АНАЛІТИЧНИЙ ЦЕНТР
СУЧАСНОЇ ГУМАНІТАРИСТИКИ

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО

МОНОГРАФІЯ



Інформаційна війна: поняття, зміст, види та засоби

Вплив інформаційних війн на економіко-політичні, соціальні процеси у світі та окремій країні

Інформаційна боротьба: особливості та структурні елементи

Культура, наука, право, освіта на захисті людини від деструктивного впливу інформаційної зброї

Спеціальні інформаційно-психологічні операції: сутність, етапи, методи проведення

Інформаційна безпека та контрпропаганда в умовах російсько-української війни

АНАЛІТИЧНИЙ ЦЕНТР СУЧАСНОЇ ГУМАНІТАРИСТИКИ

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО

Монографія

Харків
«Право»
2026

DOI: https://doi.org/10.31359/9786178852085
УДК 14+316+32+33+34+35
І-74

Авторський колектив:
Л. М. Алексеєнко, доктор економічних наук, професор; *О. М. Іванченко*, доктор юридичних наук, доцент; *У. В. Ільницька*, кандидат політичних наук, доцент; *О. В. Квасниця*, кандидат економічних наук, доцент; *Н. О. Коннова*, кандидат філософських наук, доцент; *О. С. Копитова*, доктор юридичних наук, старший дослідник; *О. В. Кравченко*, доктор історичних наук, доцент; *К. В. Настояща*, доктор соціологічних наук, доцент; *М. П. Требін*, доктор філософських наук, професор; *Н. В. Федіна*, кандидат юридичних наук, доцент; *Т. О. Чернишова*, кандидат філологічних наук, доцент; *Л. В. Чупрій*, доктор політичних наук, професор

Рецензенти:
Г. М. Куц – доктор політичних наук, професор (Харківський національний педагогічний університет імені Г. С. Сковороди);
В. І. Палагута – доктор філософських наук, професор (Національний технічний університет «Дніпровська політехніка»);
І. В. Процюк – доктор юридичних наук, професор (Національний юридичний університет імені Ярослава Мудрого)

Рекомендовано до видання вченою радою
ГО «Аналітичний центр сучасної гуманітаристики»
(протокол № 4 від 17 липня 2026 р.)

Інформаційна війна та її вплив на суспільство : монографія / І-74 [Л. М. Алексеєнко, О. М. Іванченко, У. В. Ільницька та ін.] ; Аналіт. центр сучас. гуманітаристики. – Харків : Право, 2026. – 506 с. – DOI: https://doi.org/10.31359/9786178852085.

ISBN 978-617-8852-08-5

Колективну монографію присвячено дослідженню теоретичних, методологічних і практичних основ феномену інформаційної війни, розкрито її поняття, сутність, зміст. Особливу увагу приділено розумінню сутності та специфіки когнітивної війни як концепту сучасного гуманітарного протиборства. Проаналізовано види та засоби ведення інформаційної війни, особливості та структурні елементи інформаційної боротьби, сутність, етапи, методи проведення спеціальних інформаційно-психологічних операцій. Розглянуто вплив інформаційних війн на економіко-правові, соціальні процеси у світі та окремій країні. Особливу увагу приділено інформаційній безпеці, контрпропаганді, захисту людини від деструктивного впливу інформаційної зброї в умовах російсько-української війни.

УДК 14+316+32+33+34+35

© Алексеєнко Л. М., Іванченко О. М., Ільницька У. В. та ін., 2026
© ГО «Аналітичний центр сучасної гуманітаристики», 2026
© ТОВ «Видавничий дім «Право», 2026

ISBN 978-617-8852-08-5

Зміст

Розділ 1
Інформаційна війна: поняття, зміст, види та засоби
1.1. Інформаційна війна в турбулентному світі: теоретико-методологічні засади (*Требін М. П., Коннова Н. О.*)..... 5
Список використаних джерел. 41
1.2. Трансформація змісту інформаційної боротьби: генезис, форми та методи (*Требін М. П., Коннова Н. О.*).. 47
Список використаних джерел. 79
1.3. Сутність та специфіка когнітивної війни як концепту сучасного гуманітарного протиборства (*Требін М. П., Коннова Н. О.*) 84
Список використаних джерел. 120
1.4. Феномен когнітивної війни в доктринальному дискурсі НАТО (*Чернишова Т. О.*) 124
Список використаних джерел. 154

Розділ 2
Спеціальні інформаційно-психологічні операції: сутність, етапи, методи проведення
2.1. Теоретико-методологічні засади та сутність спеціальних інформаційно-психологічних операцій (ІПсО) у контурі гібридних конфліктів (*Требін М. П., Коннова Н. О.*)..... 158
Список використаних джерел. 191
2.2. Архітектура, етапи проєктування та методи реалізації сучасних ІПсО в цифровому медіасередовищі (*Требін М. П., Коннова Н. О.*) 195
Список використаних джерел. 230
2.3. Північнокорейська тематика в спеціальних інформаційно-психологічних операціях російсько-української війни (*Чупрій Л. В., Настояща К. В.*)..... 234
Список використаних джерел. 247

Розділ 3
Вплив інформаційних війн на економіко-правові, соціальні процеси у світі та окремій країні
3.1. Інформаційна війна як фактор трансформації права (*Копитова О. С.*).. 250
Список використаних джерел. 292

3.2. Інформаційно-безпекові імперативи цифрових і фондових інновацій у сфері публічного управління, фінансів, банків і страхування: міжнародні та національні бізнес-комунікації (*Алексеєнко Л. М.*).. 297
Список використаних джерел. 323
3.3. Інформаційно-комунікаційні механізми політики згуртованості економічного розвитку територіально-господарських систем: пріоритети поведінкових фінансів та масштабування фінансової грамотності в умовах євроінтеграції (*Квасниця О. В.*) 334
Список використаних джерел. 366

Розділ 4
Інформаційна безпека та контрпропаганда в умовах російсько-української війни

4.1. Культура, наука, право, освіта на захисті людини від деструктивного впливу інформаційної зброї (*Іванченко О. М.*) 369
Список використаних джерел. 407
4.2. Стратегічні комунікації як механізм формування системи інформаційної безпеки та протидії інформаційним викликам і загрозам (*Ільницька У. В.*). 411
Список використаних джерел. 432
4.3. Особливості забезпечення інформаційної безпеки органами державного адміністрування в умовах правового режиму воєнного стану (*Федіна Н. В.*) 438
Список використаних джерел. 469
4.4. Інформаційна безпека та контрпропаганда в умовах російсько-української війни: стратегії та досвід України і Польщі (*Кравченко О. В.*). 474
Список використаних джерел. 498

Авторський колектив.....503

46. Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії.* 2024. Вип. 31. С. 1–11. DOI: https://doi.org/10.5281/zenodo.11381101
47. Штогрін І. Якою має бути інформаційна політика України в умовах війни? *Радіо Свобода*. 28.02.2017. URL: https://www. radiosvoboda.org/a/28338927.html

4.4. Інформаційна безпека та контрпропаганда в умовах російсько-української війни: стратегії та досвід України і Польщі

Кравченко Олена Валентинівна
доктор історичних наук, доцент
професор кафедри міжнародних відносин і політичної філософії
Харківський національний економічний університет імені Семена Кузнеця

Повномасштабне вторгнення російської федерації проти України актуалізувало питання необхідності забезпечення національної безпеки, в тім інформаційної безпеки та здійснення контрпропаганди щодо суперника. Під інформаційною безпекою розуміється захист життєво важливих інтересів особи, суспільства і держави від загроз в інформаційній сфері[1].

Інформаційна безпека в умовах російсько-української війни полягає у захисті національного інформаційного простору та свідомості громадян від ворожих маніпуляцій. Контрпропаганда передбачає викриття російських фейків, блокування ворожих ресурсів та проактивне поширення правдивої інформації для збереження стійкості суспільства.

Сутність поняття «інформаційна безпека» досліджували науковці В. Горовий, Б. Кормич, О. Онищенко, О. Панченко, Я. Гмир та ін., аналізували основні загрози інформаційній безпеці, характеризували

[1] Див.: Литвиненко О. В. Інформаційна безпека. *Енциклопедія Сучасної України.* 2011. DOI: 10.5281/zenodo.19971510.

стадії підвищення цієї безпеки, законодавче підґрунтя інформаційної безпеки держави, визначали механізми протидії дезінформації тощо. Існують поодинокі дослідження шляхів поширення та протидії дезінформації. Так, Б. Миколайчук виокремлює критерії оцінки дезінформації, основні шляхи протидії дезінформації. Ю. Мазур, В. Крижановський наводять найпоширеніші ознаки фейкових новин. Однак на сьогодні відсутні системні дослідження проблем забезпечення інформаційної безпеки в умовах війни, характеристика основних механізмів протидії дезінформації в умовах військових дій.

Інформаційна безпека в державній політиці в умовах конфліктів вивчається в роботах вітчизняних науковців. Проблема ця знаходить своє відображення у різних аспектах в публікаціях вітчизняних дослідників, серед яких можна відзначити праці К. І. Бєлякова, М. І. Дзямулич, О. Д. Добрянської, А. М. Новицького, Г. В. Онкович, Н. Б. Новицької, О. О. Пунди, Т. Ю. Ткачука, В. С. Цимбалюка, О. О. Чеботарьова, М. Швець та інших[1].

Л. І. Мазуренко проаналізувала механізми протидії фейковій інформації в умовах воєнного стану, виділила принципи здійснення інформаційної безпеки та складові інформаційної безпеки, розкрила можливі напрями вдосконалення забезпечення інформаційної безпеки[2]. О. В. Прудникова досліджувала інформаційну безпеку українського суспільства під час російської агресії в інформаційно-технічному та ціннісно-світоглядному контекстах[3].

О. С. Бодрук зазначає, що існує три основні підходи до визначення сутності поняття «інформаційна безпека» – компонент державної безпеки; захищеність інформаційного середовища та державних ін-

[1] Див.: Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії*. 2024. Вип. 31. DOI: https://doi.org/10.5281/zenodo.11381101.

[2] Див.: Мазуренко Л. І. Інформаційна безпека в умовах російсько-української війни : виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Питання політології.* 2022. Вип. 42. С. 50–57. DOI: https://doi.org/10.26565/2220-8089-2022-42-08.

[3] Див.: Прудникова О. В. Інформаційна безпека вітчизняного суспільства в умовах російсько-української війни. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія*. 2025. Т. 2. № 65. С. 71–81. DOI: https://doi.org/10.21564/2663–5704.65.331715.

тересів від гіпотетичних загроз; стан системи, що може гарантувати дотримання бажаних безпекових параметрів[1].

Л. Чистоклетов та С. Обрембальський здійснили правовий аналіз забезпечення інформаційної безпеки в період російсько-української війни, її правову регламентацію, законодавче закріплення та міжнародний вплив на загальне формування інформаційної безпеки[2].

М. Матковський виділив такі загрози для інформаційної безпеки під час російсько-української війни, як дезінформація, кібератаки, вплив на громадську думку через медіа та соціальні мережі, що можуть призводити до дестабілізації суспільства, порушення довіри до влади та загрози національній безпеці[3].

Інформаційна безпека є реакцією на інформаційну війну та гібридну війну. Ю. О. Горбань провів аналіз поняття «інформаційна війна», виокремив його складові, визначив основні напрями протидії інформаційній агресії[4].

Проблему інформаційної безпеки особистості в сучасному соціумі вивчали П. В. Квіткін, І. В. Дятлова та Л. О. Петрова, проаналізувавши нормативно-правове забезпечення та підходи до дослідження сутності і змісту інформаційної безпеки особистості[5]. Соціокультурні аспекти інформаційної безпеки в умовах розвитку інформаційного суспільства знайшли відображення в дослідженні А. Гетьмана, О. Данильяна, О. Дзьобаня, Ю. Калиновського[6].

---

[1] Див.: Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти: монографія. Київ: НІПМБ, 2001. 300 с.

[2] Див.: Чистоклетов Л., Обрембальський, С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни.

[3] Див.: Матковський М. С. Інформаційна безпека в умовах російсько-української війни. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів :* матеріали Міжнар. наук.-практ. конф. (Одеса, 26 квіт. 2024 р.) / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2024. С. 168. URL: https://hdl.handle.net/11300/28253.

[4] Див.: Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України.* 2015. № 1. С. 136–141.

[5] Див.: Квіткін П. В., Дятлова І. В., Петрова Л. О. Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія.* 2021. №4 (51). С. 46–62. DOI: https://doi.org/10.21564/2663–5704.51.241998.

[6] Див.: Getman A., Danilyan O., Dzeban A., Kalinovsky Y., Hetman Y. Information security in modern society: sociocultural aspects. *Amazonia Investiga.* 2020. Vol. 9. №25. P. 6–14. URL: https://amazoniainvestiga.info/index.php/amazonia/article/view/1021/946

Серед польських дослідників тема національної та інформаційної безпеки також є досить актуальна. К. Мікусек аналізувала польський підхід до питання інформаційної безпеки, роблячи особливий акцент на сферу національної безпеки, вивчала вплив інформаційної безпеки на ефективність захисту та оборони суспільства від загроз в інфосфері. На розуміння авторки, інформаційна безпека – це комплекс заходів, що вживаються суб'єктами з метою забезпечення відповідних інструментів та засобів, які дозволяють досягти належного рівня захисту інформаційних ресурсів шляхом отримання та накопичення інформації[1]. У праці «Інформаційна безпека. Нові виклики» К. Лідерман зазначав, що інформаційна безпека «стосується суб'єкта (людини або організації, в тому числі такої, як держава), який може зазнати загрози втрати інформаційних ресурсів або отримання інформації низької якості. Отже, інформаційна безпека означає обґрунтовану впевненість суб'єкта в якості та доступності інформації, що отримується та використовується»[2].

К. Торбіцка звертає увагу на чотири основні аспекти впливу російсько-української війни, які впливають на безпеку Польщі: питання енергетичної безпеки; складні польсько-російські відносини; безумовна підтримка України з боку Польщі (політична, військова, фінансова та гуманітарна), а також ймовірність збройного нападу росії на територію Польщі[3].

Отже, інформаційна безпека – багатопланове поняття, яке потребує уваги з огляду різних аспектів: політичного, правового, психологічного, соціокультурного, міжнародного тощо.

В Україні відповідальність за здійснення державної політики у сфері інформаційної безпеки та кіберзахисту реалізує кілька інституцій і профільних відомств. Ключову роль відіграє Рада національної без-

[1] Див.: Mikusek K. Polskie podejśce do bezpieczeństwa informacyjnego. *Problemy Techniki Uzbrojenia.* 2023. Nr 5. Zeszyt 167. S. 153. URL: https://ptu-biuletyn.pl/article/01.3001.0054.3001/pl.

[2] Liderman K. Bezpieczeństwo informacyjne. Nowe wyzwania. Warszawa: Wydawnictwo Naukowe PWN. 2017. S. 15.

[3] Див.: Torbicka K. Bezpieczeństwo Polski w XXI wieku: wyzwania, strategie i perspektywy. Paris: Fondapol, 2025. S. 38. URL: https://www.fondapol.org/app/uploads/2025/09/263_torbicka_pol_2025-07-10_v4.pdf

пеки і оборони України (РНБО) та спеціальні державні органи. Розглянемо їхні функції.

Рада національної безпеки і оборони координує та контролює стратегічне планування, а її робочий орган – Національний координаційний центр кібербезпеки (НКЦК) – забезпечує взаємодію державних органів, військових структур та приватного сектора для нейтралізації загроз. Ці органи відіграють ключову роль у національній системі кібербезпеки держави, забезпечуючи її сталий розвиток, збалансованість та ефективність, а також інтеграцію у міжнародну систему кібербезпеки. РНБО України забезпечує дієву координацію та контроль, ефективне стратегічне планування у сфері кібербезпеки України, аналіз та прогнозування розвитку ландшафту кіберзагроз для проактивного реагування на потенційні та актуальні виклики та загрози[1].

Наступна інституція – це Державна служба спеціального зв'язку та захисту інформації України, яка відповідає за захист державних електронних ресурсів та об'єктів критичної інфраструктури. Служба розробляє стандарти, контролює технічний та криптографічний захист інформації (зокрема застосування сучасних Базових профілів безпеки) та реагує на кіберінциденти урядовою командою CERT-UA. CERT-UA – це Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України. Завданнями CERT-UA є: накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; взаємодія з іноземними

[1] Див.: Український досвід змінює світову кібербезпеку. *Рада національної безпеки і оборони України*. URL: https://www.rnbo.gov.ua/ua/Diialnist/7376.html.

та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST зі сплатою щорічних членських внесків; взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту; сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам[1].

Ще однією інституцією, яка забезпечує державну безпеку в інформаційній сфері, є Служба безпеки України, У структурі СБУ є Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки (ДКІБ СБУ), який протидіє кібершпигунству, розслідує ворожі кібератаки, виявляє, припиняє та розкриває кримінальні правопорушення проти миру і безпеки людства, учинені в кіберпросторі, а також захищає національний інформаційний простір від деструктивного впливу. СБУ комплексно забезпечує контррозвідувальний захист інформаційної та кібернетичної безпеки держави.

Пріоритетними завданнями на цьому напрямі діяльності спецслужби є, зокрема: розслідування кіберінцидентів і кібератак на державні електронні інформаційні ресурси, критичну інформаційну інфраструктуру; протидія проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації[2].

Для виявлення та реагування на шкідливий вплив саме інформації в Україні існують дві структури: Центр протидії дезінформації при Раді національної безпеки і оборони (РНБО) та Центр стратегічних

[1] Див.: Про CERT-UA. *CERT-UA*. URL: https://cert.gov.ua/about-us.

[2] Див.: Захист інформаційного та кіберпростору. *Служба безпеки України.* URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky.

комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики.

Центр протидії дезінформації було утворено Рішенням РНБО України від 11 березня 2021 р. «Про створення Центру протидії дезінформації», яке набуло чинності за Указом Президента України від 19 березня 2021 р. № 106/2021[1].

Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою. Основна увага зосереджена на протидії поширенню неправдивої інформації та боротьбі з інформаційним тероризмом.

Основними завданнями Центру протидії дезінформації є: аналіз та моніторинг подій і явищ в інформаційному просторі України, вивчення стану інформаційної безпеки та присутності України у світовому інформаційному просторі; виявлення та аналіз поточних і прогнозованих загроз інформаційній безпеці України, а також чинників, які впливають на їх формування, прогнозування та оцінка наслідків для безпеки національних інтересів України; підготовка для Ради національної безпеки і оборони України інформаційно-аналітичних матеріалів з питань забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою; участь у розбудові системи стратегічних комунікацій, організації та координації заходів щодо її розвитку; участь у розвитку стратегічних комунікацій – розроблення та реалізація Стратегії інформаційної безпеки України, здійснення аналізу стану її реалізації, зокрема з питань ефективності заходів щодо протидії дезінформації; розроблення методології ви-

[1] Див.: Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 р. № 106/2021. URL: https://www.president.gov.ua/documents/1062021–37421.

явлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру; вивчення, узагальнення й аналіз досвіду інших держав і міжнародних організацій з протидії дезінформації та підготовка пропозицій щодо його використання в Україні тощо[1].

У березні 2021 р. було організовано Центр стратегічних комунікацій та інформаційної безпеки (ЦСКІБ) при Міністерстві культури та інформаційної політики. Головною метою роботи Центру стали контрдії зовнішнім загрозам у сфері комунікацій, зокрема, інформаційним атакам, спрямованим на Україну з боку російської федерації[2]. ЦСКІБ фокусується на спільних зусиллях громадських організацій та владних структур для протидії дезінформації, швидкій реакції на поширення фейків і на підтримці українських наративів. Хоча цей центр діє під егідою Міністерства культури та інформаційної політики, він взаємодіє з Центром протидії дезінформації РНБО, який відповідає за аспекти безпеки і розвиток міжнародних зв'язків.

Основними напрямами діяльності ЦСКІБ є:

− створення контрнаративів щодо інформаційних атак з боку рф та впровадження українських наративів в офіційну комунікацію уряду;

− розробка онлайн-ресурсів для активної реакції на інформаційні атаки;

− регулярне сповіщення про гібридну агресію росії на міжнародному рівні та співпраця з міжнародними партнерами для розробки механізмів протидії дезінформації[3].

Що стосується правового забезпечення інформаційної безпеки та контрпропаганди, то в Україні останніми роками це регулюється низкою указів. У Стратегії воєнної безпеки України, прийнятій Радою

[1] Див.: Про Центр. *Центр протидії дезінформації.* 22.12.2021. URL: https://cpd.gov.ua/documents/%D0%BF%D1%80%D0%BE-%D1%86%D0%B5%D0%BD%D1%82%D1%80/.

[2] Див.: Про центр. *Центр стратегічних комунікацій та інформаційної безпеки.* URL: https://spravdi.org/pro-nas/.

[3] Див.: Бондаренко Я. Фейкньюз та дезінформація в контексті війни Росії та України: дипломна робота на здобуття вищої освіти магістра: спец. 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» освітньої програми «Міжнародні відносини». Харків: ХНЕУ ім. С. Кузнеця, 2023. С. 71. URL: https://repository.hneu.edu.ua/handle/123456789/30845.

національної безпеки і оборони України 25 березня 2021 р. та затвердженій Указом Президента України від 25.03.2021 р. №121/2021, серед іншого, зазначається, що пропаганда є одним із засобів ведення розв'язаної російською федерацією війни проти України[1].

У грудні 2021 р. Указом Президента №685 було введено рішення Ради національної безпеки і оборони «Про Стратегію інформаційної безпеки». Цей документ ідентифікує актуальні виклики та загрози, які становлять загрозу для української національної безпеки у сфері інформації, а також визначає завдання та цілі для протидії цим загрозам. Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина[2]. У Стратегії згадується низка понять, зокрема «дезінформація», «глобальні дезінформаційні кампанії» «спеціальні інформаційні операції», «пропаганда». Проте документ не містить визначення цих понять[3].

У 2023 р. було прийнято «Стратегію інформаційної безпеки на період до 2025 року», план заходів до неї затверджений розпорядженням Кабінету Міністрів України від 30 березня 2023 р. №272-р, стратегічною метою якої визначена «протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності дер-

[1] Див.: Про рішення Ради національної безпеки і оборони України від 25 березня 2021 р. «Про Стратегію воєнної безпеки України»: Указ Президента України від 25 березня 2021 р. №121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text/.

[2] Див.: Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 груд. 2021 р. №685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

[3] Див.: Горбик Р., Дуцик Д., Шалайський С. Ефективність протидії російській дезінформації в Україні в умовах повномасштабної війни. Аналітичний звіт. ГО «Український інститут медіа та комунікації», 2023. С. 48. URL: https://www.jta.com.ua/wp-content/uploads/2023/08/UMCI_-Effectiveness-of-Russian-Disinformation-Counteration_UA.pdf

жави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини і громадянина»[1]. У цій Стратегії визначено поняття «інформаційна безпека України» – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом[2].

Говорячи про забезпечення інформаційної безпеки Республікою Польща, слід зазначити, що також є документи, які регулюють це питання. Одним із суттєвих джерел, що стосуються певного аспекту інформаційної безпеки, була Стратегія національної безпеки Республіки Польщі 2020 р.[3] У тексті концепції можна знайти посилання на питання, пов'язані з кібербезпекою та інформаційною сферою. Щодо кібербезпеки, то стратегія передбачала заходи, спрямовані на підвищення стійкості до кіберзагроз та покращення інформаційної безпеки у державному, військовому та приватному секторах[4]. У питаннях, пов'язаних з інформаційним простором, стратегічна концеп-

[1] Див.: Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272–2023-%D1%80#Text/.

[2] Див.: Про рішення Ради національної безпеки і оборони України від 15 жовт. 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 груд. 2021 р. № 685/2021.

[3] Див.: Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Warszawa, 2020. 37 s. URL: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf

[4] Там само. S. 20.

ція національної безпеки Республіки Польщі стосувалася насамперед необхідності забезпечення стабільності існування держави та громадян у інформаційній сфері. З огляду на це планувалося вживати необхідні заходи у таких сферах.

1. Встановлення стратегічних рівнів діяльності як у віртуальному, так і у фізичному та когнітивному вимірах. Це дозволить захистити інформаційну архітектуру та зменшити вплив дезінформації.

2. Створення єдиної системи урядової комунікації, завданням якої є прогнозування, планування та реалізація узгоджених комунікаційних заходів із використанням широкого спектру комунікаційних каналів та засобів масової інформації, а також застосування інструментів розвідки та впливу в різних сферах національної безпеки.

3. Активна протидія дезінформації шляхом розбудови потенціалу та створення процедур співпраці з інформаційними та соціальними медіа, залучення громадян та неурядових організацій.

4. Підвищення обізнаності щодо загроз, пов'язаних із маніпулюванням інформацією, шляхом освіти у сфері інформаційної безпеки[1].

Але цю Стратегію було прийнято до повномасштабного вторгнення російської федерації в Україну. Тому 25 липня 2025 р. польський уряд схвалив оновлену Стратегію національної безпеки. Стратегія визначає національні інтереси та найважливіші цілі Польщі у сфері безпеки. Держава зосередиться на чотирьох пріоритетах: територіальній цілісності, безпеці громадян, сталому розвитку та вигідній для Польщі структурі міжнародної системи безпеки.

Основні положення Стратегії національної безпеки визначають національні інтереси Польщі, а саме:

– збереження незалежності, територіальної цілісності, суверенітету та безпеки держави й громадян;

– збереження демократичної системи, національної ідентичності та національної спадщини;

– існування міжнародного порядку, заснованого на співпраці та повазі до права, що забезпечує гарантії безпечного розвитку Польщі;

[1] Див.: Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Warszawa, 2020. 37 s. URL: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf. S. 21.

– існування сприятливих умов для сталого та збалансованого соціального й економічного розвитку, а також для охорони навколишнього середовища.

Стратегічними цілями національної безпеки Польщі визначено збільшення здатності впливати на формування міжнародної системи, а саме: формування політики НАТО та ЄС у спосіб, що відповідає інтересам безпеки Польщі; підтримка стратегічного партнерства зі США та інтенсифікація регіональної та двосторонньої співпраці; розвиток співпраці в рамках тимчасових коаліцій з державами, що мають подібні цілі щодо захисту системи безпеки; протидія спробам Росії створити систему безпеки, засновану на зонах впливу; підтримка України як незалежної, демократичної держави із прозахідною орієнтацією, здатної до ефективної самооборони[1]. Але станом на червень 2026 р. ця нова Стратегія ще не підписана Президентом Польщі. Таким чином, актуальною залишається Стратегія національної безпеки Республіки Польщі 2020 р.

Ще одним важливим документом, що регулює питання інформаційної безпеки, є Стратегія кібербезпеки Польщі на 2026–2029 рр., ухвалена 10 березня 2026 р. Радою Міністрів Республіки Польща. Цей документ визначає напрямки розвитку цифрової безпеки держави та сприятиме зміцненню Національної системи кібербезпеки (Krajowy System Cyberbezpieczeństwa). Його реалізація має на меті підвищити стійкість Польщі до кіберзагроз та покращити безпеку громадян, підприємств і державних установ[2].

Стратегія визначає найважливіші напрямки діяльності Польщі у сфері кібербезпеки. До них належать, зокрема:

– розвиток та зміцнення Національної системи кібербезпеки;

[1] Див.: Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. *Kancelaria Prezesa Rady Ministrów*. 25.07.2025. URL: https://www.gov.pl/web/premier/strategia-bezpieczenstwa-narodowego-rzeczypospolitej-polskiej.

[2] Див.: Nowa strategia cyberbezpieczeństwa. Polska wzmacnia ochronę przed cyberatakami. *Ministerstwo Cyfryzacji.* 10.03.2026. URL: https://www.gov.pl/web/cyfryzacja/nowa-strategia-cyberbezpieczenstwa-polska-wzmacnia-ochrone-przed-cyberatakami?fbclid=IwY2xjawQeeYRleHRuA2FlbQIxMABicmlkETBJYWpHZnBsM2x0ZjVSZDdzc3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHg1lFUPSI5wRyaVMZWG1UCwI2bbwz8YCo7j7iSJtd821pqadq8eLgY07Q7vq_aem_J0cpJBTSxAzItsyiEbgMdg.

– підвищення спроможності реагувати на інциденти та протидіяти кіберзлочинності;

– підвищення стійкості інформаційних систем у державному та приватному секторах;

– розвиток співпраці між державним та приватним секторами;

– освітні, інформаційні та навчальні заходи у сфері кібербезпеки;

– розвиток досліджень, інновацій та технологій у цій сфері;

– поглиблення міжнародної співпраці[1].

2026 р. з ініціативи Міністерства закордонних справ Кабінет Міністрів Польщі ухвалив Стратегію зовнішньої політики Польщі на 2026–2030 рр. У вступному слові до Стратегії Міністр закордонних справ Польщі Радослав Сікорський підкреслює, що «важливим елементом зовнішньої політики та безпеки є суспільна стійкість у широкому розумінні. Вона охоплює боротьбу з російською пропагандою та дезінформацією, а також чесне інформування громадян про масштаби та характер загроз. Не для того, щоб лякати, а щоб формувати усвідомленість – суспільство має бути готовим до складніших часів і менш вразливим до маніпуляцій»[2]. Отже, нова Стратегія зовнішньої політики Польщі є реакцією на виклики національній безпеці, пов'язаній з повномасштабним нападом російської федерації на Україну, зростаючим гібридним та кіберзагрозам, у тому числі з використанням сучасних технологій, а також загрозам, пов'язаним з дезінформацією та маніпулюванням інформацією. У Стратегії зазначається, що зовнішня політика служить реалізації основних національних інтересів Республіки Польщі. Найважливішим з них є забезпечення безпеки держави, тобто безперервності її існування, територіальної цілісності, суверенітету та внутрішньої стабільності[3].

Ключовими загрозами національній безпеці визначено агресивну політику росії, гібридні загрози (кібератаки, дезінформація, міграційний тиск), кризу системи контролю над озброєннями та нестабільність

[1] Див.: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej. S. 12–13. URL: https://dap-static.infor.pl/dap/000/789/745/MPO_2026-0309_zal1.pdf.

[2] Strategia poskiej polityki zagranicznej na lata 2026–2030. S. 4. *Ministerstwo Spraw Zagranicznych*. URL: https://www.gov.pl/web/dyplomacja/strategia.

[3] Там само. S. 8.

у світі (Африка, Близький Схід, Індо-Тихоокеанський регіон). Особливу небезпеку становить війна росії проти України, яка впливає на всю систему міжнародної безпеки[1].

В інформаційній війни російської федерації проти України використовуються різні методи, у тому числі пропаганда, за допомогою якої нав'язуються помилкові судження, поширюється неправдива агресивна інформація, яка покликана нав'язати адресату хибну позицію чи життєву поведінку, але вигідну поширювачеві інформації[2].

Поняття «пропаганда» в науковій літературі визначається досить неоднозначно. Наведемо лише кілька дефініцій. Пропаганда – це «навмисна, систематична спроба сформувати сприйняття, маніпулювати пізнанням та керувати поведінкою для досягнення реакції, що сприятиме бажаним намірам пропагандиста»[3]. Ж. З. Денисюк під пропагандою пропонує розуміти політично мотивований інформаційно психологічний вплив на емоційно-вольову сферу масової свідомості, за допомогою якого впроваджуються політичні ідеї, погляди, установки і формується політична поведінка. Психологічною метою пропаганди є вплив на систему ідейних, громадських і політичних установок людей, яку можна змінити шляхом формування нових установок або через посилення (ослаблення) вже існуючих[4].

Контрпропаганда – це інформаційний вплив, спрямований на зниження значення цінностей, пропагованих з позицій ідеологій, далеких від панівних. І пропаганда, і контрпропаганда спрямовані на формування у масовій аудиторії певного стилю мислення і подальшої по-

[1] Див.: Рослонь Д.-А. Т. Стратегія зовнішньої політики Польщі (2026–2030): безпека, розвиток Польщі в ЄС та глобальний вимір. *Український політико-правовий дискурс*. 2026. №23. С. 7. DOI: https://doi.org/10.5281/zenodo.20391592

[2] Див.: Бєлкін Л. М., Юринець Ю. Л., Сопілко І. М., Бєлкін М. Л. Контрпропаганда vs пропаганда в умовах широкомасштабного збройного вторгнення російської федерації в Україну. *Юридичний науковий електронний журнал.* 2022. №6. С. 226. DOI: https://doi.org/10.32782/2524–0374/2022–6/52.

[3] Горбик Р., Дуцик Д., Шалайський С. Ефективність протидії російській дезінформації в Україні в умовах повномасштабної війни. С. 16.

[4] Див.: Денисюк Ж. З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління*. 2021. Том 32 (71). №2. С. 46. DOI: https://doi.org/10.32838/TNU-2663-6468/2021.2/08.

ведінки[1]. Г. Ромерштайн, колишній директор Управління США з протидії радянській дезінформації, визначав контрпропаганду як «ретельно підготовлені відповіді на фальшиву пропаганду з метою спростування дезінформації та підриву авторитету пропагандиста»[2].

Контрпропаганда використовує специфічні «похідні» методи, зокрема такі, як: моніторинг, аналіз, розкриття / викриття справжнього походження (джерела) і справжніх цілей, виявлення помилок (в аргументації, міркуваннях, судженнях тощо)[3].

Сутність контрпропаганди (погоджуємося з думкою Ж. З. Денисюк) – це активні дії, що розкривають облудність пропаганди опонентів, які поширюють негативно критичну інформацію. Головними принципами контрпропаганди дослідниця називає наступальність і послідовність, а завданням контрпропаганди – формування стійкої громадської думки й імунітету до пропаганди суб'єктів, що поширюють негативно критичну інформацію[4].

Отже, одним із ключових завдань України є протидія російській пропаганді та дезінформації в інформаційній сфері, спростування неправдивої інформації та підрив довіри до пропагандистів.

Складовими контрпропаганди є:

– *цілеспрямованість*: фокусування на конкретних пропагандистських наративах, розкриття їх неправдивості та маніпулятивності;

– *фактологічність*: базування на фактах та доказах, на відміну від пропаганди, яка часто оперує емоціями та упередженнями;

– *критичність*: заохочення критичного мислення, заклик аудиторії до ефективного фактчекінгу та аналізу інформації;

---

[1] Денисюк Ж. З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління*. 2021. Том 32 (71). №2. С. 48. DOI: https://doi.org/10.32838/TNU-2663-6468/2021.2/08.

[2] Див.: Romerstein H., Garbus M. 'The Attack on I. F. Stone': An Exchange / reply by A. Brown. The New York Review of Books. 1992. Vol. 39, No. 20 (December 3). URL: https://www.nybooks.com/articles/1992/12/03/the-attack-on-if-stone-an-exchange/.

[3] Див.: Іванова Н. Г., Паливода О. О. Контрпропаганда в контексті протидії загарбницьким діям РФ та збереження психічного здоров'я українців. *Габітус*. 2023. Вип. 23. С. 112. DOI: https://doi.org/10.32782/2663–5208. 2023.54.21.

[4] Див.: Денисюк Ж. З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. С. 48.

– *проактивність*: не лише захист, а й просування власних правдивих та консолідуючих наративів, оскільки контрпропаганда не лише реагує на пропаганду, але й намагається формувати в аудиторії стійкість до маніпуляцій[1].

Найбільш небезпечні наративи російської пропаганди, що поширювала рф проти України, були представлені Центром стратегічних комунікацій та інформаційної безпеки на основі результатів моніторингу Ukraine War Disinfo Working Group у період з 20 лютого до 30 квітня 2023 р. Ці наративи потрапили в інформаційний простір чотирьох країн, що межують з Україною на заході, – Польщі, Молдові, Угорщині та Словаччині. Антиукраїнською пропагандою було встановлено такі наративи.

Антизахідні наративи: «Захід / НАТО спровокували конфлікт між Україною та Росією»; «Захід буде боротися до останнього українця»; «Росія хоче миру, а Захід і Україна хочуть продовжувати війну»; «Країни не повинні допомагати Україні через їхні минулі історичні конфлікти»; «Західні країни загострюють війну»; «Західні країни перебувають під загрозою / будуть втягнуті у війну»; «НАТО / США /Захід беруть участь або будуть безпосередньо залучені у війну»; «Захід наживається на війні в Україні»; «Польща буде втягнута у війну» тощо.

Події на полі бою: «Україна програє війну, а російські війська наступають»; «Українці нападають на мирне населення та здійснюють інші військові злочини»; «Росія стабільно досягає успіху на полі бою, і тому нібито безглуздо намагатися вплинути на результат війни, підтримуючи Україну».

Наративи, що дискредитують Україну: «Україна жорстоко поводиться зі своїми солдатами»; «Українці – нацисти»; «Українське зерно підриває західні економіки»; «Україна продає на Захід неякісне / заражене / занадто багато зерна»; «Україна не стане членом НАТО».

[1] Див.: Ємець Д. О. Контрпропаганда як інструмент інформаційної війни: кваліфікаційна магістерська робота: спец. 281 «Публічне управління та адміністрування» освітньо-професійної програми «Державна політика та публічне управління». Київ: Київський національний економічний університет імені Вадима Гетьмана, 2024. С. 23. URL: https://ir.kneu.edu.ua/server/api/core/bitstreams/86af86cb-8ea3-4919-87b0-0daa21251717/content.

Такі заяви поєднувалися із заявами про дискримінацію в Україні етнічних меншин.

Допомога Україні: «Допомога Україні послаблює / ставить під загрозу країни, які її надають»; «Західні суспільства визнають цю загрозу, а підтримка України слабшає»; «Військова допомога продовжує війну / ставить під загрозу цивільне населення»; «Допомога Україні послаблює / ставить під загрозу країни, які її надають». Ідея надання допомоги Україні зображується як «марна» і лише продовжує війну, що призводить до подальших страждань

Теорії змови: «Війна в Україні є частиною світової змови».

Українські біженці: «Українські біженці зловживають допомогою»; «Українці вибагливі та невдячні»[1]. Ці наративи були переважно зосереджені на зображенні українських біженців як «загрози безпеці Польщі», що польський уряд надає їм «пріоритет» над громадянами Польщі, а українські біженці у відповідь «невдячні» країні, що її приймає.

Ефективна протидія російській пропаганді ґрунтується на критичному мисленні, фактчекінгу, використанні офіційних джерел інформації, створенні власного медіаконтенту та альтернативних до російських наративів. Для захисту інформаційного простору слід вживати такі заходи: викривати фейки – використання платформи Центру протидії дезінформації при РНБО, щоб оперативно перевіряти сумнівні новини, наративи та дізнаватися правду; аналізувати та спростовувати – звертатися до порталу Spravdi, який спеціалізується на розвінчанні російської дезінформації та навчає медіаграмотності; боротися правовими методами та фіксувати інформацію про злочини.

Л. Мазуренко виділила такі складники інформаційної безпеки:

– інформаційно-технічний: створення системи надійного захисту – від несанкціонованого втручання, хакерських атак до інформаційно-комп'ютерних систем та окремих сайтів; блокування комп'ютерних вірусів та радіоелектронних атак, недопущення незаконного використання телерадіомовних частот тощо;

[1] Які наративи російської пропаганди поширені у країнах-сусідах України? *SPRAVDI*. 25.05.2023. URL: https://spravdi.org/yaki-naratyvy-rosijskoyi-propagandy-poshyreni-u-krayinah-susidah-ukrayiny/.

– інформаційно-психологічний захист соціуму та країни від деструктивних інформаційних впливів. Ця проблема особливо «гостро відчувається у воєнний час, бо тоді емоції заважають критично оцінювати та аналізувати ситуацію і ту інформацію, що поширюється в соціальних мережах. Інформація під час воєнних конфліктів стає ще одним видом зброї ворога, враховуючи інформаційно-психологічний аспект інформаційної безпеки»[1].

З метою контрпропаганди слід використовувати різноманітні методи і способи протидії російській пропагандистській машині: О. І. Свідерська пропонує виставляти реальні фото з війни, розвивати волонтерство, яке об'єднує зірок, блогерів, звичайних громадян, інтелектуалів, політиків, проводити злагоджені дії кіберполіції, кіберхакерів, використовувати політичні промови президента тощо. Усі ці дії формують позитивний образ України серед міжнародного співтовариства і впливають на те, що Європа нівелює російські наративи, а дослухається до українських[2].

Як інструмент системи інформаційно-психологічної безпеки контрпропаганда працює на нейтралізацію ворожого інформаційного впливу, руйнує деструктивні наративи та захищає суспільну свідомість від маніпуляцій.

З метою спростування фейків важливе оперативне викриття брехні, використання фактів та доказів для спростування ворожих вкидів (наприклад, через платформу фактчекінгової організації StopFake[3]).

Контрпропаганда під час війни полягає у протидії хахаганді (неологізм, що утворився внаслідок поєднання слів «ха-ха» та пропаганда.) Дезінформація, заснована на висміюванні політиків та інституцій, має назву «хахаганда», термін, який було запроваджено латвійською академіком Солвітою Деніса-Ліепнієце[4]. Хахаганда використовує

[1] Мазуренко Л. І. Інформаційна безпека в умовах російсько-української війни : виклики та загрози. С. 53.

[2] Див.: Свідерська О. І. Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни. *Політикус*. 2022. Вип. 2. С. 60. DOI: https://doi.org/10.24195/24149616.2022–2.10.

[3] Див.: Шанковський О. Як розпізнати фейк. *STOPFAKE.org*. URL: https://www.stopfake.org/uk/yak-rozpiznaty-fejk/.

[4] Див.: Хахаганда: як Росія намагається посилити дезінформаційні наративи в Європі за допомогою глузування та пародії. *STOPFAKE.org*. 03.07.2026. URL: https://

гумор для просування отруйних ідей. У випадку росії, «це має тенденцію бути агресивним, зневажливим і прагне принизити або образити, часто через перебільшення чи припущення про протилежні значення», згідно з дослідженням Д. Чорноброва про гумор та російські зовнішньополітичні наративи[1]. Для забезпечення інформаційної безпеки необхідно перевіряти факти і спростовувати неправдиву інформацію.

Війну росії проти України називають «поворотним моментом» для безпеки Польщі[2], оскільки і проти Польщі ведеться гібридна війна, складовою частиною якої є інформаційна війна, у якій дезінформація, пропаганда та маніпуляції використовуються як інструменти дестабілізації всередині країни, а також для підриву іміджу Польщі за кордоном. Ведеться інформаційна війна в кіберпросторі. У 2024 р. в Польщі щодня фіксувалося в середньому 5 000 кібератак, що робить її однією з найбільш атакованих країн Європи. Найбільшими жертвами цих атак стали урядові установи, фінансовий сектор, система охорони здоров'я (лікарні), вища освіта, а також критична інфраструктура, зокрема залізниця та енергетика.

Під час президентської кампанії в Польщі 2025 р. було виявлено мережі фейкових акаунтів, пов'язаних із російськими інтересами, які поширювали дезінформацію на такі теми, як війна в Україні, міграція чи відносини з ЄС. Метою було поглиблення суспільних розбіжностей та підривання довіри до обраних кандидатів та інституцій. Повторювалися проросійські наративи, що пропагували, зокрема, тезу про те, що лише росія прагне миру. Також було виявлено конкретні операції, такі як «Overload» (інформаційний хаос) та «Doppelganger» (видавання себе за авторитетні ЗМІ) .

Серед європейських сусідів і партнерів України, проти яких спрямовані атаки Кремля, Польща посідає перше місце. Аналіз StopFake

www.stopfake.org/uk/hahaganda-yak-rosiya-namagayetsya-posiliti-dezinformatsijni-narativi-v-yevropi-za-dopomogoyu-gluzuvannya-ta-parodiyi/.

[1] Див.: Chernobrov D. Humor and Foreign Policy Narration: The Persuasive Power and Limitations of Russia's Foreign Policy Pranks. *Global Studies Quarterly.* 2024. Vol. 4, Issue 1. January. ksae007. DOI: https://doi.org/10.1093/isagsq/ksae007.

[2] Див.: Torbicka K. Bezpieczeństwo Polski w XXI wieku: wyzwania, strategie i perspektywy. S. 38.

інформаційних наративів проти країн ЄС, пов'язаних з Україною, показує: від 2014 р. найбільше російських атак припадало саме на Польщу[1].

Приводом до погіршення стосунків між Україною і Польщею стало рішення Президента України Володимира Зеленського присвоїти одному з підрозділів Сил спеціальних операцій ЗСУ найменування «Героїв УПА», а також перепоховання в Україні наприкінці травня одного з лідерів ОУН-УПА Андрія Мельника. У відповідь президент Польщі Кароль Навроцький позбавив українського лідера найвищої польської нагороди – ордена Білого орла. Далі українські посадовці один за одним повертали свої нагороди; до цього «челенджу» почали приєднуватися й польські посадовці. Потім – низка різких заяв від представників «Конфедерації», погрози заблокувати Україні вступ до ЄС та дискусія про доцільність участі Києва в конференції з відновлення в Гданську[2].

І хоча конференція в Гданську 25–26 червня 2026 р. таки відбулася, весь цей конфлікт не міг бути проігнорований у Москві. Було розгорнуто скоординовану інформаційну кампанію, яка підхоплювала, перебільшувала й поширювала, зокрема, відверті фейки, щоб ще більше погіршити стосунки між двома європейськими країнами, зірвати підтримку України в польському суспільстві та загальмувати її євроінтеграцію. StopFake зазначає: ця кампанія не виникла з нуля, а готувалася протягом усіх років російсько-української війни[3].

Зокрема, під час російсько-української війни періодично з'являлися фейки про те, що Польща нібито планує окупувати західні області України, що поляки вимагають повернути майно у Львові, а польські «найманці» воюють на сході України й готуються напасти на Білорусь. Крім того, фігурували й фейки про українських біженців – попри те, що до повномасштабного вторгнення росії їх було в країні не так

[1] Див.: Чуранова О. «Wypierdalaj na Ukrainę» – як Росія перетворила польсько-українську кризу на ще одну інформаційну операцію. *STOPFAKE.org*. 27.06.2026. URL: https://www.stopfake.org/uk/wypierdalaj-na-ukraine-yak-rosiya-peretvorila-polsko-ukrayinsku-krizu-na-shhe-odnu-informatsijnu-operatsiyu/.

[2] Там само.

[3] Там само.

багато. Утім, фейкові заяви польських урядовців про «дешеву робочу силу» з України вже й тоді запускали. О. Чуранова наводить такі найбільш поширені антиукраїнські наративи про українсько-польські взаємини.

«Польща готується до війни з Україною». Спираючись на публікацію маргінального проросійського видання Myśl Polska, ресурси рф розганяли тезу, що Київ для Варшави нібито «небезпечніший за росію», що є продовженням наративу «ЄС / Польща як агресор».

«Волинь – польська територія», «Львів – польське місто». Банери на футбольному матчі, «петиції», заяви про «відновлення кордонів 1939 р.» – також реінкарнація наративу про територіальні претензії.

Дискредитація українських біженців. Відмови у статусі PESEL UKR, вимоги зняти українські прапори з будівель у Гданську й Любліні, вигнати всіх українців з Польщі та скасувати всю соціальну допомогу.

Повторення російського наративу про «денацифікацію» – буцімто необхідну умову, «щоб вступити в ЄС» чи «відновити добросусідські відносини», – а також дегуманізаційні тексти про «фашистський генетичний код» українців.

Антиєвропейський удар: Polexit і вето. Теза, що вступ України «зруйнує» польське сільське господарство й підштовхне Польщу до виходу з ЄС, або що Польща зробить усе, аби Україна не вступила до ЄС.

«Росія тут ні до чого». Окремий шар контенту: публікації глузливо заперечували саму наявність «руки Кремля», висміюючи польські й українські заяви про дезінформаційну кампанію[1].

Головними шляхами поширення недостовірної інформації в умовах війни є соціальні мережі; підроблені акаунти відомих людей, політиків, телерадіомовні канали; особисті повідомлення або в групах Viber, WhatsApp, Telegram та інших месенджерах. У сфері забезпечення інформаційної безпеки важливе місце посідає проблема чуток –

[1] Див.: Чуранова О. «Wypierdalaj na Ukrainę» – як Росія перетворила польсько-українську кризу на ще одну інформаційну операцію.

недостовірних повідомлень, що мають різноманітну комунікативну форму[1].

З метою протидії російській пропаганді Україна активно проводить інформаційну кампанію. Діють програми, спрямовані на попередження населення про можливі випадки поширення дезінформації від противника. Зокрема, з кінця лютого 2022 р. населення України було ретельно проінформоване, з особливим акцентом на те, що можна довіряти лише офіційним українським джерелам інформації. Це допомогло протистояти стандартній російській стратегії, яка полягає в поширенні неправдивої інформації та її максимальному поширенні у соціальних мережах та інших загальнодоступних каналах. Від початку російсько-українського конфлікту журналісти та військове командування України оперативно інформували населення про досягнення та невдачі українських збройних сил. Ця прозорість сприяла об'єктивному сприйняттю тих подій, які розвивалися тоді[2].

З метою відповіді на загрози, які виникають щодо Польщі у зв'язку з російсько-українською війною, в Польщі розроблено Національний проєкт відлякування та оборони «Щит Схід» (Narodowy Projekt Odstraszania i Obrony Tarcza Wschód) на 2024–2028 рр. Цей проект є ключовою ініціативою у сфері зміцнення безпеки Польщі та східного флангу НАТО. Проєкт, оголошений у травні 2024 року, передбачає будівництво укріплень на кордоні з росією та білоруссю, системи військових фортифікацій, фізичних бар'єрів та сучасних систем моніторингу повітряного простору. Його реалізація запланована на 2024–2028 рр., а бюджет становить 10 млрд злотих[3].

---

[1] Див.: Пархоменко-Куцевіл О. І. Забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. *Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні :* матеріали Всеукр. наук.-практ. конф. у трьох томах, м. Київ, ДЗВО «Університет менеджменту освіти» НАПН України, 15–28 квітня 2022 р. / ред. колегія : І. О. Дегтярьова, В. С. Куйбіда, П. М. Петровський та ін., уклад. Т. О. Мельник. Київ: ДЗВО «УМО» НАПН України, 2022. Т. 1. С. 40–43. URL: https://ispp.org.ua/wp-content/uploads/2022/06/tezy0422-t1.pdf

[2] Див.: Бондаренко Я. Фейкньюз та дезінформація в контексті війни Росії та України. С. 71.

[3] Див.: Torbicka K. Bezpieczeństwo Polski w XXI wieku: wyzwania, strategie i perspektywy. S. 25.

Контрпропаганда в Польщі, спрямована проти російської дезінформації, ґрунтується на діяльності урядових установ, організацій з перевірки фактів та програм медіаосвіти. В аналізі російського інформаційного тиску в інтернеті в період з 26 червня по 2 липня 2026 р., проведеному сервісом Disinfo Digest, що займається протидією дезінформації, було зазначено, що цей тиск був спрямований проти «польської політики стримування». Зокрема, дезінформація стосувалася програми «Щит Схід», модернізації польської армії та навчань за участю військовослужбовців НАТО[1].

У Польщі існує багато фактчекінгових організацій, які розвінчують російську дезінформацію і здійснюють контрпропаганду. Фактчекінг – це один з напрямів журналістського контролю. Перевірка фактів спрямована на виявлення невідповідностей між наявними фактами та навколишньою дійсністю. Прикладом можна назвати польську інституцію «Демагог» (Stowarzyszenie Demagog) – одну з перших фактчекінгових організацій в Польщі, якаіснує з 2014 р., займається перевіркою висловлювань політиків, аналізує передвиборчі обіцянки, бореться з фейковими новинами та дезінформацією, проводить просвітницьку роботу[2]. Разом із партнерами – Фондом Digital Poland та Спілкою компаній з публічних відносин – у рамках Коаліції «Разом проти дезінформації» фактчекінгова організація «Демагог» запланувала кампанію, метою якої є викриття маніпуляцій та навчання критичному підходу до контенту, що публікується в соціальних мережах та інтернеті. Оскільки основним механізмом російської маніпуляції є розмноження джерел інформації в рамках одного шаблону, саме «система матрьошок», яку історик Марк Свєрчек описує як «досконалу дезінформацію», є відправною точкою роздумів цих організацій, а матрьошка – символом усієї кампанії[3].

[1] Див.: Przed szczytem w Ankarze rosyjska propaganda wymierzona w relacje Polski z NATO. *PAP*. 08.07.2026. URL: https://www.pap.pl/aktualnosci/przed-szczytem-w-ankarze-rosyjska-propaganda-wymierzona-w-relacje-polski-z-nato.

[2] Див.: Stowarzyszenie Demagog. *Demagog*. URL: https://demagog.org.pl/poznajmy-sie/.

[3] Див.: Docieraj do źródła prawdy. *Demagog*. URL: https://demagog.org.pl/zrodloprawdy/.

Для подолання негативних чинників впливу на інформаційну безпеку громадян України в умовах війни О. В. Прудникова пропонує здійснювати комплекс заходів, одним із напрямів реалізації яких є підвищення якісного стану медіаграмотності населення[1]. Ю. Ніколаєць такими векторами покращення медіаграмотності вітчизняних громадян вважає: формування негативного ставлення до інформації анонімного характеру та критичне ставлення до інформаційних оцінних повідомлень без обґрунтованих належним чином висновків; недопущення коментування чуток та неперевірених даних з метою здійснення висновків на їх підставі; недопустимість поширення меседжів з закритих джерел або джерел, походження яких приховується автором повідомлення; недоцільність використання джерел, походження яких не має можливості підтвердити за відповідними посиланнями. Також «ставлення з пересторогою має бути сформоване до раптової появи нових джерел контенту, які поширюють інсайдерську інформацію; до джерел, які подають інформацію незбалансовано, а також до інформації експертів, походження знань, умінь і навичок яких неможливо встановити або прогнози яких переважно не справджуються[2].

Отже, аналіз законодавства, стратегій і практичного досвіду засвідчує, що інформаційна безпека суспільства є важливою складовою національної безпеки як України, так і Польщі, особливо в умовах російсько-української війни. Контрпропаганда спрямована на протидію дезінформації – боротьбу з інформаційними загрозами та зміцнення суспільної стійкості. Можна виділити три рівні інформаційної безпеки: індивідуальний (інформаційна безпека особистості); суспільний (безпека окремих локальних груп); державний (національний). Російська агресія проти України підштовхнула суспільство і держави до пошуку нових, більш дієвих механізмів протистояння маніпулятивним впливам і технологіям – використанню контрпропаганди, підвищенню рівня медіаграмотності серед населення, внесенням змін

[1] Див.: Прудникова О. В. Інформаційна безпека вітчизняного суспільства в умовах російсько-української війни. С. 78.

[2] Див.: Ніколаєць Ю. Державна інформаційна політика України в умовах повномасштабного воєнного вторгнення Російської Федерації: суспільно-мобілізаційний потенціал і ефективність. *Політичні дослідження.* 2024. №1 (7). С. 58. DOI: https://doi.org/10.53317/2786-4774-2024-1-3.

у державні стратегії національної та кібербезпеки, зовнішньої політики. Цей досвід України та Польщі буде корисним для інших країн.

Список використаних джерел

1. Бєлкін Л. М., Юринець Ю. Л., Сопілко І. М., Бєлкін М. Л. Контрпропаганда vs пропаганда в умовах широкомасштабного збройного вторгнення російської федерації в Україну. *Юридичний науковий електронний журнал*. 2022. № 6. С. 224–230. DOI: https://doi.org/10.32782/2524–0374/2022–6/52.
2. Биков О. В. Інформаційна безпека: правовий та культурологічний виміри. *Аналітично-порівняльне правознавство.* 2024. № 2. С. 396–402. DOI: https://doi.org/10.24144/2788–6018.2024.02.67.
3. Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти : монографія. Київ: НІПМБ, 2001. 300 с.
4. Бондаренко Я. Фейкньюз та дезінформація в контексті війни Росії та України: дипломна робота на здобуття вищої освіти магістра: спец. 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» освітньої програми «Міжнародні відносини». Харків : ХНЕУ ім. С. Кузнеця, 2023. 97 с. URL: https://repository.hneu.edu.ua/handle/123456789/30845.
5. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України.* 2015. № 1. С. 136–141.
6. Горбик Р., Дуцик Д., Шалайський С. Ефективність протидії російській дезінформації в Україні в умовах повномасштабної війни. Аналітичний звіт. ГО «Український інститут медіа та комунікації», 2023. 66 с. URL: https://www.jta.com.ua/wp-content/uploads/2023/08/UMCI_-Effectiveness-of-Russian-Disinformation-Counteration_UA.pdf
7. Денисюк Ж. З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління.* 2021. Том 32 (71). № 2. С. 46–51. DOI: https://doi.org/10.32838/TNU-2663-6468/2021.2/08.
8. Ємець Д. О. Контрпропаганда як інструмент інформаційної війни: кваліфікаційна магістерська робота: спец. 281 «Публічне управління та адміністрування» освітньо-професійної програми «Державна політика

та публічне управління». Київ : Київський національний економічний університет імені Вадима Гетьмана. 2024. 99 с. URL: https://ir.kneu.edu.ua/server/api/core/bitstreams/86af86cb-8ea3-4919-87b0-0daa21251717/content.
9. Захист інформаційного та кіберпростору. *Служба безпеки України.* URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky.
10. Іванова Н. Г., Паливода О. О. Контрпропаганда в контексті протидії загарбницьким діям РФ та збереження психічного здоров'я українців. *Габітус*. 2023. Вип. 23. С. 111–115. DOI: https://doi.org/10.32782/2663–5208. 2023.54.21.
11. Квіткін П. В., Дятлова І. В., Петрова Л. О. Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія*. 2021. №4 (51). С. 46–62. DOI: https://doi.org/10.21564/2663–5704.51.241998.
12. Литвиненко О. В. Інформаційна безпека. *Енциклопедія Сучасної України.* 2011. DOI: 10.5281/zenodo.19971510.
13. Мазуренко Л. І. Інформаційна безпека в умовах російсько-української війни : виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Питання політології.* 2022. Вип. 42. С. 50–57. DOI: https://doi.org/10.26565/2220-8089-2022-42-08.
14. Матковський М. С. Інформаційна безпека в умовах російсько-української війни. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів :* матеріали Міжнар. наук.-практ. конф. (Одеса, 26 квіт. 2024 р.) / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2024. С. 168–170. URL: https://hdl.handle.net/11300/28253.
15. Ніколаєць Ю. Державна інформаційна політика України в умовах повномасштабного воєнного вторгнення Російської Федерації: суспільно-мобілізаційний потенціал і ефективність. *Політичні дослідження.* 2024. №1 (7). С. 42–67. DOI: https://doi.org/10.53317/2786-4774-2024-1-3
16. Пархоменко-Куцевіл О. І. Забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. *Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні :* матеріали Всеукр. наук.-практ. конф. у трьох томах, м. Київ, ДЗВО «Університет менеджменту освіти» НАПН України, 15–28 квітня 2022 р. / ред. колегія : І. О. Дегтярьова, В. С. Куйбіда, П. М. Петровський та ін., уклад. Т. О. Мельник. Київ: ДЗВО «УМО» НАПН України, 2022. Т. 1. С. 40–43. URL: https://ispp.org.ua/wp-content/uploads/2022/06/tezy0422-t1.pdf

17. Про CERT-UA. *CERT-UA*. URL: https://cert.gov.ua/about-us.
18. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272–2023-%D1%80#Text/.
19. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 р. «Про Стратегію воєнної безпеки України»: Указ Президента України від 25 березня 2021 р. № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text/.
20. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 р. № 106/2021. URL: https://www.president.gov.ua/documents/1062021–37421.
21. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.
22. Про Центр. *Центр протидії дезінформації.* 22.12.2021. URL: https://cpd.gov.ua/documents/%D0%BF%D1%80%D0%BE-%D1%86%D0%B5%D0%BD%D1%82%D1%80/.
23. Про центр. *Центр стратегічних комунікацій та інформаційної безпеки.* URL: https://spravdi.org/pro-nas/.
24. Прудникова О. В. Інформаційна безпека вітчизняного суспільства в умовах російсько-української війни. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія.* 2025. Т. 2. № 65. С. 71–81. DOI: https://doi.org/10.21564/2663–5704.65.331715.
25. Рослонь Д.-А. Т. Стратегія зовнішньої політики Польщі (2026–2030): безпека, розвиток Польщі в ЄС та глобальний вимір. *Український політико-правовий дискурс*. 2026. № 23. С. 1–19. DOI: https://doi.org/10.5281/zenodo.20391592
26. Свідерська О. І. Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни. *Політикус.* 2022. Вип. 2. С. 60–65. DOI: https://doi.org/10.24195/24149616.2022–2.10.
27. Український досвід змінює світову кібербезпеку. *Рада національної безпеки і оборони України*. URL: https://www.rnbo.gov.ua/ua/Diialnist/7376.html.

28. Хахаганда: як Росія намагається посилити дезінформаційні наративи в Європі за допомогою глузування та пародії. *STOPFAKE.org*. 03.07.2026. URL: https://www.stopfake.org/uk/hahaganda-yak-rosiya-namagayetsya-posiliti-dezinformatsijni-narativi-v-yevropi-za-dopomogoyu-gluzuvannya-ta-parodiyi/.
29. Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії*. 2024. Вип. 31. DOI: https://doi.org/10.5281/zenodo.11381101
30. Чуранова О. «Wypierdalaj na Ukrainę» – як Росія перетворила польсько-українську кризу на ще одну інформаційну операцію. *STOPFAKE.org*. 27.06.2026. URL: https://www.stopfake.org/uk/wypierdalaj-na-ukraine-yak-rosiya-peretvorila-polsko-ukrayinsku-krizu-na-shhe-odnu-informatsijnu-operatsiyu/.
31. Шанковський О. Як розпізнати фейк. *STOPFAKE.org*. URL: https://www.stopfake.org/uk/yak-rozpiznaty-fejk/.
32. Які наративи російської пропаганди поширені у країнах-сусідах України? *SPRAVDI*. 25.05.2023. URL: https://spravdi.org/yaki-naratyvy-rosijskoyi-propagandy-poshyreni-u-krayinah-susidah-ukrayiny/.
33. Chernobrov D. Humor and Foreign Policy Narration: The Persuasive Power and Limitations of Russia's Foreign Policy Pranks. *Global Studies Quarterly.* 2024. Vol. 4, Issue 1. January. ksae007. DOI: https://doi.org/10.1093/isagsq/ksae007.
34. Docieraj do źródła prawdy. *Demagog*. URL: https://demagog.org.pl/zrodloprawdy/.
35. Getman A., Danilyan O., Dzeban A., Kalinovsky Y., Hetman Y. Information security in modern society: sociocultural aspects. *Amazonia Investiga.* 2020. Vol. 9. № 25. P. 6–14. URL: https://amazoniainvestiga.info/index.php/amazonia/article/view/1021/946
36. Liderman K. Bezpieczeństwo informacyjne. Nowe wyzwania. Warszawa: Wydawnictwo Naukowe PWN, 2017. 422 s.
37. Mikusek K. Polskie podejśce do bezpieczeństwa informacyjnego. *Problemy Techniki Uzbrojenia*. 2023. Nr 5. Zeszyt 167. S. 149–159. URL: https://ptu-biuletyn.pl/article/01.3001.0054.3001/pl.
38. Nowa strategia cyberbezpieczeństwa. Polska wzmacnia ochronę przed cyberatakami. *Ministerstwo Cyfryzacji.* 10.03.2026. URL: https://www.gov.pl/web/cyfryzacja/nowa-strategia-cyberbezpieczenstwa-polska-wzmacnia-ochrone-przed-cyberatakami?fbclid=IwY2xjawQeeYRleHRuA2FlbQIxMABicmlkETBJYWpHZnBsM2x0ZjVSZDdzc3J0YwZhcHBfaWQQMjIyMD

M5MTc4ODIwMDg5MgABHg1lFUPSI5wRyaVMZWG1UCwI2bbwz8YCo7j7iSJtd821pqadq8eLgY07Q7vq_aem_J0cpJBTSxAzItsyiEbgMdg.
39. Przed szczytem w Ankarze rosyjska propaganda wymierzona w relacje Polski z NATO. *PAP*. 08.07.2026. URL: https://www.pap.pl/aktualnosci/przed-szczytem-w-ankarze-rosyjska-propaganda-wymierzona-w-relacje-polski-z-nato.
40. Romerstein H., Garbus M. 'The Attack on I. F. Stone': An Exchange / reply by A. Brown. The New York Review of Books. 1992. Vol. 39, No. 20 (December 3). URL: https://www.nybooks.com/articles/1992/12/03/the-attack-on-if-stone-an-exchange/
41. Stowarzyszenie Demagog. *Demagog*. URL: https://demagog.org.pl/poznajmy-sie/.
42. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Warszawa, 2020. 37 s. URL: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf
43. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. *Kancelaria Prezesa Rady Ministrów*. 25.07.2025. URL: https://www.gov.pl/web/premier/strategia-bezpieczenstwa-narodowego-rzeczypospolitej-polskiej.
44. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej. 74 s. URL: https://dap-static.infor.pl/dap/000/789/745/MPO_2026-0309_zal1.pdf
45. Strategia poskiej polityki zagranicznej na lata 2026–2030. *Ministerstwo Spraw Zagranicznych*. URL: https://www.gov.pl/web/dyplomacja/strategia.
46. Torbicka K. Bezpieczeństwo Polski w XXI wieku: wyzwania, strategie i perspektywy. Paris: Fondapol, 2025. 66 s. URL: https://www.fondapol.org/app/uploads/2025/09/263_torbicka_pol_2025-07-10_v4.pdf

Авторський колектив

Алексеєнко Людмила Михайлівна, доктор економічних наук, професор, професор кафедри управління та адміністрування, Івано-Франківський навчально-науковий інститут менеджменту Західноукраїнського національного університету.

Іванченко Ольга Миколаївна, доктор юридичних наук, доцент, доцент кафедри загальної теорії права та держави, Національний університет «Одеська юридична академія».

Ільницька Уляна Вікторівна, кандидат політичних наук, доцент, доцент кафедри політології та міжнародних відносин, Національний університет «Львівська політехніка».

Квасниця Оксана Василівна, кандидат економічних наук, доцент, доцент кафедри фінансів ім. С. І. Юрія, Західноукраїнський національний університет (м. Тернопіль).

Коннова Ніна Олексіївна, кандидат філософських наук, доцент, доцент кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Копитова Олена Сергіївна, доктор юридичних наук, старший дослідник, доцент кафедри економіко-правових дисциплін Навчально-наукового інституту права і психології, Національна академія внутрішніх справ (м. Київ).

Кравченко Олена Валентинівна, доктор історичних наук, доцент, професор кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Настояща Катерина Василівна, доктор соціологічних наук, доцент, завідувач Центру соціологічних досліджень, Інститут національної стійкості та безпеки; Науково-дослідний інститут українознавства Київського національного університету імені Тараса Шевченка.

Требін Михайло Петрович, доктор філософських наук, професор, професор кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Федіна Наталія Василівна, кандидат юридичних наук, доцент, доцент кафедри адміністративно-правових дисциплін Навчально-наукового інституту права та правоохоронної діяльності, Львівський державний університет внутрішніх справ.