РОЗДІЛ 1
ТЕОРІЯ ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

УДК 351.851:004.738.5
DOI https://doi.org/10.51547/ppp.dp.ua/2025.3.1

Ахмедова Олена Олегівна,
доктор наук з державного управління, доцент кафедри туризму
Харківського національного економічного університету імені Семена Кузнеця
ORCID ID: 0000-0003-1573-7710

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ПУБЛІЧНОЇ ПОЛІТИКИ ПРОТИДІЇ КОЛАБОРАЦІОНІЗМУ

INFORMATION SECURITY AS PART OF PUBLIC POLICY AGAINST COLLABORATIONISM

У статті проаналізовано сучасні виклики інформаційній безпеці України в умовах повномасштабної війни та гібридної агресії з боку російської федерації. Визначено, що інформаційна безпека є невід'ємним елементом публічної політики, оскільки саме через інформаційний простір реалізуються ключові інструменти дезінформації, пропаганди та психологічного впливу на населення, що, у свою чергу, викликає лояльність певної частини громадян до ворожої країни. Обґрунтовано, що ефективна протидія колабораціонізму неможлива без системної координації державних інституцій, зокрема Державної служби спеціального зв'язку та захисту інформації України, Міністерства цифрової трансформації, Центру стратегічних комунікацій та інформаційної безпеки, а також Центру протидії дезінформації, кожна з яких виконує чітко обумовлені функції та задачі. Досліджено, що у процесі реалізації публічної політики важливим є формування правових механізмів відповідальності за співпрацю з ворогом, а також запровадження інструментів стратегічних комунікацій, спрямованих на посилення стійкості суспільства. Визначено особливу роль кримінально-правових засобів у протидії колабораційній діяльності, водночас підкреслено значення профілактичних та просвітницьких заходів, що формують критичне мислення та інформаційну гігієну громадян. З'ясовано, що традиційні етапи розвідки і виявлення загроз поєднуються з потоками даних, що генеруються цивільними особами, а потім перевіряються супутниковими технологіями. Такий підхід радикально скорочує терміни визначення потенційних небезпек та прийняття необхідних рішень. В той же самий час постають питання щодо дотримання прав людини, етичності та правомірності такого контролю, що додають викликів демократичному устрою держави. Наголошено, що забезпечення інформаційної безпеки в умовах війни вимагає інтеграції правових, організаційних і технологічних інструментів, що дозволяє зміцнити національну безпеку, знизити ризики внутрішньої дестабілізації та забезпечити ефективну публічну політику протидії колабораціонізму.

Ключові слова: *інформаційна безпека, публічна політика, колабораціонізм, колабораційна діяльність, стратегічна комунікація, дезінформація, гібридна війна, цифрова держава.*

The contemporary challenges to Ukraine's information security in the context of full-scale war and hybrid aggression by the russian federation have been analysed in the paper. It has been identified that information security constitutes an integral component of public policy, as the information space serves as a channel for implementing key instruments of disinformation, propaganda, and psychological influence on the population. It has been substantiated that effective counteraction to collaborationism is impossible without systemic coordination among state institutions, in particular the State Service of Special Communications and Information Protection of Ukraine, the Ministry of Digital Transformation, the Centre for Strategic Communications and Information Security, and the Centre for Countering Disinformation, each performing clearly defined functions and tasks. It has been researched that in the process of public policy implementation, the development of legal mechanisms of responsibility for cooperation with the enemy is crucial, along with the introduction of strategic communication tools aimed at strengthening societal resilience. The special role of criminal-legal instruments in countering collaborative activities is determined, while the significance of preventive and educational measures fostering critical thinking and information hygiene among citizens has been emphasized. It has been clarified that traditional stages of intelligence and threat detection are combined with data flows generated by civilians and subsequently verified through satellite technologies, radically reducing the timeframe for identifying potential threats and making informed decisions. At the same time, questions arise regarding the observance of human rights, the ethics and legitimacy of such monitoring, which pose additional challenges to the democratic structure of the state. It

has been concluded that ensuring information security during wartime requires the integration of legal, organizational, and technological instruments, which strengthens national security, reduces the risks of internal destabilization, and ensures an effective public policy of countering collaborationism.

Key words: *information security, public policy, collaborationism, collaborationist activity, strategic communication, disinformation, hybrid warfare, digital state.*

Постановка проблеми. В умовах сучасних викликів кожна країна, незалежно від ступеня політичних, економічних чи соціальних проблем, має вирішувати питання інформаційної безпеки, яка є ключовою у боротьбі з інформаційними впливами, дезінформацією, небажаною пропагандою, адже наявні технологічні досягнення та можливості штучного інтелекту, який стає все розумнішим, дозволяють створювати надзвичайно реалістичний, але підроблений текстовий, відео та аудіо матеріал, який за своєю якістю майже не відрізняється від оригінального та використовуються для поширення брехні, створення певних політично спрямованих настроїв, щоб зашкодити репутації, усунути конкурентів, вимагати кошти тощо. Загальновідомим став термін «діпфейк» (з англ. «deepfake» – «глибока підробка»), який характеризує згенерований нейромережами контент на основі глибокого навчання з повною імітацією голосу, обличь, поведінки людей, який подекуди важко виявити навіть спеціалісту. В 2025 році кількість діпфейк-атак у світі зросла до п'яти на одну хвилину, а число підроблених цифрових документів на 244%; у першому кварталі поточного року вже відбулося (тільки зафіксованих) 179 політичних інцидентів [1].

Ситуація значно загострюється в країнах, де відбуваються політичні та економічні трансформації, соціальні зіткнення, воєнні, терористичні акти та інші форми насильницького протистояння, адже вплив ворожих інформаційно-психологічних впливів на конкретну цільову аудиторію дозволяє маніпулювати громадською думкою та сприяє формуванню цілого прошарку лояльного ворогу населення, який добровільно співпрацює на користь загарбникам проти власної держави. Така активність відома як колабораціонізм чи колабораційна діяльність. Для України, яка знаходиться у стані війни, проблема інформаційної безпеки, наряду з питаннями національної оборони, територіальної цілісності та економічної стабільності, виходить на перший план. У цьому контексті важливою є цілеспрямована просвітницька, навчальна та пропагандистська робота з населенням, адже велика кількість колабораціоністів свідчить про недостатній і незадовільний інформаційний вплив держави та публічної влади в цілому. Саме тому актуальність даної теми є беззаперечною.

Аналіз останніх досліджень і публікацій. Війна в Україні стала не тільки наймасштабнішою в Європі після Другої світової, а й такою, що далеко виходить за межі «класичної» війни як за методами ведення, так і ступенем впливу на всі сфери суспільного та політичного життя. Закордонні і вітчизняні дослідники, кожен в своїй площині інтересів, вивчають сучасну гібридну війну, яка є прикладом поєднання і використання як традиційних, так і новітніх технологій не тільки у воєнній сфері, а й у всіх напрямках боротьби з ворогом.

У контексті статті заслуговують на увагу роботи, що досліджують походження та еволюцію поняття інформаційної безпеки, сутність та роль інформаційної безпеки як елементу національної безпеки держави, особливості її впровадження у політичному та публічному вимірах (Новицький, В. А. (2024); М. О. Шевчук. (2023); Милосердна І. М. (2024) та роль інформаційної політики держави у попередженні колабораціонізму (Orlov, V. (2024); Syniuk O. et al (2024).

Для світу є унікальним український досвід побудови системи стратегічних комунікацій та протидії дезінформації під час війни, регулювання інформаційних потоків, реагування на використання штучного інтелекту для створення дезінформації (Danchenkova O. (2025); Marushchak, A. et al (2025). В той же час інтеграція Україною передових технологій, таких як супутникове дистанційне зондування, системи ситуаційної обізнаності, розпізнавання обличчя та голосу тощо, які використовуються в дезінформаційних кампаніях, мають значні стратегічні переваги в обороні, але несуть в собі великі ризики для демократичних норм і прав людини (Mysyshyn, A. (2024).

Незважаючи на достатню увагу науковців до зазначених проблем, питання інформаційної безпеки як складової публічної політики протидії колабораціонізму залишається актуальними і таким, що потребують постійного переосмислення і адаптації до сучасних реалій.

Постановка завдання. Метою статті є дослідження забезпечення інформаційної безпеки як складової публічної політики протидії колабораціонізму, що

Виклад основного матеріалу. За часів незалежності в Україні сформувалася державна сис-

тема забезпечення інформаційної безпеки, яка на даний момент складається з таких ключових органів – Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ), утвореної на виконання Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» 23 лютого 2006 року, Міністерства цифрової трансформації України, утвореного шляхом реорганізації Державного агентства з питань електронного урядування України 29 серпня 2019 року, Центру стратегічних комунікацій та інформаційної безпеки (ЦСКІБ) при Міністерство культури та стратегічних комунікацій України (заснованого ще 31 березня 2021, але у зв'язку з реорганізацією Міністерства на початку 2025 року ЦСКІБ також перереєстрованого), Центру протидії дезінформації при Раді Національної Безпеки і Оборони України (РНБО), створеного Указом президента від 7 травня 2021 року. Багаторівнева структура дозволяє державі протистояти сучасним викликам на всіх напрямках, поєднуючи технічні, комунікаційні, аналітичні інструменти. Кожен з органів виконує свою функцію у протидії дезінформації, формуванні публічної інформаційної політики і, як наслідок, боротьби з колабораційною діяльністю.

Державна служба спеціального зв'язку та захисту інформації України [10] являється опорою національної цифрової безпеки та кіберстійкості, забезпечуючи захист державних органів від технологічних та інформаційних атак, у тому числі таких, що мають колабораційне походження. Урядова команда CERT-UA постійно блокує фішингові кампанії, які передаються через колаборантів у регіонах (наприклад, розсилання фейкових судових повісток із зараженими файлами). У 2022-2025 роках ДССЗІ фіксувала та публічно повідомляла про спроби ворога використати колаборантів для роботи у держорганах для внутрішнього саботажу ІТ-систем. Команда ДССЗІ розробляє та впроваджує стандарти кіберзахисту, які мінімізують людський фактор як слабку ланку, що може бути використана у процесі колабораційної діяльності.

Головною задачею Міністерства цифрової трансформації України [11] є формування та реалізація державної політики у сфері цифровізації, електронного урядування, цифрової економіки та інновацій, навчання населення медіаграмотності та просування ідеї «держави в смартфоні». Зважаючи на розвиток електронного врядування, питання кіберзахисту і безпеки даних є надважливими, тому можна зазначити, що Міністерство виконує роль цифрового щита, забезпечуючи підтримкою всю технічну інфраструктуру, що ускладнює поширення дезінформації і мінімізує її використання колаборантами.

Основні функції Центру стратегічних комунікацій та інформаційної безпеки при Міністерство культури та стратегічних комунікацій України [12] полягають в формуванні публічної політики держави, що сприятимуть її інформаційній стійкості, запобіганню поширення пропаганди та маніпуляцій, особливо таким, що пов'язані із колаборайційною діяльністю. Центр представляє собою інформаційний фронт, який створює стратегічну комунікацію і аналітику та покликаний нівелювати ворожі ІПСО та атаки.

Важливу роль у боротьбі за інформаційну безпеку країни відіграє Центр протидії дезінформації при РНБО [13], серед основних задач якого виділимо наступні: виявлення і протидія маніпуляціям і фейкам, аналіз інформаційних загроз, координація дій державних органів у сфері стратегічних комунікацій; просвітницька діяльність для підвищення рівня медіаграмотності суспільства. Зважаючи на те, що колаборайційна діяльність значною мірою ґрунтується на перекручених та спотворених фактах, політичній пропаганді, представленні окупаційної влади як легітимної, робота Центру є важливим елементом для створення інформаційного бар'єру для ворожих атак, виявлення інформаційної співпраці з ворогом та створення єдиного державного комунікаційного простору, що є невід'ємною частиною функціонування держави в воєнних умовах.

Офіс Генерального прокурора України впроваджує кримінально-правове переслідування злочинів колабораціонізму, готує обвинувачення, виносить вироки за справами. Важливим етапом у забезпеченні інформаційної безпеки держави стали зміни, внесені до статей Кримінального кодексу України (зокрема, в Особливу частину «Кримінальні правопорушення проти основ національної безпеки України», ст. 111, 111^1, 111^2 ККУ) [14]. Вони були прийняті у відповідь на зростаючі загрози в період війни та інформаційні впливи, спрямовані на порушення державної цілісності та національної безпеки України. Дані статті визначають склад та специфіку правопорушень, пов'язаних з державною зрадою, колаборайційною діяльністю, пособництвом державі-агресору, конкретизують види співпраці з окупаційною владою, особливості інформаційно-пропагандистської роботи на користь країни-загарбника, визначають роль у створенні незаконних органів влади на окупованій території. Зміни набрали чинності в березні (111^1 – «Колаборайційна діяль-

ність») – квітні (111^2 – «Пособництво державі-агресору») 2022 року. Необхідно зазначити, що дані зміни мали бути прийняті ще у 2014 році, коли розпочалася анексія українських земель зі сторони російської федерації і значна кількість українців висловила підтримку таким діям.

Узагальнивши статистичну інформацію Офісу Генерального прокурора України [15], з'ясовано, що з моменту внесення змін до закону і на початок серпня поточного року в країні було зареєстровано 22757 злочинів проти національної безпеки держави, серед яких 2739 – посягання на територіальну цілісність і недоторканність України (стаття 110 ККУ), 4502 – державна зрада (стаття 111 ККУ), 10175 – колабораційна діяльність (стаття 111^1 ККУ), 1573 – пособництво державі-агресору (стаття 111^2 ККУ), 508 – диверсія (стаття 113 ККУ), 3260 – інші злочини. Вироки за подібні злочини ще не є масовими, враховуючи, що частина з них винесена заочно, тим не менш, наявність відповідальності за подібні дії повинна постійно транслюватися засобами масової інформації з метою формування у суспільстві стійкого розуміння невідворотності покарання за неправові дії та підвищення рівня свідомості громадян.

У таблиці 1 представлено коротку порівняльну характеристику ключових державних органів та установ, що впливають на боротьбу з колабораційною діяльністю через інформаційний вимір:

Окремо підкреслимо міжнародну допомогу у впровадженні захисту інформаційного простору України, яка надзвичайно швидко адаптувала такі комерційні технології як супутниковий зв'язок Старлінк, Molfar OSINT, Sherlock, See All та інші для пошуку і фільтрування профілів у соціальних мережах, цілий кластер технологій Brave1, серед яких AI-проекти з повного аналізу аудіо-відео контенту, перехоплення російських розмов (Primer AI, Collective Defense, AI Fusion Center) та ідентифікації цілей, інші інструменти для повідомлення про будь-які порушення і підтримання обміну даними в режимі реального часу. Як бачимо, традиційні етапи розвідки і виявлення загроз поєднуються з потоками даних, що генеруються цивільними особами, а потім перевіряються супутниковими технологіями. Такий підхід радикально скорочує терміни визначення потен-

Таблиця 1

Органи влади у забезпеченні інформаційної безпеки держави і реагуванні на колабораційну діяльність

№	Установа	Підпорядкування	Основні функції	Роль у боротьбі з колабораціонізмом	Сучасні технологічні інструменти
1	Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ)	Спеціалізований центральний орган виконавчої влади	Формує і впроваджує державну політику у сфері захисту державних ІТ-ресурсів, урядового зв'язку, криптозахисту, співпрацює з міжнародними партнерами для більшої кіберстійкості України	Координує національну систему інформаційної безпеки, нейтралізує тисячі атак на державні органи, енергетику, банки	CERT-UA (реагування на комп'ютерні інциденти), OSINT-платформи і інструменти, фактчекінгові організації (StopFake, VoxCheck, Bellingcat тощо)
2	Міністерства цифрової трансформації України (Мінцифри)	Центральний орган виконавчої влади	Цифрові сервіси держави, кіберзахист цифрової інфраструктури, цифрова грамотність населення	Перекриває технічні канали для ворожої пропаганди, унеможливлює використання державних цифрових платформ для колабораційної діяльності	«Дія», кіберзахист державних реєстрів, чат-бот «єВорог», BRAVE1 (кластер розвитку військових та інформаційних технологій)
3	Центр стратегічних комунікацій та інформаційної безпеки (ЦСКІБ)	Міністерство культури та стратегічних комунікацій України	Створення та поширення державних стратегічних наративів та підтримка комунікації під час криз, інформаційна безпека	Протидіє маніпуляціям та дезінформації	Моніторингові платформи, фактчекінг, системи аналізу соцмереж
4	Центр протидії дезінформації (ЦПД)	РНБО	Контроль інформаційного простору, нейтралізація кампаній з дезінформації та пропаганди, аналітика для Президента та РНБО	Виявляє джерела, напрямки і масштаби інформаційних атак, російське ІПСО у соцмережах	Big Data аналіз, автоматизовані системи (AI) відстеження діпфейків, алгоритми виявлення бот-мереж

Джерело: складено автором на основі [10-13]

ційних небезпек та прийняття необхідних рішень. Але в той же самий час постають питання щодо дотримання прав людини, етичності та правомірності такого контролю, що стане темою подальших досліджень.

Висновки. Інформаційна безпека в умовах сучасної гібридної війни набула значення стратегічного пріоритету, безпосередньо впливаючи на стійкість держави та суспільства. Колабораційна діяльність в Україні, що ґрунтується не лише на політичних чи військових чинниках, але й на маніпулятивному використанні інформації, робить питання інформаційного захисту ключовим у публічній політиці.

В Україні вже сформовано багаторівневу систему протидії дезінформації, що включає ДССЗЗІ, Міністерство цифрової трансформації, Центр стратегічних комунікацій та інформаційної безпеки, Центр протидії дезінформації та інші структури. Їхня діяльність охоплює кіберзахист, стратегічні комунікації, виявлення та нейтралізацію інформаційних атак, а також кримінальне переслідування колаборантів.

Одночасно, викликом для публічної політики в Україні є подальше грамотне проведення роз'яснювальної та просвітницької роботи серед населення для підвищення рівня соціальної відповідальності, покращання медіаграмотності та протистояння дезінформації, особливо серед найбільш вразливих категорій населення – мешканців прифронтових територій, людей похилого віку та молоді.

REFERENCES:

1. Deepfake statistics (2025): 25 new facts for CFOs. (2025). Eftsure. Retrieved from https://www.eftsure.com/statistics/deepfake-statistics/?utm_source

2. Novyts'kyi, V. A. (2024). Geneza poniattia «informatsiina bezpeka»: pokhodzhennia ta stanovlennia [Genesis of the concept of "information security": origin and formation]. Vcheni zapysky TNU imeni V. I. Vernads'koho. Seriia: Publichne upravlinnia ta administruvannia, 35(74)(4), 53–62. https://doi.org/10.32782/TNU-2663-6468/2024.4/06 [in Ukrainian].

3. Shevchuk, M. O. (2023). Do pytannia genezy poniattia informatsiinoi bezpeky yak skladovoi natsional'noi bezpeky [On the issue of the genesis of the concept of information security as a component of national security]. Naukovyi visnyk Uzhhorods'koho natsional'noho universytetu. Seriia: Pravo, 2(78). https://doi.org/10.24144/2307-3322.2023.78.2.21 [in Ukrainian].

4. Myloserdna, I. M. (2024). Informatsiina bezpeka yak element natsional'noi bezpeky: teoretychnyi vymir ta osoblyvosti vprovadzhennia [Information security as an element of national security: Theoretical dimension and implementation features]. Politychni problemy mizhnarodnykh system ta hlobal'noho rozvytku, 4, 179–185. https://doi.org/10.24195/2414-9616.2024-4.26 [in Ukrainian].

5. Orlov, V. (2024). Counteracting and preventing collaboration activities during the period of Russia's armed aggression against Ukraine. SSRN. https://doi.org/10.2139/ssrn.4898419

6. Syniuk, O., Deputat, D., Vyshnevska, I., Volkovynska, V., Chervonna, V., & Yelihulashvili, M. (2024). Survival or crime: How Ukraine punishes collaborationism? Analytical report (Ed. Lunova A.). Kyiv. Retrieved from https://zmina.ua/wp-content/uploads/sites/2/2025/04/colaboratz_eng_web.pdf

7. Danchenkova, O. (2025). Ukraine's hard-won approach to strategic communications and counter-disinformation: Lessons for Europe and beyond. Tech Policy Press. Retrieved from https://techpolicy.press/ukraines-hardwon-approach-to-strategic-communications-and-counterdisinformation-lessons-for-europe-and-beyond/

8. Marushchak, A., Petrov, S., & Khoperiya, A. (2025). Countering AI-powered disinformation through national regulation: Learning from the case of Ukraine. Frontiers in Artificial Intelligence, 7, Article 1474034. https://doi.org/10.3389/frai.2024.1474034

9. Mysyshyn, A. (2024). Advanced technologies in the war in Ukraine: Risks for democracy and human rights. ReThink.CEE Fellowship Paper. German Marshall Fund of the United States. Retrieved from https://www.gmfus.org/sites/default/files/2024-10/Mysyshyn%20-%20Ukraine%20war%20tech%20-%20paper.pdf

10. Derzhavna sluzhba spetsial'noho zv'iazku ta zakhystu informatsii Ukrainy. (n.d.). Ofitsiinyi vebsait [State Service of Special Communications and Information Protection of Ukraine. Official website]. Retrieved from https://cip.gov.ua/ua [in Ukrainian].

11. Ministerstvo tsyfrovoi transformatsii Ukrainy. (n.d.). Ofitsiinyi vebsait [Ministry of Digital Transformation of Ukraine. Official website]. Retrieved from https://thedigital.gov.ua/ [in Ukrainian].

12. Ministerstvo kul'tury ta stratehichnykh komunikatsii Ukrainy. (n.d.). Ofitsiinyi vebsait [Ministry of Culture and Strategic Communications of Ukraine. Official website]. Retrieved from https://mcsc.gov.ua/ [in Ukrainian].

13. Ofitsiinyi visnyk Prezydenta Ukrainy. (2021, May 7). Pytannia Tsentru protydii dezinformatsii: Ukaz Prezydenta Ukrainy № 187/2021 [Issues of the Center for Countering Disinformation: Decree of the President of Ukraine No. 187/2021]. Retrieved from https://zakon.rada.gov.ua/go/187/2021 [in Ukrainian].

14. Verkhovna Rada Ukrainy. (2001). Kryminal'nyi kodeks Ukrainy [Criminal Code of Ukraine]. Vidomosti Verkhovnoi Rady Ukrainy (VVR), № 25–26, st.131. Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text [in Ukrainian].

15. Ofis Heneral'noho prokurora Ukrainy. (n.d.). Ofitsiinyi vebsait [Office of the Prosecutor General of Ukraine. Official website]. Retrieved from https://gp.gov.ua/ [in Ukrainian].