокрема, Закони України "Про інформацію", "Про захист інформації в інформаційно-комунікаційних системах", "Про основні засади забезпечення кібербезпеки України", а також ключові стратегічні документи, такі як Стратегія інформаційної безпеки України, затверджена у 2021 році [3], та Стратегія кібербезпеки України на 2021-2025 роки [4].

Україна щоденно стикається з комплексними та динамічними інформаційними загрозами, лівова частка яких генерується та спрямовується Російською Федерацією в рамках її гібридної агресії. Одним із ключових інструментів є масштабні дезінформаційні кампанії та пропаганда, спрямовані на дискредитацію української державності, її Збройних Сил, політичного керівництва, а також на розкол українського суспільства, поширення панічних настроїв та підриг довіри до державних інституцій та міжнародних партнерів [5, с. 45-52]. Ворожі наративи активно поширюються через соціальні мережі, месенджери, підконтрольні ЗМІ та мережі ботів, намагаючись маніпулювати суспільною думкою як всередині України, так і за її межами [6].

Невіддільною складовою інформаційної війни є кібератаки, що мають на меті порушення функціонування державних електронних інформаційних ресурсів, об'єктів критичної інфраструктури (енергетика, транспорт, фінансовий сектор), викрадення чутливих даних та здійснення актів кібершпигунства. З 2022 року фіксується значне зростання кількості та складності кібератак, зокрема типу DDoS, атак з використанням шкідливого програмного забезпечення (ransomware, wipers), а також фішингових кампаній [7]. Окрему небезпеку становлять операції впливу та психологічні операції (ПІСО), що використовують маніпулятивні техніки для впливу на емоційний стан та поведінку цільових аудиторій, підриву морального духу та здатності до опору [1].

З розвитком технологій з'являються і нові виклики, такі як використання технології дідфейк (deepfake) для створення фальсифікованих відео- та аудіоматеріалів, що можуть бути використані для дискредитації публічних осіб або поширення неправдивої інформації високого ступеня правдоподібності [8]. Застосування штучного інтелекту (ШІ) для автоматизації створення та поширення дезінформації, а також для більш таргетованого впливу на аудиторії, також становить серйозну загрозу, що потребує розробки нових методів протидії [9, с. 112-115].

В Україні функціонує розгалужена система державних органів, відповідальних за формування та реалізацію політики у сфері інформаційної та кібербезпеки. Координаційну роль відіграє Рада національної безпеки і оборони України (РНБОУ), яка розробляє та затверджує ключові стратегічні документи [Див.: 3; 4]. Безпосередню реалізацію завдань покладено на низку суб'єктів: Служба безпеки України (СБУ) відповідає за контррозвідувальний захист інформаційної безпеки держави, боротьбу з кібертероризмом та кібершпигунством; Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) є ключовим органом у сферах кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної

інфраструктури, технічного та криптографічного захисту інформації; Кіберполіція (Департамент кіберполіції Національної поліції України) займається розслідуванням кіберзлочинів та правопорушень в інформаційній сфері; Міністерство оборони України та Збройні Сили України розвивають власні спроможності для ведення інформаційного протистояння та захисту військових інформаційних систем та ін.

У 2021 році було створено Центр протидії дезінформації (ЦПД) при РНБОУ, головним завданням якого є виявлення, аналіз та протидія дезінформаційним кампаніям та ворожим наративам. У тому ж році – Національна рада України з питань телебачення і радіомовлення та новий Закон України "Про медіа" (набув чинності у 2023 році), що відіграють важливу роль у регулюванні медійного простору та протидії поширенню забороненої інформації, одночасно прагнучи забезпечити свободу слова.

Одним із пріоритетів є захист критичної інформаційної інфраструктури. Держава впроваджує комплекс заходів, спрямованих на підвищення її стійкості до кібератак, що включає нормативно-правове регулювання, технічні аудити, створення галузевих та ситуаційних центрів кібербезпеки. Розвиток національних спроможностей у сфері кібербезпеки також передбачає підготовку кваліфікованих кадрів, проведення регулярних навчань та кібервипробувань, а також стимулювання наукових досліджень.

Забезпечення інформаційної безпеки неможливе без активної участі громадянського суспільства та підвищення рівня медіаграмотності та критичного мислення населення. Освітні програми, тренінги та інформаційні кампанії, спрямовані на навчання громадян розпізнавати дезінформацію, маніпуляції та фейки, є важливим елементом формування суспільної стійкості до ворожих інформаційних впливів. Незалежні медіа та громадські організації, що займаються фактчекінгом та моніторингом інформаційного простору, роблять значний внесок у протидію дезінформації.

Важливим напрямом є стратегічні комунікації (StratCom), які передбачають проактивне поширення правдивої інформації про Україну, її позиції та дії, як всередині країни, так і на міжнародній арені.

Ефективні стратегічні комунікації допомагають формувати позитивний імідж держави, спростовувати ворожі наративи та мобілізувати міжнародну підтримку.

З огляду на транскордонний характер інформаційних та кіберзагроз, ключове значення має міжнародне співробітництво. Україна активно розвиває партнерство з країнами-членами НАТО та ЄС, міжнародними організаціями та приватними компаніями у сфері кібербезпеки та обміну інформацією про загрози]. Це включає спільні навчання, обмін досвідом, отримання технічної допомоги та координацію зусиль у протидії глобальним кіберзагрозам та дезінформаційним кампаніям. Важливу роль відіграє взаємодія з такими структурами, як Об'єднаний центр передових технологій з кібероборони НАТО (CCDCOE), Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) та іншими.

Попри значні зусилля, система інформаційної безпеки України стикається з низкою постійних та еволюціонуючих викликів. Це, зокрема, швидка технологічна еволюція загроз, що вимагає постійної адаптації засобів захисту; дефіцит висококваліфікованих кадрів у сфері кібербезпеки та інформаційних технологій; необхідність значних фінансових ресурсів для модернізації інфраструктури та закупівлі новітніх технологій; а також складність у дотриманні балансу між посиленням заходів безпеки та захистом фундаментальних прав і свобод людини, зокрема свободи слова та доступу до інформації [2, с. 30-35].

Стратегічними пріоритетами на майбутнє є подальше зміцнення національних кібернетичних спроможностей, зокрема проактивного виявлення та реагування на кіберінциденти; вдосконалення законодавства у сфері інформаційної безпеки з урахуванням новітніх технологій (ШІ, Інтернет речей); посилення захисту критичної інфраструктури; розвиток

системи підготовки фахівців; розширення міжнародного співробітництва; та підвищення загального рівня цифрової грамотності та інформаційної гігієни громадян [3; 4]. Важливим завданням залишається розробка ефективних механізмів протидії новим формам дезінформації, включаючи діпфейки та маніпуляції, керовані штучним інтелектом.

Отже, інформаційна безпека є динамічною сферою, що вимагає постійних зусиль, адаптації та інновацій. Для України, що перебуває на передовій гібридної війни, ефективна система інформаційної безпеки є не лише запорукою захисту національних інтересів, але й умовою виживання та успішного розвитку в сучасному світі. Комплексний підхід, що поєднує технологічні рішення, законодавчі ініціативи, освітні програми та міжнародну співпрацю, є ключем до побудови стійкого та захищеного інформаційного простору.

Список використаних джерел:

1. Довгань О. Д., Чернега В. В. Інформаційно-психологічні операції в умовах гібридної війни: сутність та засоби протидії. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Вип. 77. С. 210–215.
2. Корж Є. Ю., Петров М. А. Сучасні виклики інформаційній безпеці України та шляхи їх подолання. *Юридичний науковий електронний журнал.* 2022. № 5. С. 15–19.
3. Про рішення Ради національної безпеки і оборони України від 1 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.2021 р. № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41005>
4. Про рішення Ради національної безпеки і оборони України від 1 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 р. № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-39797>

5. *Жарінов О. В. Дезінформаційні кампанії як інструмент гібридно агресії Російської Федерації проти України. Вісник Національного університету "Львівська політехніка". Серія: Юридичні науки. 2022. № 2(34). С. 44–53.*
6. *Dubov D., Ostapets Y. Countering Disinformation in Ukraine: State Policies and Civil Society Initiatives (2021-2023). Kyiv: Razumkov Centre, 2023. 120 p..*
7. *Державна служба спеціального зв'язку та захисту інформації України. Звіт про стан кіберзахисту України за 2023 рік. Київ, 2024.*
8. *Ткаченко В. О. Використання технології дінфейк в інформаційних війнах: загрози та перспективи протидії. Інформаційна безпека людини, суспільства, держави. 2023. № 1(39). С. 67–74.*
9. *Мельник С. В. Штучний інтелект в інформаційному протистборстві нові можливості та ризики для національної безпеки. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник "Повітряне і космічне право". 2022. № 3(68). С. 110–118.*

УЧАСТЬ МОЛОДІ У ФОРМУВАННІ ІНСТИТУТУ ПАРЛАМЕНТАРИЗМУ ЯК УМОВА ДЕМОКРАТИЧНОГО РОЗВИТКУ

*Краснопольська Тетяна Миколаївна,
к.політ.н., доцент,
доцент кафедри політичних теорій
Національний університет «Одеська юридична академія»
м. Одеса*

У Європі та Україні молодь бере активну участь у політичному житті, сприяючи оновленню політичних інституцій та впровадженню інноваційних підходів до управління державою. Її активна участь