Політичні інститути та процеси

УДК 327.5:351.746.1:316.77(477)

DOI https://doi.org/10.5281/zenodo.18874197

Протидія російській дезінформації в Україні в умовах російсько-української війни: роль державних інституцій та громадських ініціатив

Наталія Бєлоусова,
кандидат політичних наук, кандидат фізико-математичних наук
доцент кафедри міжнародної інформації
Навчально-науковий інститут міжнародних відносин. Київського національного університету імені Тараса Шевченка,
м. Київ, Україна, https://orcid.org/0000-0002-9656-2942

Грицун Елеонора
Студентка 2-го курсу магістратури ОП “Міжнародні комунікації”,
Навчально-науковий інститут міжнародних відносин. Київського національного університету імені Тараса Шевченка,
м. Київ, Україна

Прийнято: 17.02.2026 | Опубліковано: 28.02.2026

Анотація. Російсько-українська війна показала, що дезінформація є системним елементом гібридної агресії РФ і використовується для підриву політичної стабільності, деморалізації суспільства, дискредитації міжнародної підтримки України та делегітимації державних рішень. В українському контексті інформаційні атаки поєднуються з кібератаками, дипломатичними кампаніями та психологічним тиском, що ускладнює їх виявлення й

нейтралізацію та вимагає розглядати протидію дезінформації як компонент національної безпеки. Метою даного дослідження є комплексний аналіз української моделі протидії російській дезінформації в умовах російсько-української війни з акцентом на ролі державних інституцій та громадських ініціатив, а також визначення проблемних аспектів і перспектив її подальшого розвитку.

В ході проведення дослідження було використано наступні методи: аналіз нормативно-правових актів і державних політик у сфері інформаційної безпеки; порівняльно-правовий метод (зіставлення функцій та компетенцій інституцій у різних контурах протидії); інституційний і системний підхід (розгляд протидії як взаємопов'язаної екосистеми державних і громадських акторів); контент-аналіз звітів, офіційних повідомлень та аналітичних матеріалів ключових інституцій і громадських організацій; узагальнення.

Наукова новизна дослідження полягає у тому, що протидію російській дезінформації розглянуто не як набір розрізнених заходів, а як багаторівневу інституційну модель із визначенням функціонального розподілу ролей між державним та громадським секторами і виявленням критичних вузлів взаємодії. Як результат, було проаналізовано багаторівневу модель протидії дезінформації, що поєднує стратегічно-координаційні механізми сектору національної безпеки, комунікаційну інфраструктуру інформаційної стійкості, зовнішньополітичні комунікації, контррозвідувально-правоохоронний та кібернетичний контури, а також регуляторний сегмент у сфері мовлення; окремо визначено внесок громадського сектору (моніторинг, фактчекінг, аналітика наративів, кризові комунікаційні майданчики, медіаграмотність) у протидію російській дезінформації.

Як висновок, було доведено, що ефективність української системи протидії російській дезінформації визначається не кількістю інституцій, а якістю їхньої взаємодії: синхронізацією ролей і повідомлень у кризові періоди,

 ISSN: 3041-2110

здатністю діяти превентивно, узгодженням комунікаційного та технічного реагування, а також інституціоналізацією партнерства держави й громадянського суспільства без втрати незалежності та довіри.

Ключові слова: гібридна агресія, громадянське суспільство, дезінформація, інформаційна безпека, інформаційна стійкість, медіаграмотність, російсько-українська війна, стратегічні комунікації, Україна, фактчекінг.

Countering Russian disinformation in Ukraine in the context of the Russia–Ukraine war: The role of state institutions and civil society initiatives

Nataliia Belousova,
PhD in Political Science, PhD in Physics and Mathematics
Associate Professor, Department of International Information
Educational and Scientific Institute of International Relations, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,
https://orcid.org/0000-0002-9656-2942

Eleonora Hrytsun,
Second-year Master's student,
Educational program "International Communications"
Educational and Scientific Institute of International Relations, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Abstract. The Russia–Ukraine war has shown that disinformation is a systemic element of Russia's hybrid aggression. It is used to undermine political stability, demoralize society, discredit international support for Ukraine, and delegitimize state decisions. In Ukraine, information attacks are combined with cyberattacks, diplomatic campaigns, and psychological pressure. This complicates

detection and neutralization. It also requires treating counter-disinformation as a component of national security. The aim of this study is to provide a comprehensive analysis of Ukraine's model for countering Russian disinformation in the context of the Russia–Ukraine war. The focus is on the roles of state institutions and civil society initiatives. The study also identifies key challenges and directions for further development.

The study employs the following methods: analysis of legal and regulatory acts and state policies in the field of information security; comparative legal analysis (comparing institutional functions and mandates across different response domains); an institutional and systems approach (treating counter-disinformation as an interconnected ecosystem of state and civil society actors); content analysis of reports, official communications, and analytical materials produced by key institutions and civil society organizations; and synthesis.

The scientific novelty of the study lies in conceptualizing countering Russian disinformation not as a set of fragmented measures, but as a multi-level institutional model. The paper specifies the functional division of roles between the state and civil society sectors. It also identifies critical interaction bottlenecks. These include crisis-time synchronization of communications, alignment of cyber and communication response, and the measurability of outcomes.

As a result, the paper analyzes a counter-disinformation model that integrates strategic coordination within the national security sector, the communication infrastructure of information resilience, foreign-policy communications, counterintelligence and law-enforcement components, cyber response, and media regulation. The study also outlines the contribution of civil society. This includes monitoring, fact-checking, narrative analysis, crisis communication platforms, and media literacy.

In conclusion, the study demonstrates that the effectiveness of Ukraine's system for countering Russian disinformation depends not on the number of

 ISSN: 3041-2110

institutions, but on the quality of their interaction. Key factors include synchronized roles and messages during crises, proactive action, alignment of communication and technical response, and institutionalized partnership between the state and civil society without losing independence and trust.

Keywords: *civil society, disinformation, fact-checking, hybrid aggression, information resilience, information security, media literacy, Russia–Ukraine war, strategic communications, Ukraine.*

Постановка проблеми. Російсько-українська війна засвідчила, що дезінформація є не допоміжним інструментом інформаційного впливу, а системним елементом гібридної агресії, спрямованої на підрив політичної стабільності, деморалізацію суспільства, дискредитацію міжнародної підтримки та делегітимацію державних рішень. У сучасних умовах інформаційні операції Російської Федерації поєднуються з кібератаками, дипломатичними кампаніями, психологічним тиском та використанням мережевих платформ, що суттєво ускладнює їх виявлення та нейтралізацію. В українському контексті дезінформація функціонує як інструмент стратегічного впливу на кількох рівнях: внутрішньому (суспільна довіра, мобілізація, стійкість до втрат), зовнішньому (міжнародна підтримка, санкційна політика, порядок денний у медіа) та технологічному (компрометація ресурсів, підміна контенту, поширення маніпулятивних матеріалів через цифрові платформи). У зв’язку з цим протидія дезінформації виходить за межі журналістики або фактчекінгу та набуває ознак політики національної безпеки. Наукова проблема полягає у необхідності комплексного аналізу української моделі протидії російській дезінформації як системи, що об’єднує державні інституції різного функціонального рівня та громадські ініціативи. Попри значну кількість досліджень, присвячених окремим аспектам інформаційної війни, менш дослідженим залишається питання

 ISSN: 3041-2110

взаємодії між цими акторами, розподілу ролей, механізмів координації та ефективності їхньої спільної роботи в умовах повномасштабної війни. Таким чином, актуальність теми зумовлена необхідністю осмислення українського досвіду як прикладу формування інституційної моделі інформаційної стійкості в умовах тривалого воєнного конфлікту.

Об'єктом дослідження є протидія дезінформації як складова інформаційної безпеки України в умовах російсько-української війни. Предметом дослідження є українська інституційна модель протидії російській дезінформації, зокрема функціональний розподіл ролей між державними інституціями та громадськими ініціативами, а також механізми їх взаємодії. Дослідницьке питання статті сформульовано так: яким чином організована українська система протидії російській дезінформації у воєнний час, які її ключові компоненти та які чинники визначають ефективність взаємодії між ними?

Наукова новизна дослідження полягає у тому, що протидію російській дезінформації розглянуто не як набір розрізнених заходів, а як багаторівневу інституційну модель із визначенням функціонального розподілу ролей між державним та громадським секторами і виявленням критичних вузлів взаємодії.

Формулювання мети статті. Метою статті є комплексний аналіз української моделі протидії російській дезінформації в умовах російсько-української війни з акцентом на ролі державних інституцій та громадських ініціатив, а також визначення проблемних аспектів і перспектив її подальшого розвитку. Задля досягнення даної мети, автором визначено такі завдання дослідження:

- охарактеризувати нормативну та інституційну рамку протидії дезінформації;

ISSN: 3041-2110

- проаналізувати функціональний розподіл ролей між державними органами;
- дослідити внесок громадського сектору в забезпечення інформаційної стійкості;
- окреслити ключові виклики взаємодії між цими акторами та потенційні шляхи подолання цих викликів.

Наукова гіпотеза полягає в тому, що ефективність української системи протидії російській дезінформації визначається не кількістю інституцій або окремих інформаційних продуктів, а рівнем координації між державним і громадським секторами, здатністю діяти превентивно та синхронізувати безпекові, комунікаційні й технічні механізми реагування.

Аналіз останніх досліджень і публікацій. Термін «дезінформація» увійшов у міжнародний науковий та політичний обіг у XX столітті й найчастіше пов’язується з практиками цілеспрямованого поширення неправдивих або викривлених повідомлень для введення аудиторії в оману та досягнення політичних, військових або соціальних цілей. У сучасних дослідженнях дезінформацію трактують ширше - як системне явище цифрового інформаційного середовища**,** яке функціонує через взаємодію медіа, платформ, алгоритмів і поведінкових чинників аудиторії. Саме тому актуальним є розмежування дезінформації з близькими поняттями (мізінформацією та малінформацією), а також аналіз не лише змісту повідомлень, а й механізмів їхнього масштабування та впливу.

У сучасній науковій літературі проблематику дезінформації активно розвивають іноземні дослідники, зокрема Клер Вордл і Госсейн Дерахшан (концепція “інформаційного безладу”), Стефан Левандовський і Сандер ван дер Лінден (інокуляція / пребанкінг як превентивні стратегії), Гордон Пеннікук і Девід Ренд (когнітивні механізми сприйняття та інтервенції-нагадування про перевірку достовірності “accuracy nudges”), Ульріх Еккер

 ISSN: 3041-2110

(ефективність корекції та спростувань), Кейт Старберд (мережеві й кросплатформні дезінформаційні кампанії), а також В. Ленс Беннетт і Стівен Лівінгстон (зв'язок дезінформації з політичними комунікаціями в цифровому середовищі).

В Україні дезінформація та інформаційно-психологічні впливи в контексті гібридної війни є предметом досліджень, зокрема, Георгія Почепцова (теорія інформаційних впливів і "смислові війни"), Володимира Горбуліна (інституційний вимір протидії гібридним загрозам), а також авторських колективів і експертів Національного інституту стратегічних досліджень (НІСД). Важливий прикладний внесок у документування та аналіз російської дезінформації роблять громадські ініціативи й аналітичні центри - «Детектор медіа», StopFake, Інститут масової інформації, що формують емпіричну базу для подальших наукових узагальнень.

У сучасній науковій традиції дезінформацію дедалі частіше розглядають не як "одиничний фейк", а як процес, вбудований у цифрову медіаекосистему, де його поширення визначається взаємодією платформних алгоритмів, мережевих ефектів та змін у новинному споживанні. Важливим кроком для концептуалізації проблеми стала рамка «інформаційного безладу» (information disorder), запропонована Клер Вордл та Госсейном Дерахшаном: автори розмежовують проблемний контент за критеріями правдивості та намірів і вводять три категорії - дезінформацію (умисно неправдивий контент зі шкідливим наміром), мізінформацію (неправдивий контент без умислу завдати шкоди) та малінформацію (правдивий контент, використаний маніпулятивно) [1].

Окремий блок літератури описує, чому цифрові платформи структурно сприяють масштабуванню маніпуляцій. Ірен Паскетто та ін. показують, що обмеження доступу дослідників до даних платформ суттєво ускладнює доказову перевірку того, як саме поширюються фейки, та оцінку ефективності

 ISSN: 3041-2110

інтервенцій [2]. Том Вілсон і Кейт Старберд доводять, що сучасні інформаційні атаки часто є кросплатформними: наративи мігрують між майданчиками, а вплив формується через синхронізацію каналів, повтор і "підсилення" аудиторіями [3]. Для розуміння російських інформаційних операцій це принципово, бо окремі платформи можуть виконувати різні функції - від первинного "вкиду" до легітимації через підхоплення нібито "незалежними" ресурсами.

Водночас, велика група новітніх робіт пояснює психологічні механізми віри в дезінформацію та межі спростувань. Гордон Пеннікук і Девід Ренд показують, що поширення фейків зумовлене не лише переконаннями, а й особливостями поведінки користувачів у соцмережах: у стрічці люди часто реагують автоматично й не зосереджуються на питанні достовірності**,** навіть якщо здатні відрізнити правдиве повідомлення від неправдивого. Водночас навіть коротке нагадування оцінити точність перед взаємодією з дописом (наприклад, запитання «Наскільки це повідомлення є достовірним?») помітно зменшує готовність підтримувати або поширювати недостовірний контент [4]. У контексті російсько-української війни такі "підказки" є особливо релевантними, оскільки знижують імпульсивні репости в умовах інформаційного перевантаження та високої емоційної напруги. Подібний висновок підтверджують експерименти Гордона Пеннікука та ін. [5]: коли користувачам перед взаємодією з контентом нагадують оцінювати достовірність (тобто спеціально спрямовують увагу на критерій точності), вони рідше поширюють неправдиві повідомлення й обережніше взаємодіють із сумнівними заголовками в онлайні. Тобі Прайк та Ульріх Еккер систематизують фактори, від яких залежить успішність корекції: найкраще працюють спростування, що пропонують альтернативне пояснення, пояснюють причинно-наслідкові зв'язки і повторюються в різних форматах [6]. Таким чином, у науковому дискурсі протидія дезінформації дедалі частіше

 ISSN: 3041-2110

розуміється як комбінація реактивних і превентивних інструментів, а не лише "викриття фейків".

Превентивний підхід у сучасній літературі описують через інокуляцію (або превентивне "щеплення" від дезінформації) та пребанкінг - тобто попередження маніпуляції до того, як людина з нею зіткнеться. Логіка цього підходу полягає в тому, що аудиторії заздалегідь пояснюють типові прийоми маніпуляторів (наприклад, емоційне нагнітання, підміна причинно-наслідкових зв'язків, "фальшиві експерти", виривання цитат із контексту) і показують, як їх розпізнати. У систематичному огляді Стефан Левандовський і Сандер ван дер Лінден обґрунтовують, що така "підготовка" підвищує здатність людей критично оцінювати сумнівні повідомлення, зменшує сприйнятливість до дезінформації та може застосовуватися у масштабі великих аудиторій через медіа й цифрові платформи [7]. Ракоен Мартенс та ін. додають важливий вимір - тривалість ефекту: стійкість може зберігатися в часі, але потребує підтримувальних повторів [8]. Джуліан Нейлан та ін. демонструють, що інокуляційні підходи можуть працювати і для мультимодальної дезінформації (де поєднуються текст і зображення) [9].

Окремий напрям досліджень фокусується на медіаграмотності як інструменті зниження вразливості. Ендрю Гесс та ін. на основі експериментальних даних показують, що навіть короткі онлайн-інтервенції з медіаграмотності підвищують здатність користувачів розрізняти достовірні новини та маніпулятивні/фейкові заголовки, а в частині вибірок цей ефект зберігається протягом кількох тижнів [10]. Ці результати важливі для українського контексту, де аудиторії щоденно перебувають у середовищі високої інформаційної напруги й надлишку повідомлень.

У контексті російсько-української війни додатково формується прикладна література, що аналізує конкретні патерни російських кампаній. Домінік Гайсслер та ін. на емпіричних даних показують, що в період

 ISSN: 3041-2110

повномасштабного вторгнення проросійський контент у соцмережах посилювався, зокрема, через автоматизовані акаунти (боти), які непропорційно впливали на ранні хвилі поширення повідомлень [11]. Це створює основу для висновку, що протидія дезінформації має включати не лише комунікаційні відповіді, а й моніторинг мережевої поведінки та координації.

Український науковий і аналітичний дискурс щодо дезінформації формувався під тиском практики гібридної агресії з 2014 року й поєднує академічні підходи з емпіричним моніторингом. У роботах Георгія Почепцова дезінформація розглядається як елемент "смислових війн", де об'єктом впливу виступають інтерпретаційні рамки та наративи; відповідно, спростування є необхідним, але недостатнім без системної стратегії [12]. Інституційний і безпековий вимір проблеми розкривають праці Володимира Горбуліна та матеріали Національного інституту стратегічних досліджень, де інформаційна агресія РФ трактована як складова гібридної війни та підстава для формування цілісної державної політики інформаційної безпеки [13]. Водночас у новіших українських дослідженнях 2023–2025 років посилюється фокус на прикладних механізмах протидії та інституційній реалізації стратегічних комунікацій. Так, Олена Ауліна (2023) у статті про стратегічні комунікації у протидії деструктивним російським наративам аналізує, як саме наявні інформаційні ресурси України можуть використовуватися для нейтралізації наративних конструкцій противника, і підкреслює значення системної роботи з наративами, а не лише з окремими повідомленнями [47]. У практико-орієнтованому вимірі важливим є аналітичний звіт Романа Горбика, Діани Дуцик і Сергія Шалайського (2023) про ефективність протидії російській дезінформації в умовах повномасштабної війни, де узагальнюються спостереження щодо поточних інструментів реагування та окреслюються фактори, які підсилюють або послаблюють результативність протидії [48].

ISSN: 3041-2110

Зовнішньополітичний вимір і транскордонний характер російських інформаційних операцій відображено в дослідженні НІСД (2024) про російські дезінформаційні кампанії в Європі, що показує масштаб і логіку таких кампаній проти держав та інституцій ЄС, а також їхню релевантність для формування міжнародного порядку денного навколо війни [49]. Окремо важливою є робота Миколи Хилька (2025), присвячена трансформації комунікаційних стратегій у секторі безпеки та оборони України під впливом повномасштабної агресії РФ: автор підкреслює зростання вимог до оперативності, достовірності та координації інформаційних потоків в умовах постійної дезінформації та кібератак [50]. Важливий внесок роблять і громадські ініціативи та аналітичні центри (**«**Детектор медіа»**,** StopFake**,** IMI**)**, які виробляють регулярні моніторинги наративів, аналіз кампаній і оцінку реакцій держави та суспільства [14]. Саме на поєднанні цих підходів - платформного, психологічного, превентивного та інституційного - ґрунтується подальший аналіз ролі державних інституцій і громадських ініціатив у протидії російській дезінформації.

Виділення невирішених раніше частин загальної проблеми. Попри значну кількість робіт, присвячених російській дезінформації та інформаційній агресії проти України, у дослідницькому полі досі переважають підходи, що аналізують або окремі наративи й фейки, або окремі інструменти протидії (фактчекінг, медіаграмотність, стратегічні комунікації). Натомість менш опрацьованим залишається інституційний вимір проблеми - як саме функціонує українська модель протидії дезінформації як екосистема, в якій поєднуються стратегічно-координаційні механізми сектору національної безпеки, комунікаційна інфраструктура інформаційної стійкості, зовнішньополітичні комунікації, контррозвідувально-правоохоронний компонент, кіберконтур та медіарегуляція, а також потужний громадський сектор. У межах цієї ширшої рамки окремої уваги потребують ті фрагменти

 ISSN: 3041-2110

загальної проблеми, які залишаються вразливими саме в практиці воєнного часу: насамперед це питання координації та синхронізації ролей і повідомлень між різними державними суб'єктами під час кризових хвиль. Не менш важливою є прогалина в частині узгодження комунікаційного й технічного реагування, адже в сучасних операціях дезінформаційні хвилі нерідко підсилюються кібератаками або компрометацією офіційних ресурсів. Окремим невирішеним аспектом є якість і сталість взаємодії державного та громадського сектору: українська практика демонструє значний внесок незалежного моніторингу, фактчекінгу, аналітики, кризових комунікаційних майданчиків і медіаграмотності, однак у багатьох випадках партнерство функціонує нерівномірно й потребує більш чітких форматів взаємодоповнення ролей без втрати незалежності й довіри до громадських ініціатив. Таким чином, серед невирішених аспектів проблеми залишаються: недостатня координація між державними органами під час кризових інформаційних хвиль; потреба в уточненні та узгодженні нормативно-правових процедур реагування на інформаційні загрози; а також вдосконалення механізмів стратегічних комунікацій, зокрема стандартизація кризових повідомлень і синхронізація комунікаційного та технічного реагування на інциденти. Саме ці компоненти зумовлюють практичну вразливість системи та визначають фокус подальшого аналізу.

Виклад основного матеріалу дослідження. Протидія російській дезінформації в Україні в умовах російсько-української війни сформувалася як комплексна інституційна модель, у якій інформаційна безпека розглядається не як суто медійна проблема, а як складова національної безпеки. Нормативну рамку цієї моделі визначає Стратегія інформаційної безпеки, введена в дію Указом Президента України, яка окреслює цілі державної політики у сфері захисту інформаційного простору та реагування на деструктивні інформаційні впливи, включно з дезінформацією як

 ISSN: 3041-2110

інструментом гібридної агресії [15]. Важливо, що така рамка задає підхід до проблеми не як до «пошуку і спростування окремих фейків», а як до системної роботи із середовищем: інституцій, процедур, комунікацій та суспільної стійкості. Саме це дозволяє пояснити, чому в Україні функції протидії дезінформації розподілені між різними органами і секторами, а ефективність залежить від узгодженості їхніх дій.

У державному секторі координаційне ядро протидії дезінформації зосереджене на рівні стратегічних рішень у системі національної безпеки. У цьому контексті Рада національної безпеки і оборони України виступає міжвідомчим майданчиком, який визначає дезінформацію як загрозу і формує загальні рамки реагування в межах безпекової політики [15]. Інституційним інструментом, створеним саме для посилення державної спроможності виявляти та аналізувати дезінформаційні загрози, став Центр протидії дезінформації (ЦПД) як робочий орган РНБО: його створення закріплено рішенням РНБО, введеним у дію Указом Президента [16], а функції й повноваження деталізовано в Положенні про ЦПД, затвердженому окремим Указом [17]. З огляду на це ЦПД доцільно трактувати передусім як аналітико-координаційний вузол, а не як «медіа» чи «фактчек-проєкт». Його ключова відмінність полягає в тому, що він має працювати не лише з видимою частиною проблеми (контентом), а з її структурою: кампаніями, каналами поширення, акторами впливу та їхніми цілями. Практичний вимір діяльності ЦПД проявляється через регулярні та тематичні звіти/огляди, де фіксуються ключові тенденції, домінантні наративи, інструменти поширення та цільові аудиторії. У таких матеріалах принципово важливо, що ЦПД не зводить проблему до «перевірки фактів», а намагається показати логіку кампанії: як один і той самий меседж відтворюється різними каналами, якими «підсилювачами» він користується (анонімні телеграм-канали, проросійські спікери, псевдоекспертні ресурси), які емоції експлуатує (страх, злість, втома,

ISSN: 3041-2110

недовіра) і який очікуваний ефект може мати [18]. Окреме значення мають підсумкові публічні звіти/пресконференції ЦПД про результати роботи за рік: вони фіксують пріоритетні загрози, демонструють інституційну безперервність і дозволяють суспільству/партнерам оцінювати напрямки фокусу держави [19]. Разом із цим, для функціонування моделі недостатньо стратегічного контуру - потрібна управлінська реалізація політики, яка передбачає узгодження між відомствами, ресурсне забезпечення та підтримку процедур міжвідомчої взаємодії. Саме тут виявляється принципова різниця між координаційними ролями РНБО і Кабінету Міністрів України: якщо РНБО задає стратегічні рамки та безпекову пріоритизацію, то урядова вертикаль забезпечує перетворення цих рамок у конкретні плани та управлінські механізми реалізації політики [1]. На нашу думку, ця відмінність є критично важливою для оцінки ефективності: у кризових ситуаціях (масовані обстріли, резонансні події на фронті, інформаційні хвилі навколо мобілізації чи міжнародної допомоги) ризик неузгодженості різних органів зростає. Тому ефективна протидія дезінформації потребує не лише аналітики про загрози, а й взаємодії між установами - чітких правил, каналів обміну інформацією і ролей у кризовому реагуванні. Комунікаційний контур державної протидії доповнюється розвитком стратегічних комунікацій та інформаційної стійкості. Центр стратегічних комунікацій та інформаційної безпеки «SPRAVDI» створено при Міністерстві культури та інформаційної політики України як державний механізм протидії дезінформації у взаємодії держави й громадянського суспільства; його робота сфокусована на комунікаційній протидії зовнішнім інформаційним загрозам**,** насамперед інформаційним атакам Російської Федерації. Центр стратегічних комунікацій та інформаційної безпеки «SPRAVDI» вибудовує протидію дезінформації не лише через контрмеседжі, а як інфраструктуру інформаційної стійкості, де поєднані оперативні спростування, аналітика наративів та підвищення

 ISSN: 3041-2110

спроможності комунікаційних команд держави. Логіка роботи Центру відображена у структурі сайту: «Антифейк» (публікації зі спростуванням і поясненням маніпуляцій), «Аналітика» (дослідження/моніторинг), «Тренінги» (Школа СтратКому, проведені навчання, посібники), а також «Довідник з безпеки» як прикладний ресурс для інформаційної та поведінкової обережності [20]. З погляду протидії дезінформації принципово, що SPRAVDI працює не тільки з окремими «фактами», а з наративами як повторюваними конструкціями впливу. У дослідженні «Антиєвропейські наративи Кремля: мапа інформаційних загроз для України» Центр формулює й аналізує п'ять ключових антиєвропейських наративів, які використовуються у російських інформаційних втручаннях (FIMI), показуючи їхню мету - посилення антиєвропейських настроїв і негативних упереджень щодо ЄС [21]. На нашу думку, цінність формату «мапи загроз» у воєнний час полягає в тому, що він дає можливість працювати на випередження: прогнозувати, які рамки й меседжі активізуються під конкретні політичні події, і готувати превентивні пояснювальні комунікації замість запізнілого реагування. Другий ключовий контур - підвищення спроможності держави та місцевого самоврядування діяти під час інформаційних атак. У межах «Школи СтратКому та інформаційної безпеки» SPRAVDI прямо вказує, що навчає держслужбовців протидії дезінформації з опорою на британський підхід Resist 2.0, а також застосовує модель OASIS як покроковий алгоритм планування і реалізації комунікаційної стратегії [22]. Навчальний напрям Центр підкріплює прикладними посібниками для комунікаційників органів влади. Зокрема, в матеріалах про посібник «Комунікації у роботі державних органів влади та органів місцевого самоврядування. Сучасні практики» зазначено, що він охоплює повний цикл створення комунікаційних кампаній і особливості кризових комунікацій [23]. У контексті дезінформації це має практичний ефект: значна частина атак РФ «грає» на прогалинах у поясненні рішень і

процедур, тоді як стандартизовані підходи дозволяють швидше закривати інформаційні вакууми й не залишати їх телеграм-каналам або псевдоекспертам. Додатково прикладний сегмент «Довідника з безпеки» (зокрема матеріали на кшталт брошури про дії у разі надзвичайної ситуації або війни) підтримує базову поведінкову готовність і знижує вразливість аудиторій до панічних та маніпулятивних повідомлень [24].

Окремий сегмент комунікаційної архітектури функціонує в секторі безпеки й оборони. Діяльність Міністерства оборони України в частині стратегічних комунікацій забезпечується профільним структурним підрозділом - Департаментом стратегічних комунікацій, який формує комунікаційну політику в межах оборонного відомства та забезпечує системність комунікацій у чутливих питаннях війни [25]. У переліку завдань департаменту прямо зафіксовано**:** координацію розвитку системи стратегічних комунікацій у МОУ/ЗСУ/ДССТ у складі загальнодержавної системи; реалізацію завдань державної інформаційної політики у сфері оборони; розробку й координацію комунікаційних стратегій та інформаційних кампаній; участь у формуванні оборонної свідомості й громадянської стійкості; а також розвиток і підтримку медіаресурсів МОУ, включно з офіційними виданнями[25].З погляду протидії російській дезінформації цей перелік завдань показує, що військові стратегічні комунікації - це не “супровід новин”, а механізм управління ризиками в найуразливішій тематиці війни (втрати, мобілізація, забезпечення, міжнародна допомога, внутрішні конфлікти тощо). На нашу думку, ключова функція департаменту тут - зменшувати розсинхронізацію повідомлень між МОУ, ЗСУ й суміжними структурами, бо саме в таких розривах найшвидше розмножуються чутки та ворожі наративи. Тому в оборонному сегменті стратегічні комунікації набувають ознак елементу обороноздатності: вони не лише інформують, а й запобігають дезорганізації, деморалізації та панічним настроям**,** які противник

 ISSN: 3041-2110

намагається індукувати через емоційні вкиди та анонімні канали.

Окремий вимір державної системи протидії дезінформації формує діяльність Міністерства закордонних справ України, оскільки саме МЗС відповідає за зовнішньополітичні комунікації та представлення позиції України в міжнародному інформаційному просторі. У практичному вимірі це проявляється через публічні заяви МЗС, спрямовані на фіксацію й спростування конкретних російських кампаній за кордоном (наприклад, у матеріалі щодо системної дезінформаційної кампанії РФ у країнах Африки МЗС прямо описує інтенсифікацію дезінформації та підкреслює її цілі - дискредитувати Україну і вплинути на ставлення іноземних аудиторій) [26]. Одночасно МЗС запускає проєкти публічної дипломатії, спрямовані на довготривале зменшення вразливості міжнародних аудиторій: показовим прикладом є ініціатива Nations Against Disinformation, що позиціонується як креативний інструмент підвищення обізнаності про небезпеку дезінформації та її наслідки для держав [27]. На нашу думку, специфіка МЗС у системі протидії дезінформації полягає в тому, що воно працює не лише з “фактами”, а з міжнародним порядком денним: завданням є не просто спростувати фейк, а не допустити, щоб російська рамка (“втома Заходу”, “внутрішній конфлікт”, “делегітимність оборони”) стала домінантною в іноземних медіа та політичних дискусіях. Саме тому інструменти МЗС поєднують дипломатичну реакцію (заяви, пояснення, комунікація з урядами й міжнародними організаціями) з проактивним формуванням стійкості (публічні кампанії й міжнародні ініціативи). У цьому сенсі МЗС виступає ключовим суб’єктом формування зовнішньої інформаційної стійкості України та доповнює внутрішні механізми стратегічних комунікацій держави.

Водночас державна модель протидії дезінформації не може зводитися лише до комунікацій. У системі інформаційної безпеки воєнного часу критично важливий контррозвідувально-правоохоронний компонент, який

реагує тоді, коли інформаційні впливи виходять за межі «медійного шуму» й стають елементом підривної діяльності - наприклад, забезпечують вербування, координацію агентурних мереж, провокують диверсійні дії або спрямовані на зрив управлінських/мобілізаційних рішень. Саме в цій площині доцільно аналізувати роль Служби безпеки України, завдання та повноваження якої визначені спеціальним законом, а контррозвідувальна діяльність - окремим профільним законом [28-29]. На відміну від комунікаційних інституцій, СБУ працює не з «корекцією повідомлень», а з юридично значущими загрозами і застосовує процесуальні механізми реагування, коли дезінформаційний контент пов'язаний з організаторами, інфраструктурою впливу або іншими формами співпраці з державою-агресором. На нашу думку, системний сенс цього компонента полягає в тому, що дезінформація часто є лише видимою частиною ширшої операції: вона може маскувати підготовку реальних дій або створювати «інформаційне прикриття» для вербування та координації. Тому ефективність протидії залежить не тільки від спростувань і стратегічних комунікацій, а й від здатності держави обмежувати організаторів та канали, через які вибудовується вплив. Додатково важливо, що правова рамка воєнного часу посилила відповідальність за колабораційну діяльність, що включає й інформаційні заходи, спрямовані на підтримку держави-агресора (як окрема юридична площина) [30]. У сукупності це дозволяє розглядати СБУ як елемент не лише «безпеки», а й інформаційної стійкості, коли мова йде про нейтралізацію не окремих вкидів, а їхніх організованих мереж і механізмів.

Суміжним, але критично важливим елементом державної екосистеми протидії дезінформації є кіберзахист, оскільки сучасні інформаційні операції РФ дедалі частіше поєднуються з технічними атаками: зламами офіційних ресурсів, витоками даних, підміною контенту, фішингом, DDoS-атаками або компрометацією акаунтів, які потім використовуються як «доказова оболонка» для маніпулятивних наративів. У цьому контексті ключовим

ISSN: 3041-2110

державним інструментом виступає CERT-UA - національна команда реагування на комп'ютерні інциденти, яка на офіційному рівні визначає свої функції як реагування на кіберінциденти, аналіз загроз та надання рекомендацій, а також координацію взаємодії у сфері кіберзахисту [31]. Практичний вимір цієї роботи добре видно на прикладі публічних рекомендацій CERT-UA щодо захисту вебресурсів (організаційні й технічні заходи посилення безпеки сайтів), які зменшують ризик «інформаційних інцидентів», що виникають саме через компрометацію офіційних каналів [32]. Додатково важливо, що на рівні державних методичних документів закріплюється необхідність підготовки та реагування на кіберінциденти/кібератаки у взаємодії з CERT-UA, що посилює інституційну спроможність реагування [33]. Хоча CERT-UA не є «антидезінформаційним органом» у вузькому сенсі, його діяльність напряму впливає на стійкість інформаційної інфраструктури, без якої комунікаційні відповіді часто втрачають ефективність. На нашу думку, саме тут формується один із ключових викликів: у реальних кризах кібер-інцидент і дезінформаційна хвиля можуть бути елементами однієї операції. Якщо держава не синхронізує технічне реагування (локалізація інциденту, відновлення ресурсів) із комунікаційним (пояснення, попередження, інструкції для населення), то російська сторона отримує додатковий ефект - паніку і хаос як множник шкоди. Окремим елементом державної екосистеми є медіарегуляція та інституційний нагляд за сферою телерадіомовлення. В Україні функції такого нагляду виконує Національна рада України з питань телебачення і радіомовлення, правові засади діяльності якої визначені законом [34]. У контексті протидії дезінформації роль регулятора доцільно описувати як забезпечення стандартів і дотримання вимог законодавства у сфері мовлення в межах компетенції. У період воєнного стану ця роль стає особливо чутливою: Нацрада, з одного боку, підтримує безперервність мовлення

 ISSN: 3041-2110

(регуляторні рішення щодо процедур у воєнний час), а з іншого - фіксує порушення та застосовує санкційні механізми за результатами моніторингу (включно зі спеціальними процедурами, які діють у період воєнного або надзвичайного стану) [35]. Навіть якщо ключові “битви” дезінформаційних кампаній відбуваються в соцмережах і месенджерах, традиційні медіа продовжують формувати порядок денний, а отже дотримання правил і відповідальність мовників зменшують ризик легалізації маніпулятивних меседжів через ефірні канали. Додатково показовими є аналітичні продукти регулятора, зокрема спільні ініціативи з іншими державними структурами у сфері протидії інформаційним загрозам (наприклад, аналітичні матеріали щодо мови ворожнечі як фактора ризику в інформаційному середовищі) [36].

Однак жодна державна модель протидії дезінформації не може бути ефективною без взаємодії з громадянським суспільством, яке забезпечує гнучкість, швидкість реагування, накопичення емпіричної бази і незалежну експертизу. В Україні сформувався потужний сегмент громадських ініціатив і організацій, які працюють у різних функціональних напрямах: моніторинг інформаційного простору, фактчекінг, аналітика наративів, освітньо-просвітницька діяльність, підтримка медіаграмотності та захист стандартів журналістики. Така різноманітність важлива, тому що дезінформація РФ є багатоформатною: вона включає і «побутові» фейки, і стратегічні наративи, і маніпулятивні інтерпретації, і психологічний тиск. Відповідно, ефективна протидія потребує не одного універсального механізму, а системи, де різні інструменти взаємодоповнюють один одного.

Показовим прикладом аналітично-моніторингового напряму є діяльність ГО «Детектор медіа», місія якої прямо включає протидію дезінформації та пропаганді поряд із підвищенням якості медіа й медіаграмотності суспільства [37]. Важливо, що у воєнний час організація підтримує системний моніторинг: з 24 лютого 2022 року «Детектор медіа»

регулярно документує російську дезінформацію про війну, відстежуючи як український сегмент соцмереж, так і кремлівські медіа [38]. Принциповим є саме «серійність» такого підходу: він дозволяє бачити не окремий вкид, а динаміку повторюваних сюжетів, «піки» активізації та еволюцію аргументації. Окрему аналітичну цінність додають інструменти вимірювання впливу: наприклад, у звіті про Індекс інформаційного впливу описано підхід до оцінювання можливостей РФ здійснювати інформаційний вплив у різних країнах і логіку роботи з індикаторами, які роблять проблему вимірюваною, а не інтуїтивною [39]. На нашу думку, у воєнний час такий інструментарій важливий тим, що переводить протидію з режиму «реагувати на все» у режим пріоритизації: що є системним, що - випадковим шумом, які теми РФ намагається «втримати» у порядку денному, а які - вкидає ситуативно.

Не менш значущим є внесок Інституту масової інформації (IMI), який працює на перетині моніторингу медіасередовища, документування порушень та формування доказової бази щодо ризиків для журналістів і медіа. Зокрема, IMI веде регулярний моніторинг у форматі «Барометра свободи слова», в якому фіксує злочини та порушення проти журналістів і медіа, пов’язані з війною [40]. Окрім цього, IMI у своїх аналітичних матеріалах фіксує випадки поширення російської пропаганди, мови ворожнечі та публічних заяв, що містять ознаки підбурювання до насильства проти українців. У низці матеріалів IMI аналізує феномен так званої «геноцидної риторики» в російському інформаційному просторі, наголошуючи, що публічні заклики до знищення української державності або заперечення існування української нації мають системний характер і можуть розглядатися не лише як пропаганда, а як елемент підбурювання до міжнародного злочину [41]. Такий підхід виходить за межі класичного медіамоніторингу: організація фактично формує масив документованих кейсів, які потенційно можуть бути використані в міжнародно-правовому вимірі. З аналітичної точки зору це важливо для нашої

моделі протидії дезінформації з двох причин. По-перше, мова йде не лише про “фейк”, а про системну делегітимацію існування України як політичного суб’єкта - тобто про стратегічний рівень впливу. По-друге, документування таких висловлювань створює доказову базу, яка дозволяє переводити питання з площини інформаційної дискусії у площину юридичної відповідальності.

Фактчекінг і деконструкція наративів становлять окремий напрям громадського сектору, у якому показовою є діяльність StopFake. Проєкт, запущений у березні 2014 року, від початку зосередився на перевірці та спростуванні неправдивих повідомлень про події в Україні, що поширювалися в межах російських інформаційних кампаній [42]. З часом StopFake трансформувався у багатофункціональний інформаційний хаб, який не обмежується реактивним «викриттям фейків», а здійснює системний аналіз кремлівської пропаганди та методів інформаційного впливу - зокрема щодо України, країн Європейського Союзу та пострадянського простору [42]. Важливим елементом діяльності StopFake є освітній і міжнародний вимір: представники проєкту беруть участь у професійних дискусіях і публічних заходах, пов’язаних із протидією дезінформації, а також поширюють матеріали кількома мовами, що забезпечує доступ міжнародної аудиторії до перевіреної інформації та сприяє ширшому розумінню російських дезінформаційних практик. На нашу думку, поєднання спростувань із поясненням маніпулятивних прийомів та просвітницькими практиками показує, що громадські ініціативи працюють не лише з окремими фейками, а й із довгостроковим підвищенням інформаційної стійкості суспільства - ключовою умовою протидії російській пропаганді в умовах війни.

Окрему роль у громадському секторі відіграють інституції, що забезпечують комунікаційний «міст» між державою, медіа, експертним середовищем і суспільством. Український кризовий медіа-центр (УКМЦ) описує свій пресцентр як майданчик, що проводить брифінги, дискусії та

 ISSN: 3041-2110

круглі столи на регулярній основі [43]. У контексті протидії дезінформації цінність такого формату полягає в тому, що він скорочує «час до пояснення»: коли суспільство отримує легітимний канал для зрозумілих і послідовних роз'яснень, зменшується простір для хаотичних інтерпретацій і «паразитування» дезінформації на інформаційних прогалинах. На нашу думку, це впливає на стійкість не меншою мірою, ніж спростування фейків: дезінформація найкраще працює там, де бракує ясного і стабільного публічного пояснення.

Ще один важливий сегмент - незалежна аналітика у сфері безпеки й оборони, яка допомагає суспільству інтерпретувати складні процеси й знижувати вразливість до маніпулятивних трактувань. У цьому контексті показовою є діяльність Центру оборонних стратегій, який визначає себе як незалежну аналітичну організацію, спрямовану на підтримку національної безпеки й оборони через участь у формуванні політик і стратегій із залученням незалежного експертного середовища [44]. З аналітичної точки зору, цінність таких інституцій - у «перекладі» складних тем (переговори, мобілізація, військова допомога, стратегія партнерів) у зрозумілу рамку, яка конкурує з простими емоційними поясненнями пропаганди. Там, де є дефіцит зрозумілих пояснень, зростає вплив чуток і пропагандистських «інтерпретацій» - отже незалежна аналітика виступає профілактикою інформаційної вразливості.

Нарешті, довгостроковий рівень протидії дезінформації пов'язаний із медіаграмотністю та просвітою. У цьому напрямі показовою є діяльність Академії української преси: в описі проєкту з медіаграмотності зазначено розробку навчальної програми, підготовку тренерів у регіонах і проведення тренінгів для великої кількості громадян, а також інформаційної кампанії щодо протидії пропаганді й маніпуляціям [45]. Паралельно громадський сектор реалізує масштабні комунікаційні кампанії, спрямовані на підвищення стійкості до дезінформації: зокрема «Інтерньюз-Україна» публічно комунікує

запуск соціальної кампанії «ДезАут», яка прямо позиціонується як інструмент допомоги українцям у підвищенні стійкості до дезінформації та розвитку критичного мислення [46]. На нашу думку, саме тут протидія переходить із реакції на контент у формування «когнітивних бар'єрів»: суспільство стає менш вразливим не лише до конкретної хвилі фейків, а до повторюваних маніпулятивних схем, які РФ відтворює під різні інформаційні приводи.

Загалом аналіз діяльності державних інституцій та громадських ініціатив дозволяє зробити кілька ключових узагальнень щодо того, як саме працює українська модель протидії російській дезінформації. Ми з'ясували, що модель державного реагування є багаторівневою: стратегічна координація у сфері безпеки (РНБО та ЦПД), управлінська реалізація політики (урядовий контур), комунікаційна протидія та стратегічні комунікації (профільні центри й міністерства), зовнішньополітичний вимір (МЗС), правоохоронно-контррозвідувальний компонент (СБУ), суміжна підтримка кіберзахисту (CERT-UA) та медіарегуляції (Нацрада) формують взаємодоповнювальну систему, яка не зводиться до одного інструмента. Громадський сектор забезпечує те, що держава не завжди може робити достатньо швидко або гнучко: незалежний моніторинг і аналітику (Detector Media, IMI), фактчек і деконструкцію наративів (StopFake), кризові комунікаційні майданчики (УКМЦ), а також незалежну експертизу в сфері безпеки й оборони та освітню складову стійкості (ЦОС, АУП, Internews Ukraine).

Разом із тим практика воєнного часу підтверджує, що найбільш уразливим параметром системи є не наявність чи відсутність окремих інституцій, а здатність діяти як єдина мережа - синхронізувати повідомлення, швидко обмінюватися інформацією, узгоджувати ролі та реагувати на комплексні операції, у яких дезінформація поєднується з технічними інцидентами та психологічним тиском. Саме в цих точках взаємодії проявляються ключові «болі» української системи протидії.

ISSN: 3041-2110

Насамперед, проблемною зоною є обмежена вимірюваність результатів антидезінформаційних практик. Значна частина інституційних продуктів має описовий характер (огляди, спростування, аналітичні матеріали, рекомендації), однак зв'язок між цими діями та реальними змінами в поведінці аудиторій (зменшення поширення фейків, зростання довіри до офіційних каналів, зниження підтримки ворожих наративів) часто залишається непрямим або фрагментарним. Це ускладнює оцінку ефективності й у короткострокових кризах, і в довгостроковій перспективі інформаційної стійкості.

Окрему групу ризиків формує розрив між технічним і комунікаційним реагуванням. Кібератаки, компрометація ресурсів чи підміна контенту здатні швидко перетворюватися на «доказову оболонку» для маніпулятивних наративів. Якщо технічна локалізація інциденту не супроводжується зрозумілими публічними поясненнями (що сталося, як відрізнити підміну, які канали є офіційними, що робити користувачам), противник отримує додатковий ефект - паніку, хаос і недовіру як множник шкоди.

Ще одна проблемна зона - нерівномірність і неформалізованість взаємодії держави та громадського сектору. Громадські ініціативи забезпечують швидкий моніторинг, фактчекінг, аналітику наративів, кризові майданчики й медіаосвіту, однак механізми системної взаємодії з державними структурами не завжди є стабільними. У результаті в окремі періоди співпраця може бути продуктивною, а в інші - слабшати або залежати від ситуативних контактів і проєктної логіки. Нарешті, суттєвим викликом для всієї системи залишається поширення дезінформації в месенджерах та локальних напівзакритих спільнотах, де офіційні комунікації та фактчекінг мають обмежене проникнення. У поєднанні з фактором інформаційної втоми й підвищеної тривожності у воєнний час це підсилює схильність до імпульсивного поширення емоційних повідомлень і знижує ефективність навіть якісних спростувань, якщо вони надходять запізно або не в тому каналі.

ISSN: 3041-2110

Висновки. Проведене дослідження дозволяє стверджувати, що в Україні протидія російській дезінформації еволюціонувала від точкових спростувань до більш цілісної практики інформаційної стійкості, у межах якої дезінформація розглядається як інструмент гібридної агресії та фактор національної безпеки. Аналіз показав, що ця модель функціонує як екосистема взаємодоповнюваних контурів: безпеково-координаційного (РНБО, ЦПД), комунікаційного (SPRAVDI та комунікаційні підрозділи), зовнішньополітичного (МЗС), контррозвідувально-правоохоронного (СБУ), кібернетичного (CERT-UA) та регуляторного у сфері мовлення (Нацрада), при цьому громадянське суспільство забезпечує незалежний моніторинг, фактчекінг, аналітику наративів, кризові комунікаційні майданчики та навчання медіаграмотності. Дослідження засвідчує: найбільш уразливим місцем системи є не кількість інституцій, а їхня здатність діяти узгоджено - синхронізувати повідомлення, швидко обмінюватися даними й реагувати на комплексні атаки, що поєднують дезінформацію з технічними інцидентами та психологічним тиском. Саме ця потреба в інституційній узгодженості і вимірюваності результатів є ключовим містком до подальших практичних і наукових розвідок.

Практичні рекомендації за результатами дослідження полягають у посиленні кризової синхронізації комунікацій між ключовими інституціями, узгодженні технічного (кібер) та комунікаційного реагування під час інцидентів, а також у формуванні індикаторів ефективності антидезінформаційних заходів, що дозволять оцінювати вплив не лише за кількісними показниками, а за змінами в поведінці аудиторій. Отримані висновки корелюють із метою і завданнями статті, оскільки дозволяють описати модель протидії дезінформації як цілісну систему та визначити ключові параметри її результативності.

ISSN: 3041-2110

Перспективи подальших розвідок у цьому напрямі пов'язані з (1) розробкою підходів до оцінювання результативності антидезінформаційних інструментів та формуванням індикаторів ефективності; (2) дослідженням механізмів кризової синхронізації комунікацій між інституціями та виробленням моделей швидкого реагування; (3) аналізом узгодження технічного (кібер) та комунікаційного контурів у межах комплексних операцій; (4) вивченням моделей партнерства, які зберігають незалежність громадського сектору, але забезпечують регулярний обмін даними (держава - координація та повноваження; громадські організації - незалежний моніторинг, експертиза, просвітницькі практики); (5) дослідженням ефективних форматів медіаграмотності та інформаційної стійкості для різних цільових груп в умовах тривалого конфлікту.

Список використаних джерел.

1. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe report. 2017.

2. Pasquetto I. V., Swire-Thompson B., Amazeen M. A., et al. Tackling misinformation: What researchers could do with social media data. Harvard Kennedy School Misinformation Review. 2020. Vol. 1, No. 8. DOI https://doi.org/10.37016/mr-2020-49

3. Wilson T., Starbird K. Cross-Platform Disinformation Campaigns: Lessons Learned and Next Steps. Harvard Kennedy School Misinformation Review. 2020. Vol. 1, No. 1. DOI https://doi.org/10.37016/mr-2020-002

4. Pennycook G., McPhetres J., Zhang Y., Lu J. G., Rand D. G. Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention. Psychological Science. 2020. Vol. 31, No. 7. P. 770–780. DOI https://doi.org/10.1177/0956797620939054

5. Pennycook G., Epstein Z., Mosleh M., Arechar A. A., Eckles D., Rand D. G. Shifting attention to accuracy can reduce misinformation online. Nature. 2021. Vol. 592, No. 7855. P. 590–595. DOI https://doi.org/10.1038/s41586-021-03344-2

6. Prike T., Ecker U. K. H. Effective correction of misinformation. Current Opinion in Psychology. 2023. Vol. 54. 101712. DOI https://doi.org/10.1016/j.copsyc.2023.101712

7. Lewandowsky S., van der Linden S. Countering Misinformation and Fake News Through Inoculation and Prebunking. European Review of Social Psychology. 2021. Vol. 32, No. 2. P. 348–384. DOI https://doi.org/10.1080/10463283.2021.1876983

8. Maertens R., Roozenbeek J., Basol M., van der Linden S. Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments. Journal of Experimental Psychology: Applied. 2021. Vol. 27, No. 1. P. 1–16. DOI https://doi.org/10.1037/xap0000315

9. Neylan J., Biddlestone M., Roozenbeek J., van der Linden S. How to “inoculate” against multimodal misinformation: A conceptual replication of Roozenbeek and van der Linden (2020). Scientific Reports. 2023. Vol. 13, No. 1. 18273. DOI https://doi.org/10.1038/s41598-023-43885-2

10. Guess A. M., Lerner M., Lyons B., Montgomery J. M., Nyhan B., Reifler J., Sircar N. A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. Proceedings of the National Academy of Sciences of the United States of America. 2020. Vol. 117, No. 27. P. 15536–15545. DOI https://doi.org/10.1073/pnas.1920498117

11. Geissler D., Bär D., Pröllochs N., Feuerriegel S. Russian propaganda on social media during the 2022 invasion of Ukraine. EPJ Data Science. 2023. Vol. 12, No. 1. 35. DOI https://doi.org/10.1140/epjds/s13688-023-00414-5

12. Почепцов Г. Г. Інформаційні війни. Київ: Вид. дім «Києво-Могилянська академія», 2015.

13. Горбулін В. П. (ред.). Світова гібридна війна: український фронт. Київ: Національний інститут стратегічних досліджень, 2017.

14. Президент України. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021.

15. Президент України. Про рішення РНБО від 11.03.2021 «Про створення Центру протидії дезінформації» : Указ Президента України від 19.03.2021 № 106/2021.

16. Президент України. Положення про Центр протидії дезінформації : Указ Президента України від 07.05.2021 № 187/2021.

17. Центр протидії дезінформації при РНБО України. Звіти / аналітичні матеріали (офіційний розділ). URL: https://cpd.gov.ua/ (дата звернення: 26.11.2025).

18. Центр протидії дезінформації при РНБО України. Підсумки роботи (офіційні матеріали/пресконференції/звіт за рік). URL: https://cpd.gov.ua/ (дата звернення: 26.11.2025).

19. SPRAVDI. Центр стратегічних комунікацій та інформаційної безпеки (офіційний сайт). URL: https://spravdi.org/ (дата звернення: 26.11.2025).

20. Міністерство культури та стратегічних комунікацій України. Центр стратегічних комунікацій та інформаційної безпеки (SPRAVDI) (опис проєкту). URL: https://mincult.gov.ua/projects/a-href-https-spravdi-gov-ua-tsentr-stratehichnykh-komunikatsiy-ta-informatsiynoi-bezpeky-a/ (дата звернення: 29.11.2025).

21. SPRAVDI. Антиєвропейські наративи Кремля: мапа інформаційних загроз для України : дослідження. 2025. URL: https://spravdi.org/wp-content/uploads/2025/04/doslidzhennya-antyyevropejski-

 ISSN: 3041-2110

naratyvy-kremlya.-mapa-informaczijnyh-zagroz-dlya-ukrayiny.pdf (дата звернення: 29.11.2025).

22. SPRAVDI. Школа СтратКому та інформаційної безпеки (Resist 2.0; OASIS). URL: https://spravdi.org/treningy-dlya-derzhsluzhbovcziv/ (дата звернення: 29.11.2025).

23. SPRAVDI. Посібник «Комунікації у роботі державних органів влади та органів місцевого самоврядування. Сучасні практики». 2026. URL: https://spravdi.org/posibnyk-komunikacziyi-u-roboti-derzhavnyh-organiv-vlady-ta-organiv-misczevogo-samovryaduvannya-suchasni-praktyky/ (дата звернення: 29.11.2025).

24. SPRAVDI. Брошура «У разі надзвичайної ситуації або війни». 2022. URL: https://spravdi.org/broshura-u-razi-nadzvychajnoyi-sytuacziyi-abo-vijny/ (дата звернення: 29.11.2025).

25. Міністерство оборони України. Департамент стратегічних комунікацій (офіційна сторінка; опис функцій і завдань). URL: https://mod.gov.ua/pro-nas/aparat-ministerstva-oboroni/departament-strategichnih-komunikaczij (дата звернення: 30.11.2025).

26. Міністерство закордонних справ України. Заява МЗС щодо системної дезінформаційної кампанії Росії проти України в країнах Африки. 2025. URL: https://mfa.gov.ua/en/news/zayava-mzs-shchodo-sistemnoyi-dezinformacijnoyi-kampaniyi-rosiyi-proti-ukrayini-v-krayinah-afriki (дата звернення: 30.11.2025).

27. Ministry of Foreign Affairs of Ukraine. Nations Against Disinformation: A New Creative Tool To Counter Disinformation. 2023. URL: https://mfa.gov.ua/en/news/nations-against-disinformation-zapusk-novogo-kreativnogo-instrumentu-z-protidiyi-dezinformaciyi (дата звернення: 30.11.2025).

 ISSN: 3041-2110

28. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2229-12 (дата звернення: 02.12.2025).

29. Про контррозвідувальну діяльність : Закон України від 26.12.2002 № 374-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/374-15 (дата звернення: 02.12.2025).

30. Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність : Закон України від 03.03.2022 № 2108-IX // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2108-20 (дата звернення: 02.12.2025).

31. CERT-UA. About us. URL: https://cert.gov.ua/about-us (дата звернення: 02.12.2025).

32. CERT-UA. Рекомендації з безпеки вебресурсів. URL: https://cert.gov.ua/recommendation/19 (дата звернення: 02.02.2026).

33. Державна служба спеціального зв'язку та захисту інформації України. Методичні рекомендації щодо підготовки та реагування на кіберінциденти/кібератаки (взаємодія з CERT-UA). 03.07.2023. URL: https://zakon.rada.gov.ua/go/v0570519-23 (дата звернення: 02.12.2025).

34. Про Національну раду України з питань телебачення і радіомовлення : Закон України від 23.09.1997 № 538/97-ВР (чинна редакція) // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/538/97-%D0%B2%D1%80 (дата звернення: 02.12.2025).

35. Національна рада України з питань телебачення і радіомовлення. Національна рада вперше призначила штраф за спеціальною процедурою на час дії воєнного чи надзвичайного стану. 30.05.2025. URL: https://webportal.nrada.gov.ua/natsionalna-rada-vpershe-pryznachyla-shtraf-za-

 ISSN: 3041-2110

spetsialnoyu-protseduroyu-na-chas-diyi-voyennogo-chy-nadzvychajnogo-stanu/ (дата звернення: 02.12.2025).

36. National Council of Ukraine on Television and Radio Broadcasting. Analytical reports. URL: https://webportal.nrada.gov.ua/en/category/analytical-reports/ (дата звернення: 02.12.2025).

37. ГО «Детектор медіа». Про нас. URL: https://go.detector.media/about/ (дата звернення: 03.12.2025).

38. ГО «Детектор медіа». Моніторинг інтернету (огляд/хроніка фейків; матеріал про системний моніторинг з 24.02.2022). 18.02.2026. URL: https://detector.media/monitorynh-internetu/article/247768/ (дата звернення: 03.12.2025).

39. ГО «Детектор медіа». Індекс інформаційного впливу Кремля 2017 : звіт. 2017. URL: https://ms.detector.media/content/files/dm_iik_ukr.compressed.pdf (дата звернення: 06.12.2025).

40. Інститут масової інформації. Барометр свободи слова (моніторинги). URL: https://imi.org.ua/monitorings/barometr-svobody-slova (дата звернення: 06.12.2025).

41. Institute of Mass Information (IMI). About. 2024. URL: https://imi.org.ua/about (дата звернення: 06.12.2025).

42. StopFake. Про нас. 2024. URL: https://www.stopfake.org/uk/pro-nas/ (дата звернення: 06.12.2025).

43. Український кризовий медіа-центр. Про нас. URL: https://uacrisis.org/uk/pro-nas (дата звернення: 06.12.2025).

44. Центр оборонних стратегій. Про центр. URL: https://defence.org.ua/pro-czentr/ (дата звернення: 06.12.2025).

 ISSN: 3041-2110

45. Академія української преси. Проєкт «Програма медіаграмотності для громадян». URL: https://www.aup.com.ua/mediaosv/programa-mediagramotnosti/ (дата звернення: 07.12.2025).

46. ГО «Інтерньюз-Україна». Соціальна кампанія «ДезАут». 07.03.2025. URL: https://internews.ua/opportunity/disout-campaign (дата звернення: 07.12.2025).

47. Аулін О., Ауліна О. Стратегічні комунікації у протидії деструктивним російським наративам. Наукові праці Національної бібліотеки України імені В. І. Вернадського. 2023. Вип. 67. С. 82–95. DOI https://doi.org/10.15407/np.67.082. URL: https://nbuviap.gov.ua/images/e_biblioteka/naukovi_resursi/Socialni%20komunikacii/Aulin%20O.%20Aulina%20O.%20Strategicni%20komunikacii%20.pdf (дата звернення: 28.12.2025).

48. Горбик Р., Дуцик Д., Шалайський С. Ефективність протидії російській дезінформації в умовах повномасштабної війни: аналітичний звіт. 2023. URL: https://www.jta.com.ua/wp-content/uploads/2023/08/UMCI_-Effectiveness-of-Russian-Disinformation-Counteration_UA.pdf (дата звернення: 28.12.2025).

49. Національний інститут стратегічних досліджень. Російські дезінформаційні кампанії в Європі. 2024. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/rosiyski-dezinformatsiyni-kampaniyi-v-yevropi (дата звернення: 28.12.2025).

50. Хилько М. І. Вплив російської агресії на трансформацію комунікаційних стратегій у секторі безпеки та оборони. Політичне життя. 2025. № 3. С. 92–97. DOI https://doi.org/10.31558/2519-2949.2025.3.11. URL: https://jpl.donnu.edu.ua/article/view/17918/17810 (дата звернення: 28.12.2025).