МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Кваліфікаційна наукова
праця на правах рукопису

СТЬОПКІН АНДРІЙ ОЛЕГОВИЧ

УДК 327.32(4)+ 316.77(4-6ЄС)

ДИСЕРТАЦІЯ

МЕХАНІЗМИ ТА ІНСТРУМЕНТИ РЕАЛІЗАЦІЇ ЄВРОПЕЙСЬКОЇ ПОЛІТИКИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

052 – Політологія
Галузь знань 05 – Соціальні та поведінкові науки

Подається на здобуття наукового ступеня доктора філософії.
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ А. О. Стьопкін

Науковий керівник: доктор політичних наук, професор Ротар Наталія Юріївна

Чернівці – 2026

АНОТАЦІЯ

Стьопкін А. О. Механізми та інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії зі спеціальності 052 – Політологія. Чернівецький національний університет імені Юрія Федьковича, Чернівці, 2026.

У дисертації здійснено комплексне політологічне дослідження механізмів та інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни. Його актуальність визначається тим, що сучасний міжнародний порядок перебуває у стані геополітичної турбулентності, коли інформаційні загрози стають одним із ключових чинників впливу на політичні системи, суспільну стабільність та безпекові стратегії ЄС. Гібридна війна, почата Росією проти України в 2014 р., довела, що дезінформація, яка традиційно сприймалася як інструмент маніпуляції громадською думкою, постала як засіб підриву довіри до легітимних політичних інститутів та демократичних процесів. Дослідження європейських практик протидії дезінформації набуває особливої ваги для визначення взаємозв'язку між Україною, як державою-кандидатом, та ЄС, що мають різний статус в гібридній російсько-українській війні, але однаковою мірою вразливі до дезінформаційних наративів, поширюваних Росією.

Об'єктом дослідження є європейський політичний дискурс вироблення та реалізації політики протидії дезінформації в умовах загроз гібридної війни, предметом – механізми та інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни.

Метою дослідження є визначення сукупності та дослідження функціональності механізмів й інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни, яка досягнута через вирішення низки дослідницьких завдань: охарактеризувати теоретико-методологічні засади дослідження протидії дезінформації в умовах гібридної війни; визначити основні принципи політики протидії дезінформації в ЄС та державах-членах як основи

формування європейського механізму реагування на інформаційні загрози в умовах гібридної війни; дослідити безпекові інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни; вивчити інформаційно-комунікаційні інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни; розкрити роль національних моделей протидії дезінформації у формуванні віяла інструментів європейської політики протидії дезінформації; визначити роль та місце досвіду України у формування стійкості європейської політики протидії дезінформації.

Структурно робота відповідає предмету дослідження, його меті та завданням, тому складається зі вступу, чотирьох розділів, які поділені на 12 підрозділів, висновків, списку використаних джерел та додатків. У першому розділі визначені теоретико-методологічні засади дослідження політики протидії дезінформації в умовах гібридної війни, зокрема теоретичні основи вивчення дезінформації в умовах гібридної війни та методологічні принципи і концептуальні рамки дослідження протидії дезінформації в сучасній політичній науці, здійснено аналіз джерельної бази дослідження. Доведено, що методологічний потенціал неоінституціоналізму в дослідженні інструментів та механізмів протидії дезінформації полягає в тому, що політичні інститути регулюючи формальні процеси, формують культурні норми, когнітивні рамки та очікування, які впливають на сприйняття інформаційних загроз та визначають його стійкість в умовах гібридної війни. Застосування методології неофункціоналізму дозволяє досліджувати, як політика протидії дезінформації може зміцнювати інституційну довіру, сприяти соціальній згуртованості та формувати нові стандарти взаємодії між державою, громадянським суспільством і медіа. Встановлено, що використання концепту стійкості у теоретичному вимірі дозволяє аналізувати політику протидії дезінформації в ЄС як процесу балансування між свободою слова та безпекою демократичних інститутів. В сучасній політичній науці він є універсальною дослідницькою рамкою, що поєднує адаптивність соціальних систем із їхньою здатністю зберігати функціональність в умовах постійних інформаційних загроз. Теоретичне

застосування концепту стійкості у дослідженні дезінформації дозволило пояснити, чому загрози, згенеровані дезінформацією є не зовнішнім явищем до політичного поля ЄС, а постають системним викликом для європейської демократії, що потребує комплексної відповіді.

У другому розділі дослідницька увага сфокусована на структурі механізму європейської політики протидії дезінформації, яка вивчалася через деталізацію основних принципів політики протидії дезінформації в ЄС, визначення особливостей національних моделей політики протидії дезінформації в державах-членах ЄС та означення перспективи наближення політики протидії дезінформації України до принципів та стандартів ЄС. Механізм політики протидії дезінформації в ЄС охарактеризований як багаторівнева та інтегрована система, що поєднує нормативні, інституційні, комунікаційні та освітні інструменти. Його сутність полягає у створенні комплексної моделі співрегулювання, в якій державні інституції, цифрові платформи, медіа-індустрія та громадянське суспільство взаємодіють у межах узгоджених принципів і процедур. Інституційний вимір механізму охоплює діяльність Єврокомісії, Європейської служби зовнішніх дій, стратегічних комунікаційних підрозділів та спеціалізованих структур, які здійснюють моніторинг інформаційного простору, координують дії держав-членів та забезпечують взаємодію з міжнародними партнерами. Комунікаційний компонент механізму полягає у розвитку співпраці між платформами та незалежними фактчекінговими організаціями, створенні системи швидкого оповіщення для обміну інформацією між державами-членами. Механізм політики протидії дезінформації в ЄС можна охарактеризувати як модель, що поєднує правові норми, інституційні структури, інструменти співрегулювання та освітні заходи. Разом з тим національні механізми протидії дезінформації, до певної мір, будучи частиною європейського механізму, функціонують автономно.

У третьому розділі розглянуто безпекові інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни. Основна привернута до визначення характеристик стратегічних комунікацій як

інструменту реалізації політики протидії дезінформації, процесу формування системи цифрових безпекових інструментів протидії дезінформації в ЄС та створення онлайн екосистеми ЄС як перспективного інструменту політики протидії дезінформації. Дослідження особливостей формування системи цифрових безпекових механізмів протидії дезінформації в ЄС дало підстави зробити висновок, що період 2014–2025 рр. став етапом примусового дорослішання європейської системи цифрової безпеки. Якщо на початку російської агресії у 2014 р. реакція ЄС мала переважно символічний та реактивний характер, то на сьогодні спостерігається поєднання політичної волі у протидії дезінформації з жорсткою нормативною базою, синергією державних інституцій та громадянського суспільства, міжнародною кооперацією між державами-членами ЄС та використанням нейромережевих технологій. Головним результатом цієї еволюції стала відмова від трактування дезінформації як «фейкових новин» і перехід до концепції FIMI, що дозволило змістити акцент із боротьби з окремими інформаційними вкидами на виявлення ворожих суб'єктів та їхніх методів. Створення спеціалізованих оперативних груп та Системи швидкого сповіщення надало ЄС необхідну гнучкість, дозволивши враховувати культурні особливості різних регіонів світу при збереженні єдиного інформаційного периметра.

У четвертому розділі проаналізовані інформаційно-комунікаційні інструменти реалізації політики протидії дезінформації в умовах гібридної війни, зокрема формування системи засобів верифікації інформації, компетентністні інструменти формування стійкості до дезінформації та визначена роль інститутів громадянського суспільства у реалізації політики протидії дезінформації. Верифікація інформації позиціонується в ЄС як важливий операційний інструмент організації протидії дезінформації, оскільки вона є засобом управління ризиками, що забезпечує стійкість демократичних інституцій у багатомовному та багатокультурному середовищі ЄС. Європейська практика довела, що верифікація інформації є частиною багаторівневої системи, в якій технологічні інновації (InVID/WeVerify, Horizon 2020), професійні стандарти

(IFCN, EUvsDisinfo) та низові ініціативи (Demagog.cz, VoxCheck, StopFake, Ґвара Медіа) взаємодіють, забезпечуючи ефективність європейського та національних механізмів протидії дезінформації. Медіаграмотність та медіаосвіта в сучасних умовах гібридної війни є ключовим елемент формування стійкості спільнот до дезінформації, вони формують когнітивний імунітет, що забезпечує довготривалу захищеність суспільства від іноземних інформаційних маніпуляцій. Європейські практики демонструють перехід від логіки дебанкінгу до стратегії пребанкінгу, яка опирається на необхідність превентивного навчання як «інформаційної вакцинації». Дослідження ролі інститутів громадянського суспільства у протидії дезінформаційним викликам у Латвії, Литві та Естонії показує, що саме ці структури стають ключовими агентами у формуванні когнітивної стійкості суспільства.

У висновках зазначено, що ефективність європейської політики протидії дезінформації в умовах гібридної війни визначається здатністю Європейського Союзу, держав-членів ЄС та України як держави-кандидата формувати багаторівневу та динамічну систему взаємодії, в якій функціонує множинність механізмів і множинність інструментів, що утворюють спільну для всіх матрицю захисту європейського демократичного простору від інформаційних загроз. ЄС задає нормативні рамки та визначає стратегічні пріоритети, держави-члени адаптують їх у власних інституційних і правових системах, а Україна інтегрує ці практики у власну модель, модифікуючи їх відповідно до умов війни та високої інтенсивності інформаційних атак. У цій системі правове регулювання, інституційна координація, освітні програми та цифрові інновації створюють багатовимірний захист. Синергія наднаціонального рівня (ЄС), національних практик (держави-члени ЄС) та кандидатської адаптації (Україна) забезпечують розгортання процесу формування стійкої моделі протидії дезінформації, здатної протистояти загрозам гібридної війни та забезпечувати довготривалу інформаційну безпеку на основі демократичних цінностей ЄС.

Ключові слова: політика, політичні інститути, дезінформація, пропаганда, гібридна війна, протидія дезінформації, безпека, правове

забезпечення, Європейський Союз, Україна, стратегічні комунікації (StratCom), комунікація, маніпулювання, медіаграмотність, громадська думка.

ABSTRACT

Stopkin A. Mechanisms and Instruments for Implementing the European Policy of Countering Disinformation in the Context of Hybrid Warfare. – Qualification scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 052 – Political Science. Yuri Fedkovych Chernivtsi National University, Chernivtsi, 2026.

In this dissertation, a comprehensive political science study is conducted on the mechanisms and instruments of implementing European policies to counter disinformation under conditions of hybrid warfare. Its relevance is determined by the fact that the contemporary international order is experiencing geopolitical turbulence, where information threats have become one of the key factors influencing political systems, social stability, and the EU's security strategies. The hybrid war launched by Russia against Ukraine in 2014 demonstrated that disinformation, traditionally perceived as a tool of manipulating public opinion, has emerged as a means of undermining trust in legitimate political institutions and democratic processes. Research into European practices of countering disinformation acquires particular importance in defining the relationship between Ukraine, as a candidate state, and the EU, which hold different statuses in the Russian-Ukrainian hybrid war but are equally vulnerable to disinformation narratives disseminated by Russia.

The object of the study is the European political discourse on the development and implementation of policies to counter disinformation under hybrid war conditions; the subject is the mechanisms and instruments of implementing European policies to counter disinformation under hybrid war conditions.

The aim of the study is to identify and examine the functionality of mechanisms and instruments for implementing European policies to counter disinformation in hybrid warfare. This aim is achieved through several research tasks: to characterize the theoretical and methodological foundations of studying disinformation counteraction

in hybrid war; to define the core principles of EU and member-state policies against disinformation as the basis for shaping a European mechanism of response to information threats; to investigate security instruments of implementing EU disinformation counteraction policies; to examine information and communication instruments of policy implementation; to reveal the role of national models of disinformation counteraction in shaping the spectrum of European instruments; and to determine the role and place of Ukraine's experience in strengthening the resilience of European disinformation counteraction policies.

Structurally, the dissertation corresponds to its subject, aim, and tasks, consisting of an introduction, four chapters divided into twelve subsections, conclusions, a bibliography, and appendices. The first chapter defines the theoretical and methodological foundations of studying disinformation counteraction in hybrid war, including theoretical bases for analyzing disinformation, methodological principles, Stopkithe source base. It is demonstrated that the methodological potential of neo-institutionalism lies in the ability of political institutions, by regulating formal processes, to shape cultural norms, cognitive frameworks, and expectations that influence perceptions of information threats and determine resilience under hybrid war conditions. The application of neo-functionalism enables exploration of how disinformation counteraction policies can strengthen institutional trust, foster social cohesion, and establish new standards of interaction between the state, civil society, and media. The concept of resilience, in theoretical terms, allows analysis of EU disinformation counteraction as a process of balancing freedom of speech with the security of democratic institutions. In modern political science, resilience serves as a universal research framework combining the adaptability of social systems with their capacity to maintain functionality under constant information threats. Its application explains why disinformation-generated threats are not external to the EU political sphere but constitute a systemic challenge to European democracy requiring a comprehensive response.

The second chapter focuses on the structure of the EU disinformation counteraction mechanism, examined through the principles of EU policy, the features

of national models in member states, and the prospects of aligning Ukraine's policies with EU standards. The EU mechanism is characterized as a multi-level, integrated system combining normative, institutional, communicative, and educational instruments. Its essence lies in creating a co-regulation model where state institutions, digital platforms, the media industry, and civil society interact within agreed principles and procedures. The institutional dimension encompasses the activities of the European Commission, the European External Action Service, strategic communication units, and specialized structures that monitor the information space, coordinate member states, and ensure cooperation with international partners. The communicative component involves collaboration between platforms and independent fact-checking organizations, as well as the establishment of rapid alert systems for information exchange among member states. National mechanisms, while partly integrated into the European framework, retain a degree of autonomy.

The third chapter examines security instruments of EU disinformation counteraction under hybrid war conditions. Particular attention is given to strategic communications, the development of digital security tools, and the creation of an EU online ecosystem as a prospective instrument. The evolution of EU digital security mechanisms between 2014 and 2025 is described as a period of forced maturation. Whereas the initial EU response to Russian aggression in 2014 was largely symbolic and reactive, today it combines political will with a robust regulatory framework, synergy between institutions and civil society, international cooperation, and the use of neural network technologies. A key outcome of this evolution was the shift from treating disinformation as "fake news" to adopting the FIMI (Foreign Information Manipulation and Interference) concept, which redirected focus from isolated information incidents to hostile actors and their methods. The establishment of specialized task forces and the Rapid Alert System provided the EU with flexibility to account for cultural differences across regions while maintaining a unified information perimeter.

The fourth chapter analyzes information and communication instruments of disinformation counteraction, including verification systems, competence-based tools

for resilience, and the role of civil society institutions. Verification is positioned as a crucial operational tool for risk management, ensuring the resilience of democratic institutions in the EU's multilingual and multicultural environment. European practice demonstrates that verification is part of a multi-level system where technological innovations (InVID/WeVerify, Horizon 2020), professional standards (IFCN, EUvsDisinfo), and grassroots initiatives (Demagog.cz, VoxCheck, StopFake, Gwara Media) interact to ensure effectiveness. Media literacy and education are identified as key elements of resilience, forming cognitive immunity against foreign information manipulation. European practices show a shift from debunking to pre-bunking strategies, emphasizing preventive learning as "information vaccination." Civil society institutions in Latvia, Lithuania, and Estonia are highlighted as crucial agents in building cognitive resilience.

The conclusions state that the effectiveness of EU disinformation counteraction policies under hybrid war conditions depends on the ability of the EU, its member states, and Ukraine as a candidate state to form a multi-level, dynamic system of interaction. This system integrates diverse mechanisms and instruments into a shared matrix for protecting the European democratic space from information threats. The EU sets normative frameworks and strategic priorities, member states adapt them within their institutional and legal systems, and Ukraine incorporates and modifies these practices according to wartime conditions and the intensity of information attacks. Legal regulation, institutional coordination, educational programs, and digital innovations together create multidimensional protection. The synergy of supranational (EU), national (member states), and candidate-level (Ukraine) practices ensures the development of a resilient model of disinformation counteraction capable of withstanding hybrid war threats and safeguarding long-term information security based on EU democratic values.

Key words: Policy, political institutions, disinformation, propaganda, hybrid warfare, countering disinformation, security, legal support, European Union, Ukraine,

strategic communications (StratCom), communication, manipulation, media literacy, public opinion.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці у виданнях, включених до переліку наукових фахових видань України:

1. Стьопкін А. Інституціоналізація політики протидії дезінформації в Європейському Союзі. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2022. Том 10. С. 196–208.
2. Стьопкін А. Особливості концептуалізації поняття дезінформація в сучасній політичній науці. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2024. Том 15. С. 320–336.
3. Стьопкін А. Особливості національних моделей політики протидії дезінформації в державах-членах ЄС. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2025. Вип. 4(24). С. 115–137.

Наукові праці, які засвідчують апробацію матеріалів дисертації

4. Стьопкін А. О. Європейські інструменти спротиву дезінформації. *Розвиток політичної науки: європейські практики та національні перспективи: матеріали Міжнародної науково-практичної конференції, Чернівці, 28 червня 2022 року*. Чернівці: Технодрук, 2022. С. 195–196.
5. Стьопкін А. О. Стратегічні комунікації НАТО як інструмент реалізації політики протидії дезінформації РФ. *Збірник матеріалів IV Всеукраїнської науково-практичної конференції «Політичні процеси сучасності: глобальний та регіональний виміри»*. ІІ частина. Івано-Франківськ: Прикарпатський національний університет імені Василя Стефаника, 2022. С. 377–386.
6. Стьопкін А. Перспективи формування онлайн-екосистеми як інструменту політики протидії дезінформації. *Розвиток політичної науки: європейські практики та національні перспективи: матеріали Міжнародної науково-практичної конференції, Чернівці, 14 червня 2023 року*. Чернівці : Технодрук, 2023. С. 114–117.

7. Стьопкін А. О. Особливості інтеграції інструментів формування медіакомпетентності до інформаційно-комунікаційного механізму протидії дезінформації в умовах російсько-української війни. *Інтернет-конференція «Україна в координатах Східного партнерства: пошук геополітичних пріоритетів крізь призму національної безпеки».* Львів: Видавництво Львівської політехніки, 2023. С. 42–44.
8. Стьопкін А. О. Наближення політики протидії дезінформації України до принципів та стандартів ЄС. *Розвиток політичної науки: європейські практики та національні перспективи: матеріали Міжнародної науково-практичної конференції, Чернівці, 29 травня 2025 року*. Чернівці: Технодрук, 2025. С. 106–109.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

Скорочення	Повна назва
ГО	Громадська організація
ЄКПЛ	Європейська конвенція з прав людини
ЄС	Європейський Союз
ЗМІ	Засоби масової інформації
МОН	Міністерство освіти і науки України
ООН	Організація Об’єднаних Націй
РНБО	Рада національної безпеки і оборони України
РФ	Російська Федерація
УКМЦ	Український кризовий медіа-центр
ЦЄІ	Центральноєвропейська ініціатива
ЦПД	Центр протидії дезінформації
ADMO	Adria Digital Media Observatory
AFP	L’Agence France-Presse (Агентство Франс Прес)
AI (ШІ)	Artificial intelligence (Штучний інтелект)
ANSSI	Agence nationale de la sécurité des systèmes d'information (Національне агентство безпеки інформаційних систем)
APD	Action Plan against Disinformation (Спільний план дій проти дезінформації)
AVMSD	Audiovisual Media Services Directive (Директива про аудіовізуальні медіапослуги)
BENEDMO	Belgian Netherlands Digital Media Observatory **(**Бельгійсько-Нідерландська обсерваторія цифрових медіа)
BIS	Bezpečnostní informační služba (Служба інформаційної безпеки)
BPB	Bundeszentrale für politische Bildung (Федеральне агентство громадянської освіти)
CCDCOE	Cooperative Cyber Defense Center of Excellence (Об’єднаний центр передових технологій з кібероборони НАТО)
CRRT	Cyber Rapid Response Teams (Швидкі команди кібернетичного реагування)
CSA	Conseil supérieur de l’audiovisuel (Вища аудіовізуальна рада)
CSCIS	Centre for Strategic Communication and Information Security (Центр стратегічних комунікацій та інформаційної безпеки)
DFRLab	Digital Forensic Research Lab (Лабораторія цифрової криміналістичної експертизи)
DSA	Digital Services Act (Закон про цифрові послуги)

EDMO	European Digital Media Observatory (Європейська обсерваторія цифрових медіа)
EEAS	European External Action Service (Європейська служба зовнішніх справ)
EMFA	European Media Freedom Act (Європейський акт про свободу медіа)
ENISA	European Union Agency for Network and Information Security (Агентство Європейського Союзу з питань мережевої та інформаційної безпеки)
ERGA	European Regulators Group for Audiovisual Media Services (Група європейських регуляторів аудіовізуальних медіапослуг)
ESTF	East StratCom Task Force (Східна робоча група зі стратегічних комунікацій)
EUAM	European Union Advisory Mission Ukraine (Консультативна місія Європейського Союзу в Україні)
EUMAM	European Union Military Assistance Mission for Ukraine (Місія ЄС з військової допомоги на підтримку України)
FIMI	Foreign Information Manipulation and Interference (іноземні маніпуляції інформацією та втручання)
GDPR	General Data Protection Regulation (Загальний регламент про захист даних)
GLOBSEC	Global Security Policy Institute
HADOPI	Haute Autorité pour la Diffusion des Œuvres et la Protection des droits d'auteur sur Internet (Верховний орган з питань розповсюдження творів та захисту авторських прав в Інтернеті)
HFC	Hybrid Fusion Cell (Гібридний координаційний осередок)
ICDS	International Centre for Defence and Security (Міжнародний центр оборони та безпеки: Головна сторінка)
IFCN	International Fact-Checking Network (Міжнародна мережа перевірки фактів)
IFJ	International Federation of Journalists (Міжнародна федерація журналістів)
IoC	Indicator of Compromise (індикатор компрометації/ ознака порушення безпеки)
IREX	International Research & Exchanges Board (Рада міжнародних наукових досліджень та обмінів)
ISAC	Information Sharing and Analysis Centers (Центри обміну та аналізу інформації)
JRC	Joint Research Centre (Об’єднаний дослідницький центр)

KAVI	Kansallinen audiovisuaalinen instituutti (Національний аудіовізуальний інститут)
KSI	Keyless Signature Infrastructure (Інфраструктура підписів без ключів)
MENA	Middle East & North Africa (Близький Схід та Північна Африка)
NAFO	North Atlantic Fella Organization (Північноатлантична організація чуваків)
NATO	North Atlantic Treaty Organization (Організація Північноатлантичного договору, НАТО)
NCSI	National Cyber Security Index (Національний індекс кібербезпеки)
NetzDG	Netzwerkdurchsetzungsgesetz (Закон про захист прав у мережі)
OSINT	Open Source Intelligence (розвідка на основі відкритих джерел)
PESCO	Permanent Structured Cooperation (Постійна структурована співпраця)
RAS	Rapid Alert System (Система швидкого реагування/сповіщення)
RT	Russia today (Росія сьогодні)
SCPD	Strengthened Code of Practice on Disinformation (Посилений кодекс практики щодо дезінформації)
SSTF	South StratCom Task Force (Південна група зі стратегічних комунікацій Західні Балкани)
StratCom	Strategic Communication Task Forces (оперативні/робочі групи зі стратегічних комунікацій)
USAID	United States Agency for International Development (Агентство США з міжнародного розвитку)
VERA.ai	Verification Assisted by Artificial Intelligence
VIGINUM	Vigilance et protection contre les ingérences numériques étrangères (Пильність та захист від іноземного цифрового втручання)
VLOPs	Very Large Online Platforms (Дуже великі онлайн-платформи)
WBTF	Western Balkans Task Force (Робоча група зі стратегічних комунікацій Західні Балкани)
ZEAM	Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation (Центральне управління з виявлення маніпуляцій іноземною інформацією)

ВСТУП

Актуальність теми. Актуальність політологічного дослідження механізмів та інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни визначається тим, що сучасний міжнародний порядок перебуває у стані геополітичної турбулентності, коли інформаційні загрози стають одним із ключових чинників впливу на політичні системи, суспільну стабільність та безпекові стратегії ЄС. Гібридна війна, почата в Росією проти України в 2014 р., довела, що дезінформація, яка традиційно сприймалася як інструмент маніпуляції громадською думкою, постала як засіб підриву довіри до легітимних політичних інститутів та демократичних процесів.

Сучасний інформаційний простір перетворився на поле стратегічного протистояння, в якому дезінформація використовується як інструмент впливу на суспільну свідомість, політичні процеси та міжнародну безпеку. Європейський Союз, зіткнувшись із системними кампаніями зовнішнього втручання, опинився перед потребою формування багаторівневої політики, яка поєднує правові, інституційні та освітні механізми, спрямовані на захист демократичних інститутів та інформаційного простору на рівні ЄС та у державах-членах ЄС.

Дослідження європейських практик протидії дезінформації набуває особливої ваги для визначення взаємозв'язку між Україною, як державою-кандидатом, та ЄС, що мають різний статус в гібридній російсько-українській війні, але однаковою мірою вразливі до дезінформаційних наративів, поширюваних Росією та Китаєм. Відтак, і перед ЄС, і перед Україною стоїть завдання формування інституційної та індивідуальної стійкості до дезінформаційних атак, що актуалізує необхідність політологічного дослідження взаємодії між політичними інститутами та інституціями ЄС, державними структурами України та інститутами громадянського суспільства в розгортанні формальних та неформальних інструментів протидії дезінформації.

Мета і завдання дослідження. Метою дослідження є визначення сукупності та дослідження функціональності механізмів й інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни. Мета дослідження спрямувала до визначення таких **дослідницьких завдань:**

- охарактеризувати теоретико-методологічні засади дослідження протидії дезінформації в умовах гібридної війни;
- визначити основні принципи політики протидії дезінформації в ЄС та державах-членах як основи формування європейського механізму реагування на інформаційні загрози в умовах гібридної війни;
- дослідити безпекові інструменти реалізації європейської політики протидії дезінформації;
- вивчити інформаційно-комунікаційні інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни;
- розкрити роль національних моделей протидії дезінформації у формуванні віяла інструментів європейської політики протидії дезінформації;
- визначити роль та місце досвіду України у формування стійкості європейської політики протидії дезінформації.

Об'єктом дослідження є європейський політичний дискурс вироблення та реалізації політики протидії дезінформації в умовах загроз гібридної війни.

Предметом дослідження є механізми та інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни.

Гіпотеза дослідження. Гіпотезою дослідження є припущення, що ефективність європейської політики протидії дезінформації в умовах гібридної війни визначається здатністю трьох суб'єктів (Європейського Союзу, держав-членів та України як держави-кандидата) формувати багаторівневу та динамічну систему взаємодії, де множинність механізмів і множинність інструментів поєднуються у спільній матриці захисту демократичного простору від інформаційних загроз. ЄС задає нормативні рамки та визначає стратегічні пріоритети, держави-члени адаптують їх у власних інституційних і правових

системах, а Україна інтегрує ці практики у власну модель, модифікуючи їх відповідно до умов війни та високої інтенсивності інформаційних атак. У цій системі правове регулювання, інституційна координація, освітні програми та цифрові інновації створюють багатовимірний захист. Саме синергія наднаціонального рівня, національних практик та кандидатської адаптації формує стійку модель протидії дезінформації, здатну протистояти багатовимірним загрозам гібридної війни та забезпечувати довготривалу інформаційну безпеку на основі демократичних цінностей ЄС.

Методи дослідження. Політологічне дослідження механізмів та інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни потребувало комплексного використання методологічних підходів та методів, які є загальнонауковими та відповідають специфіці предмета дослідження. Зокрема, в дослідженні були використані загальнонаукові принципи пізнання: використання історико-генетичного принципу дозволило простежити витоки та еволюцію політики ЄС у сфері протидії дезінформації, з'ясувати причини трансформації її змісту з моменту активізації гібридних загроз та визначити передумови формування якісно нових інструментів впливу на інформаційний простір; субстратно-подієвий метод уможливив системну впорядкованість фактів (субстрату), в яких відображена політика ЄС та держав-членів у період після 2014 р., коли дезінформація стала одним із ключових інструментів гібридної війни, зокрема проти України. Діалектичний метод дозволив розглядати політику протидії дезінформації як динамічний процес, у якому внутрішні суперечності між свободою слова та потребою захисту інформаційного простору спричиняють трансформацію протидії дезінформації. Це дало можливість осягнути зміст, сутність та роль механізмів протидії дезінформації в управлінні інформаційними ризиками, розглядаючи їх у нерозривному зв'язку з еволюцією політичного дискурсу дезінформації в ЄС, держава-членах та державах-кандидатах. Метод аналізу та синтезу забезпечив: узагальнення на основі значного фактологічного матеріалу, що дозволило виділити основні інструменти реалізації політики протидії дезінформації

(безпекові та інформаційно-комунікаційні); формування методологічного каркасу дослідження; вивчення нормативно-правового поля протидії дезінформації в ЄС, державах-членах ЄС та державах-кандидатах.

У дослідженні були використані методологічні принципи неоінституціоналізму. Їх застосування дозволило: по-перше, розглядати політику протидії дезінформації як цілісну систему, що складається з низки взаємопов'язаних елементів, серед яких ключове місце займають інституційні механізми та інструменти регулювання інформаційного простору; по-друге, пояснити, як створення спеціалізованих структур, запровадження нормативно-правових інструментів та розвиток технологічних засобів протидії дезінформації набувають статусу механізмів та інструментів протидії дезінформації, що забезпечують стійкість ЄС до зовнішніх і внутрішніх інформаційних атак.

Застосування методології неофункціоналізму дозволило дослідити та пояснити, яким чином реалізація політики протидії дезінформації в ЄС зміцнює довіру до інститутів ЄС, сприяє соціальній згуртованості та формує нові стандарти взаємодії між державою, громадянським суспільством і медіа. Принципи методології неофункціоналізму дозволили пояснити, чому протидія дезінформації потребує комплексної інтеграції з іншими політиками, зокрема безпековою та інформаційно-комунікаційною.

Одним із основних методів дослідження є порівняльний метод, який дозволив: простежити крос-темпоральну динаміку різних моделей реагування на дезінформацію та визначити їхню ефективність у конкретних політичних і безпекових контекстах; визначити спільне та відмінне між WSTF, SSTF та ESTF в протидії дезінформації засобами стратегічних комунікацій ЄС. Використання цього методу дало можливість дослідити форми та принципи реалізації політики протидії дезінформації в державах-членах ЄС, зіставити їх із загальноєвропейськими підходами та виявити чинники, що впливають на формування інституційних механізмів захисту інформаційного простору. Порівняльний аналіз дозволив оцінити, як різні держави-члени ЄС після 2014 р. адаптували свої інструменти протидії дезінформації до умов гібридної війни, які

саме фактори визначають якість та результативність цих інструментів, а також які перспективи відкриває використання новітніх технологій у сфері цифровізації політичних відносин.

Використання методу прогнозування дозволило визначити: які саме моделі взаємодії між інституціями ЄС та громадянами мають найбільший ресурсний потенціал для забезпечення стійкості демократичних систем держав-членів ЄС та ЄС загалом; як цифрові платформи можуть бути перетворені на механізмами контролю або верифікації інформації та взаємодії з інститутами, що дозволяє громадянам брати активну участь у реалізації політики протидії дезінформації та означити перспективи наближення політики протидії дезінформації України до принципів та стандартів ЄС

Метод кейс-стаді був використаний для визначення ролі та місця досвіду України у формування стійкості європейської політики протидії дезінформації та під час дослідження найбільш виразних практик протидії дезінформації в державах-членах ЄС (держави Балтії, Франція, Чехія та інші).

Узгоджене застосування визначених методологічних підходів та методів політологічного дослідження сприяло тому, що здійснене дослідження набуло всебічного характеру, охопивши як теоретичні моделі, так і практичні механізми й інструменти, які забезпечують ефективність європейської політики протидії дезінформації в умовах гібридної війни. Відповідність методологічної основи предмету дослідження забезпечила належний рівень наукової обґрунтованості отриманих результатів, їхню комплексність та практичну значущість для політичної науки.

Зв’язок роботи з науковими програмами, планами, темами. Тема дисертаційного дослідження відповідає науковим темам кафедри політології та державного управління Чернівецького національного університету імені Юрія Федьковича: «Політичні процеси та публічне управління в умовах сучасних викликів і загроз» (№ державної реєстрації 0119U103774), яка виконувалася впродовж 2019–2024 рр. та «Забезпечення стійкості політичної системи управлінської діяльності в умовах російсько-української війни та глобальної

нестабільності» (№ державної реєстрації 0124U004630), яка затверджена в 2024 р. та виконується колективом кафедри політології та державного управління до сьогодні.

Наукова новизна отриманих результатів визначається розробкою моделі, що пояснює функціонування сукупності механізмів та інструментів європейської політики протидії дезінформації в неоінституційній та неофункціональній методологічних парадигмах.

Уперше:

- доведено, що ефективність європейської політики протидії дезінформації в умовах гібридної війни визначається здатністю трьох суб'єктів (Європейського Союзу, держав-членів та України як держави-кандидата) формувати багаторівневу та динамічну систему взаємодії, де множинність механізмів і множинність інструментів поєднуються у спільній матриці захисту демократичного простору від інформаційних загроз. ЄС задає нормативні рамки та визначає стратегічні пріоритети, держави-члени адаптують їх у власних інституційних і правових системах, а Україна інтегрує ці практики у власну модель, модифікуючи їх відповідно до умов війни та високої інтенсивності інформаційних атак. Синергія наднаціонального рівня, національних практик та кандидатської адаптації формує стійку модель протидії дезінформації, здатну протистояти багатовимірним загрозам гібридної війни та забезпечувати довготривалу інформаційну безпеку на основі демократичних цінностей ЄС.
- на основі методології неоінституціоналізму доведено, що інституційні рамки ЄС моделюють дії держав-членів у виробленні політики протидії дезінформації, створюючи умови для узгодженості дій у сфері інформаційної безпеки, при цьому виявляється двосторонній ефект –інституційної конвергенції, коли національні політики адаптуються до європейських стандартів та дивергенції – коли, держави-члени ЄС адаптують норми та принципи протидії дезінформації до власних політичних та соціокультурних умов.

- сформульовано поняття множинності механізмів протидії дезінформації, що є взаємодоповнюваними в умовах демократичних інтеграційних об'єднань, таких як ЄС, тому діють в одному смисловому полі демократії через взаємопов'язані безпекові, інституційні, нормативні, комунікаційні та освітні інструменти, що утворюють динамічну матрицю протидії дезінформації на основі цінностей ЄС.
- обґрунтовано, що держава-кандидат (Україна), що має статус суб'єкта першої лінії в гібридній війні, може впливати на зміст політики ЄС щодо протидії дезінформації та артикулювати потребу в систематизації регуляторних механізмів управління інформацією на демократичних принципах.

Удосконалено:

- концепт європейської політики протидії дезінформації як динамічної матриці, в якій множинність механізмів (нормативних, інституційних, комунікаційних, освітніх) та множинність інструментів (регламенти, кодекси практики, плани дій, системи моніторингу, механізми співрегулювання) взаємодіють у межах єдиної логіки демократичних цінностей, що дозволяє розглядати європейський підхід до протиді дезінформації як цілісний;
- розуміння логіки процесу адаптації механізмів протидії дезінформації, що використовуються Україною як державою-кандидатом, до європейських стандартів у протидії дезінформації, що постає як формування нової інституційної якості, яка поєднує національні практики, сформовані в умовах російсько-української війни та європейські інструменти, створюючи європейську модель національної стійкості, яка має значення як для внутрішньої стабільності, так і для процесу європейської інтеграції;
- визначення сукупності інструментів протидії дезінформації як таких, що через співрегулювання, в якому поєднані наднаціональні норми ЄС, національні політики держав-членів та адаптаційні практики держав-кандидатів, зокрема України, створюють умови для багаторівневої інтеграції у сфері інформаційної безпеки.

Набули подальшого розвитку:

- ідеї методології неофункціоналізму, які застосовуються для пояснення того, як політика протидії дезінформації стає сферою поступового розширення інтеграції, коли початкові заходи у сфері прозорості реклами та співпраці з платформами трансформуються на більш комплексні регуляторні механізми, що охоплюють управління системними ризиками та забезпечення демократичної стійкості в умовах гібридної війни;
- концептуальні рамки поняття стійкості як аналітичної категорії, що дозволяє оцінювати ефективність політики протидії дезінформації через формальні результати та здатність інституцій ЄС, держав-членів та України адаптуватися до нових інформаційних загроз, зберігаючи демократичні цінності та забезпечуючи довгострокову стабільність політичних систем;
- характеристики функціональної взаємодії між різними інструментами політики протидії дезінформації, такими як Кодекс практики щодо дезінформації, Digital Services Act та План дій щодо європейської демократії, що сукупно формують принципи управління ризиками, пов'язаними з поширенням неправдивої інформації.

Практичне значення отриманих результатів полягає в тому, що вони можуть бути використані в процесі узгодження нормативно-правового механізму протидії дезінформації між ЄС та Україною, щодо забезпечення прозорості цифрових платформ та підвищення відповідальності медіа за поширення дезінформаційних наративів. Отримані результати можуть бути застосовані у процесі розробки освітніх програм з медіаграмотності, у створенні технологічних рішень для моніторингу та верифікації інформації, а також у формуванні інституційних практик, які забезпечують стійкість політичної системи України до інформаційних атак. Висновки та результати дослідження можуть бути використані органами державної влади для вироблення довгострокових стратегій, що поєднують правові, комунікаційні та технологічні інструменти у єдину систему протидії дезінформації та можуть бути застосовані як інструмент забезпечення стійкості на національному, регіональному та локальному рівнях.

Особистий внесок здобувача. Усі наукові положення дисертації, отримані результати дослідження та сформульовані висновки і рекомендації розроблені автором самостійно.

Апробація результатів дослідження. Основні положення та висновки дослідження були апробовані в доповідях на всеукраїнських та міжнародних науково-практичних конференціях: Розвиток політичної науки: європейські практики та національні перспективи (Чернівці, 28 червня 2022 р.); IV Всеукраїнська науково-практична конференція «Політичні процеси сучасності: глобальний та регіональний виміри» Івано-Франківськ, 27-28 жовтня 2022 р.); Розвиток політичної науки: європейські практики та національні перспективи: (Чернівці, 14 червня 2023 р.); Україна в координатах Східного партнерства: пошук геополітичних пріоритетів крізь призму національної безпеки (Львів, 24 березня 2023 р.); Розвиток політичної науки**:** європейські практики та національні перспективи (Чернівці, 29 травня 2025 р.), що були опубліковані; на міжнародних наукових та науково-практичних конференціях: «Сучасні тенденції регіональної співпраці: україно-румуно-молдовський вимір» (Чернівці 24 травня 2024 р.) та «Протидія російським інформаційно-психологічним впливам в умовах повномасштабної російсько-української війни: механізми та можливі рішення» (Чернівці, 11 квітня 2025 р.) без публікації. Результати дослідження були апробовані під час долучення до виконання проєктів «EU Strategic Communications: Counteraction to Destructive Influences» (Волинський національний університет імені Лесі Українки, 2024 р., сертифікат), «Протидія ЄС зовнішньому інформаційному маніпулюванню та втручанню» (Волинський національний університет імені Лесі Українки, 2025 р., сертифікат) «Політика пам’яті та гібридні загрози: інструменти РФ і вплив на європейський популізм» (Карпатський національний університет імені Василя Стефаника, з 1 січня 2026 р.).

Публікації. Результати наукового дослідження опубліковані в трьох наукових статтях, що є українськими фаховими виданнями категорії «Б» за

спеціальністю 052 – Політологія та п’яти збірниках матеріалів міжнародних наукових та науково-практичних конференцій.

Структура роботи відповідає предмету дослідження, його меті та завданням, тому складається зі вступу, чотирьох розділів, які поділені на 12 підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 284 сторінки, з яких 207 є основним текстом дисертації. Список використаних джерел налічує 405 позиції.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПОЛІТИКИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

1.2. Теоретичні основи вивчення дезінформації в умовах гібридної війни

Починаючи від давніх цивілізацій, дезінформація неперервно впливала на організацію суспільних відносин та функціонування політичної системи. Сьогодні дезінформація позиціонується сталими демократіями як виклик для системи демократичних цінностей та стабільного функціонування системи політичних інститутів на принципах демократичних конституційних норм. Привертає увагу й дедалі більш виразна залежність громадян від споживання вторинної інформації, що розширює можливості вироблення та реалізації політики дезінформації у внутрішньополітичних процесах та на міжнародній арені. Особливо виразною, в означеному контексті, є російська дезінформаційна політика в умовах російсько-української війни, спрямована на підрив структурної та функціональної цілісності Української держави. Російська дезінформація має на меті сприяти становленню, консолідації та поширенню нераціональних ментальних моделей реальності у форматі концепту *рускогo міра.* Попри ірраціональний зміст, сучасні дезінформаційні кампанії є раціональними інструментами руйнування демократичних основ організації політичної влади. Тому, розуміння сутності дезінформації, її базових характеристик та механізму функціонування є основою для формування стійкості та певної імунізації проти потенційної активації тригерів споживання дезінформації в сучасних умовах геополітичної невизначеності. Формування такого розуміння відбувається, зокрема, і в процесі концептуалізації поняття *дезінформація* в сучасній політичній науці.

В наукових дослідженнях дезінформації особлива роль належить війнам: Перша та Друга світові війни вирішально вплинули на становлення дискурсу потенціалу дезінформації, а російсько-українська війна інтегрувала до нього

проблеми вироблення та реалізації політики протидії дезінформації. Водночас, дослідники в сфері концептуалізації поняття *дезінформація* в сучасній політичній науці перебувають в динамічному пошуку стрункіх та гнучких концептів, що пояснюється важливістю контексту вироблення, поширення та споживання дезінформації в перманентних умовах невизначеності та ризиків.

Смисловим контекстом визначення змісту поняття «дезінформація» для нас буде поняття гібридної війни, сформоване в рамках відповідного концепту американським військовим стратегом, дослідником у сфері національної безпеки та оборонної політики Ф. Гофманом у 2007 р.: «Гібридна війна – це нова форма одночасного використання кількох типів ведення війни гнучкими та добре підготовленими противниками, які розуміють, що успішний конфлікт вимагає різноманітних форм, підібраних відповідно до поставлених цілей у конкретний момент» [252]. Саме це визначення використовують сучасні науковці для відображення взаємозв'язку між дезінформацією та гібридною війною [158].

Методологічні проблеми політологічного вивчення дезінформації та політики протидії дезінформації пов'язані з тим, що сучасна наука оперує низкою концептів (наприклад, «концептуальних попередників» [82, p. 3]), на рівні яких було здійснене теоретичне осмислення політичних чинників та наслідків викривлення інформації у формі пропаганди, чуток, теорії змов, фейкових новин. На сьогодні, всі означені форми викривлення інформації чітко розмежовуються за такими критеріями як контекст появи недостовірної інформації, її зміст та функції в політичному процесі [242]. Водночас, в сучасній політичній науці сформувалося чітке розуміння можливості опертя на теорії пропаганди, чуток, фейкових новин та теорії змов в концептуалізації змісту дезінформації та структури політики протидії їй [82, p. 4], уникаючи наділення категорії дезінформація ознаками парасолькового терміну щодо всіх інших, пов'язаних з неправдивою інформацією (Додаток А).

Попри численні спроби концептуалізації політичних вимірів дезінформації, до сьогодні в політичній науці не сформувалося однозначного розуміння даного явища. Більшість науковців привертають увагу до такого

смислового ядра цієї категорії як неправдивість та неточність: А. Ґесс та Б. Лайонс визначають дезінформацію як «твердження, що суперечить чи спотворює розуміння фактів, які можна перевірити» [242, p. 17]; К. Борн та Н. Едінгтон виходять з того, що це «ненавмисно оприлюднена неточна інформація» [112]; Л. Флоріді маркує дезінформацію як псевдоінформацію, виводячи її за межі «різновидів інформації» [228, p. 104]; К. Фокс виходить з того, що інформація не обов'язково має бути правдивою, наголошує, що «дезінформація вимагає брехні, тому має бути неправдивою» [231, p. 193]; С. Джек підкреслює, що дезінформування опирається на навмисно створену неправдиву інформацію [263], що на нашу думку, вказує на політику дезінформування; В. Саутвелл, Е. Торсон та Л. Шелбі конкретизують основні характеристики дезінформації через відсутність консенсусу щодо її істинності «в конкретний час на підставі конкретних доказів» [370, p. 369]. Наведені визначення вказують, що поняття *дезінформація* корелюється з поняттям *інформація*, тому необхідно визначити характер зв'язку між ними.

Дискусії щодо співвідношення інформації та дезінформації розгортаються довкола проблеми доречності класифікувати дезінформацію як інформацію, адже інформативність дезінформації визначається як обмежена невизначеність, що не має інформаційної цінності. Тобто, якщо інформація є суспільно значимим фактом, правдивою та здатною забезпечити ціннісну складову процесу прийняття рішень [228, p. 54–57], то з таких позицій дезінформація не може позначатися як той чи інший вид (форма) інформації. На противагу означеному розумінню співвідношення інформації та дезінформації постає підхід, який маркує інформацію як етично нейтральну: «інформація не потребує правди, тому вона не обов'язково має бути правдивою. Але, й дезінформація, що є брехнею, не обов'язково має бути хибною» [231, p. 193]. На думку С. Леша, дезінформація може бути інформативною «інформацією, що вийшла з-під контролю», а інформація – ірраціональною (неінформативною) [282, p. 2]. Тобто,

дезінформація може мати інформативний характер, але він завжди буде пов’язаний з метою досягнення певних політичних цілей.

Позиціонування інформативності як характеристики дезінформації дозволило перенести фокус дослідницької уваги на її комунікативний вимір: «дезінформація виникає як функція системи [політичної – *Авт.*], що відображає потребу людини в інформації та здатність людини помилятися» [383, p. 292] в умовах невизначеності, кризи, ризиків та загроз. Визнання інформативності дезінформації спрямувало дослідників до визначення матриці суб’єкт-об’єктних відносин, що виникають в процесі вироблення та реалізації політики дезінформування, дослідження її наслідків та вироблення політичних інструментів протидії дезінформації. Тобто, інформативність дезінформації дозволяє використовувати теорії обміну інформацією в медіа середовищі з метою дослідження того, як суб’єкти медіасистеми формують судження та приймають рішення, якщо споживають неправдиву інформацію.

Ще один вектор дебатів в процесі концептуалізації дезінформації спрямовано на визначення змісту таких її характеристик як *умисел* та *фальшування*. Проблема умислу як джерела створення дезінформації пов’язана з диференціацією понять *місінформація* та *дезінформація*. Частина науковців вважають дезінформацію та місінформацію паралельними поняттями, які не мають предметного перетину [246], відповідно, місінформація означається як ненавмисна помилка [124, p. 13]. Водночас, достатньо численним є коло дослідників, які вважають, що місінформація є видом дезінформації [242], тому постає необхідність встановити співвідношення цих понять, що здійснюється через категорії *намір* та *мета введення в оману*. Останні позиціонуються як характеристики дезінформації [263].

Фальшування, як один з елементів дезінформації, зазвичай обмежується теоретичними рамками концептів хибності, неправди та неточності інформації. Класичне розуміння неточності інформації пов’язане К. Шенноном з появою шуму під час передачі сигналу [364]. З розвитком концептуальних досліджень, предметом яких є дезінформація, хибність, описується науковцями як її ознака,

а фальшування як процес. Хибність є матеріальним аспектом дезінформації, який піддається операціоналізації, відтак може бути виявлений та виміряний. Попри доведені маркери ідентифікації та класифікації хибності інформації та її неправдивості [115], її операціоналізація потребує опертя на контрольну точку – істину, що в дослідженнях дезінформації зазвичай означається як «доступні докази» та «експертний консенсус» [392, p. 140–141]. Але, як справедливо зазначають Дж. Куклінскі, П. Квірк, Д. Швідер та Р. Річ [280, p. 145–146] встановлення доступних доказів та експертних думок залежить від предмету політичного дискурсу, тому об'єктивна інформація (фактичні твердження), наприклад, щодо державної політики, формуються під час політичного процесу, а не виникають до його розгортання. Тому, оцінка істинної цінності інформації має здійснюватися в конкретний час [369].

Фальшування як процес створення та поширення дезінформації відображає наукову позицію дослідників, які фокусують увагу на процесі виникнення дезінформації та формуванні твердження щодо її (не)правдивості. Зазвичай науковці опираються на діаграму істини та сили М. Фуко [230], в якій відображена важливість дискурсу та боротьби за владу на основі легітимації однієї інформації як правдивої, а іншої як брехні (дезінформації). Таке постмодерністське заперечення об'єктивної істини має обмежені переваги для багатьох сучасних досліджень дезінформації. Зокрема, дослідження зусиль Європейського Союзу та України з розробки стратегій протидії дезінформації та розуміння її впливу на розгортання російсько-української війни вимагають, з метою розмежування правдивої інформації та дезінформації, опертя на оцінку та аналіз на основі доказів. Але, варто пам'ятати про доведені застереження щодо ризиків, пов'язаних із нормативним розмежуванням дезінформації та інформації, та продуктивний потенціал дихотомії *брехня – правда* в кризових ситуаціях. В таких ситуаціях особливого значення набувають технологічний та суспільний контексти, що можуть посилювати, або навпаки, нівелювати продуктивність дихотомії *брехня – правда* в досягненні політичних цілей [305]. Важливим контекстом є й тип політичного режиму, який може опиратися на дезінформацію

як риторичну зброю (авторитаризм) або інструмент переслідування (тоталітаризм).

Важливою частиною наукового дискурсу дезінформації є відсутність академічного консенсусу щодо визначення змісту даного поняття, яке необхідне для нормативно-правового регулювання протидії дезінформації. Попри відсутність чіткого правового визначення дезінформації в європейському праві, привертає увагу орієнтація на три впливові визначення дезінформації, які пройшли тривалий шлях стандартизації в академічних і політичних дебатах. По-перше, це визначення дезінформації, запропоноване К. Вордл і Х. Дерахшаном [393], по-друге – визначення, вироблене Європейською Комісією [168], по-третє – визначення, сформоване Групою експертів високого рівня з фейкових новин та онлайн дезінформації [179] (далі – HLEG). Всі вони мають особливе значення для концептуалізації дезінформації, оскільки закладені в поточне визначення політики протидії дезінфрмації та є основою Кодексу практик ЄС щодо дезінформації [168].

У доповіді К. Вордл і Х. Дерахшана, підготовленої для політичних інститутів ЄС, науковці проаналізували циркуляцію місінформації в контексті параметрів нанесення суспільної шкоди та порівняли її з дезінформацією у вимірі недоброчесності намірів: «Місінформація – це поширення неправдивої інформації, але без навмисного умислу нашкодити. Дезінформація – це свідомо поширена неправдива інформація, що має на меті завдати шкоди» [393, p. 20]. Згодом, HLEG у своєму звіті визначила дезінформацію як «неправдиву, неточну або оманливу інформацію, розроблену, представлену та пропаговану з метою навмисного заподіяння шкоди суспільству або з метою отримання прибутку» [179]. Опираючись на цей звіт, Єврокомісія означила такий зміст дезінформації: «підтверджена неправдива або оманлива інформація, створена, представлена та поширена з метою отримання економічної вигоди або навмисного обману громадськості та може завдати шкоди суспільству» [185]. З таких позицій дезінформація є загрозою демократичним політичним процесам в ЄС та

процедурі вироблення політики в усіх сферах функціонування Об'єднання [53, с. 184-185].

Порівняємо ці три визначення дезінформації за такими критеріями: характер інформації, суспільні наслідки, наміри, економічна вигода та мотиви дезінформування. Що стосується характеру інформації, то К. Вордл і Х. Дерахшан вказують, що дезінформація є «неправдивою інформацію» [393, p. 20], але в позиції Єврокомісії ми зустрічаємо, по-перше уточнення («перевірена неправдива» [185] інформація) та, по-друге, деталізацію («інформація, що вводить в оману» [185]. Експерти та аналітики HLEG також розширюють визначення К. Вордла і Х. Дерахшана, включи до нього «неточну» інформацію [179]. Ці відмінності у формулюваннях, на думку науковців, можуть мати суттєво більший вплив на свободу вираження поглядів, якщо застосовуються не у політичній, а у правовій площині [344]. Значна розмаїтість типів неправдивої інформації може бути розташована вздовж континууму від високої до низької фактичності, що актуалізує питання, чи може бути взагалі встановлена достовірність, якщо достовірність корелює з *низькою/високою* фактичністю інформації [58].

Проблема суспільних наслідків дезінформації також має відмінності на рівні трьох означених позицій, на які опираються в ЄС. К. Вордл і Х. Дерахшан найширше визначають суспільні наслідки дезінформації, позиціонуючи їх як шкоду «особі, соціальній групі чи державі» [393, p. 20], тоді як в позиціях Єврокомісія та HLEG йдеться лише про «суспільну шкоду» [179]. Експерти та аналітики HLEG деталізують визначення суспільної шкоди як «загрози демократичним політичним процесам і цінностям, які можуть бути спрямовані на різні сфери, такі як охорона здоров'я, наука, освіта, фінанси тощо» [179]. Єврокомісія, будучи політичним інститутом ЄС та приймаючи позицію HLEG, додає до запропонованої деталізації «процеси формування політики» [185].

Зауважимо, що у всіх трьох деталізованих означеннях суспільної шкоди дезінформації йдеться не про те, що шкода має бути заподіяна, щоб інформація

була кваліфікована як дезінформація. В позиції Єврокомісії йдеться про потенціал дезінформації («може завдати шкоди суспільству» [185]. Це означає, що незалежно від того, чи дезінформація тільки може спричинити шкоду суспільству чи вона вже її спричинила, не є суттєвим для того, щоб кваліфікували інформацію як дезінформацію. Натомість, К. Вордл і Х. Дерахшана та експерти HLEG вважають суспільну шкоду однією з матеріальних умов для дезінформації, що пов'язує останню з намірами. Позиція К. Вордла і Х. Дерахшана та експертів HLEG передбачає, що намір суб'єкта дезінформування спрямований на заподіяння шкоди, тоді як для позиції Єврокомісії характерним є означення дезінформації з позицій наміру ввести громадськість в оману. При чому, намір – це дія, спрямована на введення людей в оману, але не на заподіяння шкоди [375, p. 147]. Саме через використання категорії *намір*, визначення Єврокомісії є напрочуд широким, оскільки включає будь-яку неправдиву інформацію, яка транслюється в комунікаційному ланцюгу з наміром ввести громадськість в оману. На нашу думку, найбільш проблематичним у всіх трьох визначеннях дезінформації, на які опирається ЄС, є припущення про те, що вироблення дезінформації здійснюється одним суб'єктом в кожному окремому випадку, відтак, ми констатуємо відсутність позиції ЄС щодо перетину намірів різних суб'єктів (дез)інформування, залучених до створення та поширення дезінформації.

Така характеристика дезінформації як економічна вигода взагалі не згадується у концепті К. Вордла і Х. Дерахшана, але є помітно означеною у визначеннях Єврокомісії та HLEG, в яких позиціонується як альтернативна чи додаткова мета поширення дезінформації. Деталізуючи мету дезінформації як економічну вигоду, «навмисне введення громадськості в оману» (Єврокомісія) або «навмисне заподіяння шкоди громадськості» (HLEG), на рівні ЄС була сформована розширена сфера застосування категорії дезінформація до будь-якого типу неправдивої інформації в комерційному контексті. Зрештою, така характеристика дезінформації як мотивація розгортається через звернення не до властивостей інформації чи суб'єктів створення, а через те, як вони діють – якою

є стратегія дезінформування. Усі три аналізовані визначення дезінформації включають такі дії суб'єктів дезінформування, як «створення» (К. Вордл та Х. Дерахшан), «створення, представлення та поширення» (Єврокомісія) та «проєктування, презентація та просування» (HLEG). Зауважимо, що у позиціях Єврокомісії та HLEG залишається відкритим питання про те, чи є означені види дій характеристикою одного суб'єкта дезінформування, чий йдеться й про об'єктів дезінформування, що споживають дезінформацію та можуть її поширювати. Певні застереження щодо розширення рамок суб'єктності в процесі дезінформування через дії з поширення дезінформації можемо знайти в твердженні про те, що варто диференціювати стратегічне поширення дезінформації та споживацьке поширення.

Аналіз трьох концептів дезінформації, на які опирається ЄС у виробленні та реалізації політики протидії дезінформації вказує на те, що жоден із них не позиціонується як джерело правової норми. Експерти та аналітики HLEG заявили, що дезінформація не збігається з будь-якою існуючою правовою нормою, тому їх концепт «не стосується питань, що виникають унаслідок створення та розповсюдження незаконного контенту в Інтернеті, які підлягають регулятивним заходам згідно з законодавством ЄС або національними законами, а також з іншими формами навмисного спотворення фактів, але такими, що не вводять в оману, таких як сатира та пародія» [179]. Єврокомісія диференціює концепти дезінформації та політики протидії дезінформації від уже врегульованих європейським законодавством аспектів введення в оману. Політика ЄС щодо дезінформації є такою, що не впливає на «застосовні правові норми на рівні Союзу або на національному рівні» [185]. Тобто, на сьогодні, можемо констатувати концептуалізацію дезінформації та протидії дезінформації на рівні ЄС поза існуючими правовими категоріями незаконного та шкідливого контенту. На нашу думку, такий підхід обмежує як використання існуючих правових норм, такі і вироблення правового механізму обмеження поширення дезінформації.

Процес концептуалізації дезінформації та політики протидії дезінформації відображає пошук відповіді на питання про домінуючий фактор, що перетворює дезінформацію на суспільно значиму та політичну проблему. Наукові дискусії в цій площині пов'язані з осмисленням життєвого циклу дезінформації, відображеного в інформаційних потребах аудиторії, поширення (дез)інформації та споживанні (дез)інформації [124, p. 15]. Деталізуємо зміст цих дискусій.

Інформаційні потреби аудиторії багатьма науковцями розглядаються в контексті потенційного прояву інтересу до дезінформації. До основних причин проявів уваги до дезінформації вони відносять, по-перше, неуважність, яка відображає недостатність критичного мислення, підживлюється соціальними медіа, що монополізують фактичний контент та монетузують увагу аудиторії засобами простих повідомлень [335]. По-друге, психологічні особливості аудиторії, які відображають схильність вірити вмісту повідомлень або поширювати їх, якщо вони узгоджуються з переконаннями або підтверджують сформовані оцінки, особливо, коли інформаційне повідомлення має політично збалансований вміст [330]. Контент, який викликає сильні емоції чи актуалізує приховані почуття щодо політичних явищ, швидше за все, буде поширюватися, так само, як і дезінформація, що корелюється наративами теорії змови, які «усувають хаос» [372, p. 120]. По-третє, епістемологічні особливості, що відображають пошук інформації, застосування індивідуальних оцінювальних стандартів, індивідуальні стратегії перевірки інформації, ставлення до доказів та фактів. Зауважимо, що апробованою тактикою авторитарних політичних режимів є підрив здатності суспільства відрізняти правду (інформацію) від брехні (дезінформації) та формування зневажливого ставлення до доказів і фактів. На макрорівні це проявляється у глобальному зниженні рівня довіри до тих професій, які пов'язані з точністю інформації та її наданні суспільному загалу: політики, науковці, експерти. По-четверте, це рамки політичної ідентичності, які визначають ймовірність сприйняття, віри та поширення вмісту (дез)інформації, якщо він узгоджується з політичними переконаннями, навіть тоді, коли він доведено неправдивий. В низці сучасних досліджень кореляції

ідентичності, політичних переконань та дезінформації доведено, що праві політичні сили виробляють більше неправдивого контенту та перетворюють дезінформацію на функцію партійної ідентичності, яка постає як основа логіки взаємодії з прихильниками партійної ідеології [330]. На думку В. Філіпс і Р. Мілнер, сталі партійні ідентичності створюють стабільну інфраструктуру наративів, що визначає як людина розуміє політичний процес, вона: «формує наші реалії та, відповідно, наші дії, настільки ґрунтовно й безперебійно, що люди … навіть не підозрюють» [338] про це. Відповідно, якою є інформація – правдивою чи хибною, є не таким важливим для людини, як інфраструктура значення та наративу, що резонує з дез(інформацією).

Розв'язання проблеми концептуалізації дезінформації, як зазначалося вище, конкретизується в осмисленні процесу поширення та циркуляції (дез)інформації, провідна роль в якому науковцями відводиться соціальним мережам та новинним медіа (ЗМІ). Роль соціальних мереж в циркуляції дезінформації пов'язується зі структурою стимулів, які застосовуються ними під час поширення неправдивого або екстремального контенту, зокрема, пропозиція використати позначки *подобається* та *поділитися* стимулюють зацікавленість до повідомлення, незалежно від його (дез)інформаційного характеру. Свого часу М. Цукерберг визнав [98, p. 19], що чим більше вміст контенту наближений до порушення стандартів спільноти, чим більш екстремальним він є, тим більшу увагу він викликає у користувачів соціальної мережі, має більше охоплення аудиторії та вищий рівень залучення уваги. Не менш важливим фактором є широке віяло можливостей монетизації від споживання та поширення (дез)інформації, що стимулює власників контенту, орієнтованих на отримання прибутку, створювати максимально широку аудиторію за допомогою провокативного та дезінформаційного контенту [122]. Сприяє цьому алгоритмізована природа рекомендацій цифрових платформ, яка здатна забезпечити просування неправдивого контенту. Виразним прикладом впливу алгоритмів на привернення уваги до дезінформаційних повідомлень є алгоритми рекомендацій на YouTube. Попри численні спроби платформи модерувати відео,

які поширюють дезінформацію, їх циркуляція на YouTube продовжується [377]. Для демократичного політичного процесу найбільш небезпечним є опертя на алгоритми мікротаргетингу в соціальних мережах, що передбачає адаптацію реклами до інформаційних потреб кожного члена спільноти через використання персональних демографічних та поведінкових даних [157]. Концептуалізація ролі ЗМІ в поширенні дезінформації в сучасній політичній науці здійснюється через розгортання проблем: критичного скорочення незалежних та високоякісних новинних і аналітичних ЗМІ, як фактору, що сприяє утворенню новинного вакууму, який заповнюється дезінформацією [116]; порушенням логіки руху новинного контенту, коли джерелом інформації для новин стають маргінальні цифрові ЗМІ [98]; агресивною та епатажною стилістикою інформування як засобу привернення уваги до ЗМІ, але й водночас, простору для продукування елементів дезінформації [102].

Теоретизування проблеми споживання (дез)інформації як фактору, що перетворює дезінформацію на суспільно значиму та політичну проблему здійснюється в парадигмі намірів і мотивації створення й поширення неправдивого вмісту з метою отримання фінансових чи політичних дивідендів. Зокрема, науковці привертають увагу до суб'єктності держав (Росія, Китай, Іран) в процесі вироблення та реалізації політики дезінформації під час електоральних процесів в США, ЄС та державах-членах ЄС не тільки з метою впливу на результати виборів, але й з метою підриву демократичних норм і довіри до демократичних інститутів та переформатування геополітичної карти світу через російсько-українську війну [51, с. 232-234]. Останнім часом до площини теоретичного осмислення дезінформації була включена проблема використання дезінформації національними політичними акторами в просторі внутрішньої політики, які «стратегічно використовують відмінності, засновані на ідентичності та ставленні до існуючих структур влади» [82, p. 4] з метою створення гомогенного та неконкурентного політичного середовища на рівні національної держави.

Таким чином, якщо дезінформація як інструмент зовнішньої політики спрямований на домінування, то у внутрішній політиці – на підкорення громадського та суспільного. Неперервність сучасної геополітичної турбулентності спричинила зростання інтересу академічних спільнот до вивчення процесів вироблення та циркуляції дезінформації й принципів політики протидії поширенню дезінформаційних наративів. Небезпеки дезінформації пов'язані з її можливостями проявлятися як на суспільно-політичному рівні у формах, що спотворюють процес демократичного політичного управління, так й індивідуальному, впливаючи на формування громадської думки та сприйняття демократично ухвалених політичних рішень.

Здійснений аналіз особливостей концептуалізації поняття *дезінформація* в сучасній політичній науці вказує на неможливість створення уніфікованої теорії дезінформації, навіть в ситуації актуальної потреби посилення концептуальної точності. Однією з основних проблем, розв'язання якої сприятиме формуванню чіткого, але гнучкого концепту дезінформації, є проблема одночасного, а часом синонімічного, застосування низки категорій та понять через які описують емпіричний зріз дезінформації. Досягнення наукового консенсусу щодо вимірюваних характеристик дезінформації буде тим кроком, який наблизить можливість вироблення актуальних та застосовних в реальних політичних процесах моделей політики протидії дезінформації. Принциповим, на нашу думку, є визначення належного місця політичного та політично значимого контексту виникнення та поширення дезінформації. Результати дослідження вказують на те, що можна означити низку характеристик дезінформації, які є спільними для більшості позицій, артикульованих в сучасному політологічному дискурсі: оманливий характер інформації; суспільна шкода; наміри суб'єкта дезінформування (політичного актора); економічна вигода; зв'язок з проблемами, що мають суспільне значення; стратегічний характер поширення.

1.2. Методологічні принципи та концептуальні рамки дослідження протидії дезінформації в сучасній політичній науці

Для дослідження політики протидії дезінформації, її механізмів та інструментів особливе значення мають концептуальні рамки неоінституціоналізму. У максимально широкому вимірі цей методологічний підхід дозволяє пояснити, як політичні інститути та інституції формують правила гри у сфері інформаційної безпеки та визначають моделі діяльності політичних акторів. Неоінституціоналізм у політичній науці бере свій початок із публікації Дж. Марча та Й. Олсена «Новий інституціоналізм: організаційні фактори у політичному житті» [304, p. 734-739] 1984 р., яка стала знаковою для переосмислення методологічних засад дослідження політики. Автори наголошували, що період «забуття інститутів» суттєво обмежив аналітичні можливості політичної науки, оскільки дослідження надмірно зосереджувалися на поведінкових та функціоналістських поясненнях. Дж. Марч і Й. Олсен підкреслювали необхідність подолання контекстуалізму, який трактував політику як просте відображення середовища; редукціонізму, що зводив політичні явища до індивідуальної поведінки; утилітаризму, який пояснював дії виключно через раціональний інтерес; функціоналізму, що розглядав історію як механізм досягнення рівноваги; та інструменталізму, який зводив політику до процесу ухвалення рішень і розподілу ресурсів. Усі ці підходи, на їхню думку, були підживлені біхевіоралізмом та структурним функціоналізмом і не відображали складності політичної реальності [304, p. 735]. Водночас неоінституціоналізм вони пропонували розглядати не як радикально нову методологію, а як пошук альтернативних ідей, що дозволяють упорядкувати практичний досвід у теоретично придатній формі. Його сутність вони визначали як «узагальнений підхід до вивчення політичних інститутів, набір теоретичних ідей та гіпотез, що стосуються відносин між інституціональними характеристиками політичних акторів, їх діями» [303] та трансформаціями у політичному просторі.

Запропоноване Дж. Марчем та Й. Олсеном визначення політичного інституту стало основним для науковців, які покладаються на дослідницький інструментарій методології неоінституціоналізму: «Інститут є відносно стійким набором правил і організованих практик, втілених в структурах значень та ресурсів, які є інваріативними стосовно індивідів та стійкими перед специфічними перевагами і очікуваннями індивідів та перед зовнішніми умовами, що змінюються» [304]. У цьому підході центральним припущенням є те, що саме інститути забезпечують порядок і передбачуваність у політичному просторі. Відповідно, базовими одиницями аналізу виступають категорії, що відображають мезорівень політики – правила, норми, порядки та значення, які визначають функціонування інститутів, а не індивідуальні раціональні дії чи макросоціальні тенденції. На основі дослідження внутрішньої динаміки розвитку інститутів Дж. Марч та Й. Олсен запропонували розрізняти інститути агрегування, які характеризуються укладанням внутрішніх угод та рішень, що випливають із перебігу політичного процесу, та інститути інтеграції, для яких властивий інтегративний характер ухвалення рішень, що спирається на історичний досвід, зобов'язання та раціональність. Зосередження уваги на нормах і правилах функціонування політичних інститутів стало підґрунтям для окреслення цих ідей як нормативного інституціоналізму, що визначив новий напрям у політичній науці.

На нашу думку, ці ідеї Дж. Марча та Й. Олсена можуть бути застосовані для політологічного дослідження механізмів та інструментів протидії дезінформації. Якщо виходити з їхнього припущення, що саме інститути забезпечують порядок і передбачуваність у політичному просторі, то політика протидії дезінформації має розглядатися як інституційно закріплена система норм, правил і значень, що визначають дії політичних акторів. Запропонована дослідниками диференціація інститутів агрегування та інститутів інтеграції дозволяє зрозуміти, як ухвалюються рішення щодо конкретних заходів протидії дезінформації (інститути агрегування) та пояснити, як ці рішення інтегруються

у ширший політичний порядок, заснований на історичному досвіді, зобов'язаннях та раціональності (інститути інтеграції).

Згідно з аналізом П. Ґолла та Р. Тейлора, у перше десятиліття після виходу праці Дж. Марча та Й. Олсена у політичній науці сформувалося три основні напрями неоінституціоналізму. Одним із них став історичний неоінституціоналізм, витоки якого пов'язують із дослідженням Г. Алмонда «Повернення до держави» (1988) [79]. Г. Алмонд, який раніше активно просував ідею використання біхевіоралізму та структурного функціоналізму в політологічних дослідженнях, сприяв поверненню категорям «держава» та «політичний інститут» статусу центральних у політичній науці [79, p. 863]. Для історичного інституціоналізму характерним є розуміння політичного інституту як комплексу формальних і неформальних процедур, рутин, норм та домовленостей, що глибоко вкорінені в організаційній системі політичної структури [245, P. 936]. Базовим методологічним принципом цього напряму є концепція «траєкторії попереднього розвитку» [394], яка пояснює, що первинний інституційний вибір, здійснений у минулому, визначає логіку політичного процесу та ухвалення рішень у майбутньому. Зауважимо, що історичний неоінституціоналізм розвивається у трьох основних напрямах, які по-різному пояснюють джерела формування інституційного дизайну та взаємодію політичних акторів. К. Оррен та С. Сковронек трактують виникнення й трансформацію політичних інститутів як процес, що рухається згори донизу, тому головну увагу приділяють діям еліт, лідерів та груп інтересів, які ухвалюють політичні рішення,створюють структури влади, продукують ідеї, що визначають модель дій інших суб'єктів політичного процесу [367]. Т. Скокпол та Е. Клеменс, навпаки, інтерпретують динаміку інститутів як процес, що йде знизу догори, акцентуючи на ролі інститутів громадянського суспільства у зміні інституційного дизайну в історичній перспективі [366]. В. Меркель та Н. Круассан пропонують третій підхід, у якому розвиток інститутів розглядається як результат взаємодії політичних інститутів та агентів публічної політики, що

дозволяє пояснити інституційні зміни як продукт постійного діалогу між владою та суспільством [310].

Для нашого дослідження можуть бути використані окремі ідеї історичного неоінституціоналізму, що дозволяють пояснити, як траєкторії розвитку політичних систем визначають сучасні можливості реагування на інформаційні загрози. Це означає, що політика протидії дезінформації не може бути зрозумілою без аналізу того, як у минулому формувалися механізми комунікації, інституційні практики та відносини між державою, суспільством і медіа. Методологічний принцип опертя на «траєкторії попереднього розвитку» дає змогу пояснити, чому одні держави здатні виробляти більш ефективні інструменти протидії дезінформації, тоді як інші залишаються вразливими, оскільки цикл публічної політики в сучасних державах (об'єднаннях держав) є, зокрема, й наслідком історично сформованого характеру політичної комунікації та практик формування довіри до політичних інститутів. Ідеї В. Меркеля та Н. Круассана про роль взаємодії політичних інститутів та агентів публічної політики відкривають можливість аналізувати протидію дезінформації як результат постійного діалогу між владою та громадянським суспільством.

Інституціоналізм раціонального вибору став другим напрямом методології неоінституціоналізму. Його прихильники пропонують трактувати політичні інститути крізь призму теорії раціонального вибору [337], тому політичні інститути «моделюються як обмежувачі дії ..., що регулюють послідовність кроків, до яких вдаються актори під час їх взаємодії, що пливають на вибір рішення конкретних акторів або на структуру доступної для них інформації» [396]. Така перспектива надає досліднику інструменти для аналізу мікрорівня функціонування політичних інститутів, концентруючи увагу на двох рівнях: по-перше, на дослідженні результатів діяльності інститутів як відносно незмінних та екзогенних величин; по-друге, на визначенні причин, чому інститути набувають конкретних форм, що дозволяють їм залишатися ендогенними елементами політичного процесу. Поєднання цих рівнів аналізу відкриває можливість пояснювати результати впливу інститутів, особливості політичної

взаємодії та процеси еволюції й відтворення інституцій у політичному часі, що робить інституціоналізм раціонального вибору важливим інструментом для розуміння складної динаміки політичних систем. Б. Вейнгаст окреслив чотири ключові характеристики, які відрізняють інституціоналізм раціонального вибору від інших напрямів неоінституціоналізму. По-перше, цей підхід забезпечує можливість систематичного аналізу політичних інститутів, що дозволяє досліднику працювати з чітко визначеними аналітичними рамками. По-друге, його «виключно компаративний характер» відкриває шлях до прогнозування різних варіантів та кінцевих результатів інституційних обмежень, а також дає змогу отримувати статистичні дані, які демонструють взаємозв'язок між діями акторів та інституційними структурами. По-третє, цей підхід дозволяє досліджувати, як політичні актори впливають на інститути в умовах змін, що робить можливим пояснення процесів адаптації та трансформації інституцій. По-четверте, інституціоналізм раціонального вибору створює умови для застосування мікроаналітичних інструментів до вивчення макрополітичних явищ, що забезпечує комплексне розуміння політичної динаміки та дозволяє поєднувати індивідуальний рівень дій із системними процесами [396].

Прихильники неоінституціоналізму раціонального вибору визначають інститути як «створені людиною обмежувальні рамки, що організують взаємовідносини між людьми» [327, p. 8-9], надаючи структурованості соціальним і політичним взаємодіям. Виникнення інститутів трактується не як об'єктивна даність, а як результат раціонального вибору політичних акторів, які створюють правила гри для забезпечення передбачуваності та стабільності. Водночас, після формування, інститути набувають статусу зовнішньої реальності щодо політичних акторів і починають функціонувати як об'єктивні рамки, що визначають політичні дії. Дотримання встановлених правил у цьому підході не є імперативом, а розглядається як наслідок раціонального вибору, коли актори зважують вигоди та ризики. Хоча представники цього напряму неоінституціоналізму визнають можливість спонтанного виникнення інститутів, зорієнтованих на виконання регулятивних функцій у політичному просторі, вони

заперечують, що такі «спонтанні інститути» можуть самостійно формувати переваги політичних акторів [52, с. 121]. Натомість акцент робиться на очікуваних реакціях учасників політичної взаємодії, які визначаються нормативно-ціннісними рамками інституційного середовища.

Ідеї неоінституціоналізму раціонального вибору можуть бути використані для дослідження механізмів та інструментів протидії дезінформації для дослідження та пояснення того, як саме інституційні обмеження впливають на вибір стратегій протидії дезінформації, які ресурси мобілізуються та які результати досягаються. Важливим методологічним принципом для нашого дослідження є те, що інститути не є даністю, а формуються як продукт раціонального вибору, проте після створення вони набувають ознак зовнішньої реальності, що змушує політичних акторів враховувати їх як об'єктивні рамки. У контексті протидії дезінформації це означає, що політичні інститути можуть бути сконструйовані для забезпечення прозорості, підзвітності та ефективності інформаційної політики, але водночас їхня стійкість залежить від того, наскільки раціонально актори дотримуються встановлених правил.

Разом з тим, неоінституціоналізм раціонального вибору має методологічні обмеження, на які звертали увагу Б. Вейнгаст та Д. Норт. Вони пов'язані з: недостатньою увагою до неформальних практик та варіативності невизначеності у момент вибору, що потребує поєднання його з іншими неоінституціональними концепціями для комплексного аналізу політики протидії дезінформації. Так, Д. Норт, аналізуючи інституційні зміни в системі економічних та політичних відносин, звернув увагу на проблему, яка має безпосереднє значення і для дослідження механізмів протидії дезінформації. Він наголошував, що роль неформальних обмежень у функціонуванні інститутів не може бути точно описана чи визначена, проте «вони мають велике значення» [327, p. 43]. На думку Д. Норта, природа цих неформальних правил закорінена в інформації, яка передається через соціальні механізми і становить «частину тієї спадщини, яку ми називаємо культурою» [327, p. 44]. Саме процес передачі та особливості обробки інформації він вважав ключем до розуміння моделей поведінки, що

формуються на основі очікуваної корисності. У контексті політики протидії дезінформації ця ідея дозволяє пояснити, чому неформальні інституційні практики, закріплені культурою та соціальними нормами, можуть мати вирішальний вплив на ефективність інструментів боротьби з маніпулятивними інформаційними потоками.

Неформальні правила, які виникають як механізми координації стійких і повторюваних форм людської взаємодії, мають кілька вимірів. По-перше, вони виступають продовженням і модифікацією формальних інституційних норм, по-друге, функціонують як соціально санкціоновані стандарти поведінки, а по-третє, стають внутрішньо обов'язковими для індивіда [327, p. 51]. Д. Норт наголошував, що перші дві характеристики цілком узгоджуються з методологічними принципами неоінституціоналізму раціонального вибору, який ґрунтується на моделі максимізації вигод. Водночас третя характеристика виходить за межі цієї моделі, адже передбачає ситуації, коли людина приймає рішення, що означають відмову від матеріальних вигод чи доходу на користь інших цінностей, важливих у межах її індивідуальної функції корисності [327, p. 53]. Це вимагає звернення до складнішого аналізу мотивації, ніж той, що пропонує проста модель очікуваної корисності. Д. Норт підкреслював, що сучасні поведінкові науки не мають пояснювальної моделі для оцінки ефективності чи неефективності організованих ідеологій або для розуміння вибору в ситуаціях, коли чесність, непідкупність, наполеглива праця чи голосування не приносять вигоди [327, p. 53]. Саме тому він пропонував досліджувати неформальні практики та норми за допомогою теорії ігор, яка дозволяє моделювати поведінку акторів у складних умовах взаємодії та невизначеності.

Д. Найт, аналізуючи артикульовану проблему невизначеності у момент вибору, виокремив кілька аспектів, які мають значення для розуміння політичної взаємодії та можуть бути використані у дослідженні механізмів протидії дезінформації. Він зазначав, що невизначеність може виникати щодо: альтернатив, доступних для політичних акторів у конкретний момент; наслідків

вибору з наявних альтернатив; вибору, який здійснять інші актори, що вступають у взаємодію; власних майбутніх переваг; альтернатив, які можуть з'явитися у майбутньому; потенційних наслідків вибору з доступних альтернатив [276, p. 45]. У контексті політики протидії дезінформації ці аспекти дозволяють пояснити, чому політичні актори стикаються з багаторівневою невизначеністю, коли ухвалюють рішення щодо інформаційних стратегій. Д. Найт наголошував, що оцінка невизначеності здійснюється за допомогою методів політичного прогнозування, проте стандартизованих методик у сучасній політичній науці ще не вироблено.

Соціологічний неоінституціоналізм, який сформувався у перше десятиліття розвитку неоінституціоналізму як методологічного напряму політичної науки, став одним із ключових його відгалужень. Його інтелектуальні витоки сягають концепцій М. Вебера, котрий довів, що процес інституціоналізації нерозривно пов'язаний із легітимністю та механізмами легітимації. Продовжуючи веберівську традицію, В. Скотт визначив інститути як поєднання «когнітивних, нормативних та регулятивних структур і діяльності, які виробляють стабільність і надають значимість соціальній поведінці» [361. p. 33]. Відтак головним завданням політичного аналізу, на думку Е. Іммергута, є дослідження умов, за яких інститути здобувають легітимність у мінливому суспільному середовищі [255, p. 21]. Зосереджуючи увагу на процесах агрегування та артикуляції групових інтересів, а також на їх трансляції мовою домінантних цінностей, соціологічний інституціоналізм пропонує інструментарій для вивчення самоорганізації суспільних структур, норм і практик. Позиції його представників сходяться на тому, що політичні уподобання формуються через агреговані інститути, а колективні рішення на інституційному рівні не є простою сумою індивідуальних виборів, а виникають під впливом інституціональних рамок і структур. Методологічні принципи соціологічного неоінституціоналізму в нашому дослідженні можуть бути застосовані для аналізу політичних механізмів протидії дезінформації, оскільки вони дозволяють розглядати інститути як складні поєднання когнітивних,

нормативних та регулятивних елементів, що формують сталість і надають значення соціальній поведінці. Це означає, що політика протидії дезінформації має опиратися на ідею здатності політичних інститутів артикулювати суспільні інтереси в рамках загальноприйнятих норм і цінностей, що підвищує їхню легітимність у динамічному інформаційному середовищі. В свою чергу, інституційні рамки впливають на процеси самоорганізації громадян, які створюють практики перевірки інформації, формують стандарти комунікації та беруть участь у прийнятті рішень щодо протидії форм організації протидії дезінформаційним впливам.

Завершення етапу становлення традицій неоінституціоналізму було позначене виходом монографій «Теорії інституціонального дизайну» [238] (1996). Проте навіть передбачене методологією неоінституціоналізму поєднання якісного опису та кількісного вимірювання політичних інститутів залишає низку концептуальних і практичних питань відкритими. Серед них, зокрема, питання про те, які саме характеристики інституцій сприяють трансформаціям, а які забезпечують їхню стійкість; які чинники здатні порушити процес відтворення та регенерації політичних інститутів; чи можна простежити закономірний зв’язок між фазами адаптації та періодами радикальних змін; які елементи інституційної моделі виявляються найбільш результативними для досягнення очікуваних політичних ефектів.

Здійснений аналіз основних напрямів методології неоінституціоналізму, що можуть бути застосовані для дослідження політики протидії дезінформації дозволяє визначити зміст поняття «механізм протидії дезінформації». У межах історичного неоінституціоналізму поняття механізму протидії дезінформації визначається через аналіз довготривалих траєкторій розвитку політичних інститутів та їх здатність адаптуватися до нових викликів, тому механізм протидії дезінформації постає як результат накопичених інституційного досвіду конкретних політичних інститутів, що функціонують в рамках однієї політичної системи, забезпечують її стійкість до впливів дезінформації та здатність до відновлення в процесі протидії дезінформації. Версія раціонального вибору у

неоінституціоналізмі дозволяє визначати механізм протидії дезінформації як систему стратегічних дій індивідів та груп, які діють у межах інституційних правил і прагнуть максимізувати власні вигоди. У цьому випадку інститути виступають як арбітри, що встановлюють правила гри, а механізми протидії дезінформації розглядаються як набір стимулів і санкцій, які змушують акторів дотримуватися норм достовірної комунікації. Методологічні принципи соціологічного неоінституціоналізму уможливлюють визначення механізму протидії дезінформації через призму когнітивних, нормативних та регулятивних структур, які забезпечують легітимність інститутів у динамічному середовищі гібридної війни. Легітимність інституцій, що є частиною механізму протидії дезінформації, є вирішальною умовою їхньої ефективності, адже саме вона забезпечує довіру суспільства до колективних рішень, які формуються під тиском інституційних рамок. Відповідно, інструменти протидії дезінформації постають як історично зумовлені практики, раціонально сконструйовані стимули та санкції, соціально легітимізовані норми і цінності, що забезпечують ефективність інституційної відповіді на дезінформацію.

Дезінформація є багатовимірним явищем, яке впливає на всю сукупність суспільно-політичних, економічних та соціокультурних процесів, що розгортаються в рамках тієї чи іншої політичної системи. Саме така характеристика дезінформації спрямовує на використання методології неофункціоналізму в дослідженні механізмів та інструментів протидії дезінформації. Неофункціоналізм акцентує увагу на механізмах «spillover», коли зміни в одній підсистемі стимулюють трансформації в інших, і саме це дає змогу зрозуміти, як інформаційна безпека стає частиною ширших процесів.

Застосування методології неофункціоналізму до вивчення політики протидії дезінформації в ЄС передбачає перенесення ключових концептів цієї теорії, зокрема поняття «spillover», ролі наднаціональних акторів і процесів інтеграції, які описав Е. Гаас (1958) [244], на аналіз сучасних інформаційних політик, в яких секторні ініціативи в одній сфері (наприклад, медіа- та цифрове регулювання) породжують тиск на посилення координації й регулювання в

суміжних сферах, що створює ланцюгові ефекти у протидії дезінформації [267, p. 60]. Неофункціоналістська методологічна перспектива дозволяє розглядати Єврокомісію та Європейську службу зовнішніх справ як агентів політичного «справжнього інтеграційного двигуна», здатних ініціювати технічні та нормативні рішення, які потім «розтікаються» по національних системах через механізми співпраці, мережеві зв'язки і процедури імплементації, що важливо в дослідженні ініціатив із координації політики протидії дезінформації в ЄС, державах-членах та державах-кандидатах [325]. У методологічному плані це означає фокус на процесах, які породжують політичні ефекти через міжінституційні взаємодії: з'являється можливість відстежувати, як технічні рішення (наприклад, стандарти модерації контенту або алгоритмічної прозорості) трансформуються в політичні норми і як ці норми «перетікають» між рівнями управління, генеруючи нові інструменти та практики [359].

Застосування методології нефункціоналізму дозволить, зокрема, проаналізувати як Action Plan on Disinformation [183], що є ініціативою на рівні ЄС, стимулював створення мереж реагування, які вплинули на дії соціальних платформ, політичних інститутів держав-членів та громадянського суспільства. Методологічно це передбачає поєднання процес-трейсингу для виявлення причинно-наслідкових ланцюгів «spillover», аналізу політичних мереж для картографування акторів і каналів впливу, а також інституційного аналізу політичного дизайну для оцінки, які саме інституційні конфігурації найбільш сприятливі для стійкої протидії дезінформації [359]. Методологія неофункціоналізму також дозволяє враховувати зворотні зв'язки, тобто реакції держав-членів та практики соціальних платформ у відповідь на європейську політику протидії дезінформації, що модифікує наднаціональні політики, створюючи цикли інтеграції чи фрагментації принципів та моделей протидії дезінформаційним загрозам [272].

Таким чином, методологія неофункціоналізму є тією частиною аналітичної рамки дослідження, яка підкреслює динамічну, багаторівневу і мережеву природу політики протидії дезінформації в ЄС. Відповідно, поняття механізму

протидії дезінформації не може бути зведене до окремих інструментів чи санкцій, а розглядається як інтеграційний процес, де взаємодія між наднаціональними та національними інститутами породжує нові практики, що стають обов'язковими для всіх учасників. Він відображає інтеграційну динаміку, що поєднує нормативні, інституційні та комунікативні елементи, забезпечуючи поступове розширення та поглиблення політики боротьби з інформаційними загрозами в багаторівневому європейському просторі. Відтак, інструменти протидії дезінформації, відповідно до методологічних рамок неофункціоналізму, можуть бути визначені як сукупність технічних, організаційних, комунікаційних, правових та нормативних засобів, що формуються унаслідок взаємодії наднаціональних агентів, національних урядів та приватних акторів, і які поступово набувають обов'язкової сили через механізми «spillover» та інституційне закріплення.

Методологія неоінституціоналізму та методологія неофункціоналізму, які визначають каркас дослідження механізмів та інструментів протидії дезінформації в ЄС пов'язані з політологічним концептом стійкості. В методології неоінституціоналізму стійкість означається як здатність політичних інститутів зберігати легітимність, відтворювати нормативні структури й забезпечувати сталість політичних практик навіть у динамічному інформаційному середовищі [359]. Неофункціоналізм визначає стійкість як результат інтеграційної динаміки «spillover», коли інституційні інструменти, створені на наднаціональному рівні, поступово поширюються на національні політики та корпоративні практики, формуючи багаторівневу систему реагування. У цьому підході стійкість політики протидії дезінформації забезпечується здатністю наднаціональних агентів створювати нормативні рамки, які закріплюються через інституційні механізми та зворотні зв'язки між рівнями управління.

В сучасній політичній науці концепт стійкості стає ключовим для осмислення політики протидії дезінформації, адже саме він дозволяє зрозуміти, як суспільні та інституційні системи реагують на інформаційні атаки,

відновлюють баланс і формують довготривалу здатність до захисту. Зазвичай, в дослідницьких стратегіях стійкість постає, по-перше, як багатовимірний аналітичний інструмент, що допомагає пояснити різні рівні опору та адаптації. Якщо розглядати її як здатність до відновлення, то мова йде про швидкість і ефективність повернення суспільства до нормального функціонування після хвилі дезінформаційних кампаній. По-друге, у випадку інтерпретації стійкості як підтримання бажаного стану, акцент робиться на збереженні демократичних норм і довіри до інституцій, що є критично важливим у контексті інформаційної безпеки. По-третє, коли стійкість розуміється як здатність протистояти стресу, вона описує межу, за якою дезінформація може трансформувати політичну систему, змінюючи її у небажаному напрямі. По-четверте, у сучасних дослідженнях особливого значення набуває підхід, де стійкість трактується як здатність адаптуватися та навіть динамічно розвиватися після кризових інформаційних впливів: суспільство не лише відновлює рівновагу, але й виробляє нові механізми захисту, підвищуючи свою готовність до майбутніх викликів [292]. Таким чином, концепт стійкості стає не просто теоретичною категорією, а практичним орієнтиром для формування політики протидії дезінформації, яка має бути одночасно реактивною, превентивною та інноваційною.

Ми підтримуємо наукову позицію українського дослідника М. Назарова, який довів, що стійкість має багатовимірний концентричний характер і проявляється на індивідуальному рівні, рівні спільнот та національному рівнях [323]. Найбільше уваги в сучасному науковому дискурсі стійкості приділяється індивідуальній стійкості, оскільки саме вона формує основу здатності людини протистояти інформаційним атакам. У цьому контексті йдеться не лише про психологічну рівновагу, а й про здатність підтримувати критичне мислення, розпізнавати маніпулятивні повідомлення та зберігати стабільність функціонування в кризових умовах [92, с. 136]. Індивідуальна стійкість стає ключовим чинником нейтралізації негативних наслідків дезінформаційних впливів, адже саме персональні навички та когнітивні ресурси визначають, чи

зможе людина протидіяти інформаційному тиску [274, с. 143–145]. Вона описує винятково особистісний вимір, проте, водночас, закладає основу для формування стійкості спільнот і національної стійкості, які вибудовуються на базі індивідуальної здатності до опору.

Концепт індивідуальної стійкості дозволяє зрозуміти, як конкретна людина реагує на провокативні інформаційні впливи. Різні індивіди демонструють різний рівень здатності протистояти маніпуляціям, і тут вирішальну роль відіграє контекст – характер інформаційної події, її масштаб та соціальне середовище, у якому вона відбувається. Важливим чинником, що визначає рівень індивідуальної стійкості, є наявність соціальної підтримки, яка проявляється у стабільних міжособистісних контактах, здатності до сумлінної взаємодії та емоційній врівноваженості [286]. Дослідження показують, що сталі соціальні зв’язки суттєво підсилюють здатність людини зберігати психологічну стабільність і критичне мислення, що є ключовим для протидії дезінформаційним атакам. Водночас дефіцит соціальних контактів негативно позначається на емоційній рівновазі та знижує індивідуальну стійкість, роблячи людину більш вразливою до маніпулятивних повідомлень. Саме тому у вивченні політики протидії дезінформації індивідуальна стійкість розглядається як базовий рівень, від якого залежить ефективність колективних та інституційних механізмів захисту.

Стійкість спільнот у дослідженні політики протидії дезінформації має особливе значення, оскільки вказує на те, як індивіди здатні самоорганізовуватися та діяти колективно для досягнення спільної мети. Таким чином, стійкість спільноти визначається як здатність групи мобілізувати внутрішні ресурси, підтримувати взаємодію та ефективно працювати в умовах невизначеності [251, с. 401]. У цьому контексті важливо підкреслити, що дезінформаційні атаки спрямовані не лише на окремих індивідів, а й на соціальні спільноти, намагаючись підірвати їхню згуртованість і довіру, тому стійкість спільнот у протидії маніпуляціям та дезінформаційним впливам дозволяє, зберігаючи соціальну єдність, створювати механізми колективного реагування,

які підсилюють і індивідуальну, і національну (інституційну) стійкість. Уміння спільнот адаптуватися до непередбачуваних викликів, залучати ресурси та підтримувати внутрішню інтеграцію формує основу для ефективної політики протидії дезінформації, оскільки саме колективна дія забезпечує довготривалу здатність суспільства витримувати інформаційний тиск [249, p. 377].

Для вироблення дієвих інструментів політики протидії дезінформації принципове значення мають дві характеристики стійкості спільнот. По-перше, це методи посилення стійкості як реакції спільноти на кризові явища, коли відбувається мобілізація інтелектуальних, матеріальних, культурних та організаційних ресурсів для протидії загрозам [91]. Досвід спільного реагування, який закріплюється у колективній пам'яті спільнот стає основою формування стану потенційної готовності спільнот до повторних кризових явищ. У контексті дезінформаційних атак така здатність до колективної мобілізації та вироблення спільних стратегій дозволяє зміцнювати довіру та згуртованість, що в підсумку підсилює національну (інституційну) стійкість. По-друге, це капітал спільноти як сукупність фінансових та матеріальних активів, соціальних зав'язків, інтелектуальних можливостей, політичного впливу та людського потенціалу [227, p. 318]. Важливим елементом цього капіталу виступає лідерство, яке може бути як формальним, представленим офіційними керівниками, так і неформальним, коли активну роль відіграють лідери думок, підприємці чи представники цифрових спільнот. Ефекти соціального капіталу в протидії дезінформації проявляються як готовність членів спільноти брати участь у колективних діях, спрямованих на верифікацію інформації та аргументоване спростування дезінформації.

Зважаючи на те, що стійкість спільнот формується завдяки спільним зусиллям, які потребують участі та лідерства всієї спільноти, цей процес створює основу для довготривалої здатності протидіяти маніпуляціям. Коли різні соціальні групи, що мають власну автономію, об'єднуються навколо спільної мети, вони здатні виробляти узгоджені стратегії реагування, що значно підсилює ефективність протидії дезінформаційним кампаніям [93, p. 42]. Важливо

враховувати, що стійкість спільнот включає в себе елементи індивідуальної стійкості, адже кожна спільнота складається з окремих людей, і їхня здатність до психологічної та когнітивної адаптації впливає на колективний результат.

Національна (інституційна) стійкість охоплює інституційні механізми, правові рамки та стратегічні комунікації, які забезпечують системний опір масштабним інформаційним атакам і водночас підтримують довіру громадян до демократичних процесів [249, p. 370-374]. У дослідженні політики протидії дезінформації національна (інституційна) стійкість постає як один із найбільш значущих концептів, актуальність якого зумовлена тим, що сучасні інформаційні загрози не можуть бути пояснені лише крізь призму військової сили чи матеріальних ресурсів. Національна (інституційна) стійкість має спільні риси з індивідуальною стійкістю та стійкістю спільнот, адже йдеться про адаптацію до кризових умов, протидію негативним впливам та формування механізмів відновлення. Її вимірювання дозволяє оцінити, наскільки держава (об'єднання держав) здатні зберігати функціональність, підтримувати довіру громадян і водночас розвивати інституційні та комунікативні практики, які мінімізують ефект дезінформаційних кампаній [404, p. 39-40]. Зважаючи на те, що масштаб національної (інституційної) стійкості охоплює рівень держави (об'єднання держав), йдеться про системну здатність інституцій та громадян діяти разом, формуючи спільну відповідь на дезінформаційні виклики [144]. Саме тому концепт національної стійкості стає ключовим для розуміння того, як політика протидії дезінформації може бути інтегрована у ширший контекст безпеки та демократичного розвитку.

Визначення національної (інституційної) стійкості, запропоноване Н. Фрідландом, акцентує на тому, що справжня сила держави полягає не лише у військовому потенціалі чи матеріальних ресурсах, а й у здатності адаптуватися до кризових умов, впроваджувати зміни та водночас зберігати фундаментальні засади демократичного устрою. Це означає, що національна стійкість має аксіологічний вимір: у протидії зовнішнім загрозам, зокрема і дезінформаційним, важливо не просто вистояти, а захистити базові цінності, які

формують європейську ідентичність. У даному контексті особливої ваги набувають ідеї Б. Дора [96], який спільно з колегами запропонував чотири ключові складові, що характеризують здатність держави (об'єднання держав) до стійкості. В контексті дослідження проблеми вироблення механізмів та інструментів протидії дезінформації ці складові набувають такого змісту: патріотизм як емоційне ставлення до держави (об'єднання держав) та готовність громадян діяти заради спільного блага, що створює основу для мобілізації проти маніпулятивних впливів; оптимізм як віра у можливість позитивного сценарію нейтралізації загрози, що формує психологічну готовність спільнот до тривалого протистояння; соціальна інтеграція як здатність різних груп діяти узгоджено, створюючи колективні механізми протидії дезінформації та формуючи спільне бачення майбутнього; довіра до політичних та громадських інституцій як елемент координації зусиль, мінімізації хаосу і забезпечення ефективності стратегій інформаційної безпеки. Саме поєднання цих компонентів робить концепт національної стійкості ключовим для дослідження політики протидії дезінформації, адже воно показує, що успіх залежить від інституційних рішень, психологічних, соціальних та ціннісних чинників, які формують здатність суспільства витримувати і трансформувати інформаційні виклики.

Тема національної стійкості у політиці протидії дезінформації потребує розуміння її як процесу, що постійно змінюється та адаптується до нових викликів. Тому стійкість не є статичною характеристикою держави (об'єднання держав), а радше гнучкою системою, що реагує на політичні кризи, соціальні трансформації та інформаційні атаки. Ключові елементи стійкості держави (об'єднання держав), визначені Б. Дором (патріотизм, оптимізм, соціальна інтеграція та довіра до інституцій) не залишаються незмінними, а коливаються залежно від суспільних настроїв і зовнішніх загроз. Саме ця мінливість робить концепт стійкості держави (об'єднання держав) критично важливим для аналізу динаміки інструментів політики протидії дезінформації, що опирається на стратегічні програми, спрямовані на довгострокове посилення інституційної здатності до опору та оперативні політичні рішення, що дозволяють

відстежувати дієвість застосованих інструментів протидії дезінформації у реальному часі [120, p, 512-513]. Регулярний моніторинг функціональності інструментів політики протидії дезінформації дає змогу визначати, які фактори зміцнюють здатність суспільства протистояти інформаційним загрозам, а які, навпаки, її послаблюють. На нашу думку, європейська політика протидії дезінформації як джерело національної (інституційної) стійкості держави (об'єднання держав) постає як динамічна структура, що потребує постійного аналізу, корекції та адаптації.

Для оцінки функціональності механізмів та інструментів протидії дезінформації через концепт національної (інституційної) стійкості важливими є ідеї Ш. Кімхі, який пропонує трактувати явище стійкості як баланс між уявленням про силу держави та її вразливістю після кризових чи травматичних подій [164, p. 839-840], до яких, на нашу думку, належать і дезінформаційні впливи. Така інтерпретація дозволяє зрозуміти, що високий рівень стійкості означає здатність держави зберігати психологічну та інституційну рівновагу навіть після серйозних потрясінь, тоді як низький рівень демонструє переважання відчуття вразливості над відчуттям сили. Дослідження Ш. Кімхі, проведені в Ізраїлі, значною мірою зосереджені на реакції суспільства на терористичні загрози та тривалі військові конфлікти, що робить їх особливо релевантними для аналізу інформаційних атак, які мають подібний дестабілізуючий ефект.

Для застосування концепту стійкості в дослідженні механізмів та інструментів протидії дезінформації важливим є розуміння того, які чинники посилюють або послаблюють здатність індивіда, спільнот та держави (об'єднання держав) протистояти інформаційним загрозам. Національна (інституційна) стійкість виявляє негативні кореляції з рівнем негараздів, що переживають окремі індивіди та спільноти, адже слабкість на індивідуальному чи локальному рівні неминуче відображається на загальній здатності держави витримувати тиск [278]. Водночас відчуття узгодженості, соціальний добробут та стабільність економіки створюють позитивний ефект, підсилюючи

колективну готовність до протидії маніпуляціям. Психологічні чинники також мають вирішальне значення: дистрес і відчуття особистої небезпеки знижують рівень стійкості, тоді як здатність знаходити сенс у пережитих труднощах формує основу для посттравматичного – зростання [273, p. 519–520; 274]. Цей феномен показує, що навіть після серйозних криз суспільство може відновити позитивне бачення майбутнього, зберегти віру у власні сили та сформувати нові механізми адаптації [251, p. 351–353]. У контексті дезінформаційних атак це означає, що здатність людей і спільнот знаходити конструктивні інтерпретації власного досвіду стає ключовим ресурсом для підтримання національної (інституційної) стійкості.

Кожен із проаналізованих рівнів концепту стійкості має власну логіку та дозволяє визначати набір індикаторів для оцінки ефективності політики протидії дезінформації у кількісному та якісному вимірі. Саме через таку багаторівневу диференціацію концепт стійкості стає ключовим для розуміння того, як держава (об’єднання держав) може витримати інформаційний тиск в умовах гібридної війни та трансформувати його на поштовх до розвитку більш дієвих практик протидії дезінформації.

У сучасній науковій дискусії щодо протидії дезінформації та фейковим новинам окреслюються дві концептуальні моделі, які можна розглядати як крайні точки одного континууму, де на одному полюсі перебуває свобода, а на іншому – безпека. Патерналістська парадигма передбачає обмеження автономії індивіда, що виправдовується виключно міркуваннями про його благо, щастя, інтереси чи цінності [159, с. 65]. У цьому підході вважається допустимим застосування будь-яких інструментів, які здатні мінімізувати негативні наслідки дезінформації, включно з блокуванням джерел поширення інформації або навмисним коригуванням публічного дискурсу через пропагандистські практики [90]. Втручання у сфері інформаційної політики через заборони та обмеження традиційно розглядається як прояв патерналістського підходу [402]. Водночас патерналізм не обмежується діями державних інституцій, тому він може бути

характерним для корпоративних структур та наднаціональних організацій, які прагнуть контролювати інформаційні потоки [285].

Як альтернатива цьому підходу, що не вступає у суперечність зі свободою слова, сформувалася адаптивна парадигма. Її сутність полягає у зміцненні стійкості суспільства до дезінформації та фейкових новин шляхом впливу на громадян без застосування заходів, які «могли б... шкодити свободі слова» [313, p. 42]. У межах цього підходу акцент робиться на розвитку медіаграмотності, інституціоналізації фактчекінгу, покладанні відповідальності за якість інформації на її продуцентів та впровадженні механізмів саморегулювання цифрових платформ [78; 119; 290; 326]. Адаптивна парадигма у сфері протидії дезінформації трактує стійкість як здатності системи не просто відновлюватися, а здійснювати «стрибок уперед» [126, p. 6-7]. У цьому підході значна частина функцій делегується громадянам, тоді як держава обмежується формуванням інституційгного каркасу забезпечення стійкості.

У межах ЄС поняття «стійкість» вводилося поступово: перше офіційне використання терміну зафіксоване у документах Єврокомісії у 2012 р., а після ухвалення EUGS у 2016 р. воно стало центральним елементом зовнішньої політики. Н. Точчі, яка координувала процес розробки EUGS [20, с. 88], пояснює актуалізацію концепту стійкості необхідністю нелінійного підходу до сучасних загроз та визнанням обмежених можливостей держави (об’єднання держав) у запобіганні та прогнозуванні ризиків. ЄС маркує дезінформацію як складову таких викликів, тому використовує рамки, вироблені соціальними науками, для інституціоналізації поняття стійкості. Неоліберальна природа ЄС стала додатковим чинником прийняття моделі стійкості, відповідної адаптивній парадигмі, проте офіційні документи ЄС та його держав-членів демонструють різні інтерпретації того, яким чином слід забезпечувати стійкість до дезінформаційних загроз.

1.3. Аналіз джерельної бази дослідження

Визначення сукупності та функціональності механізмів та інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни потребувало використання різноманітних джерел. Використаний у дослідженні масив джерел дозволив нам ґрунтовно та всебічно охарактеризувати теоретико-методологічні засади дослідження протидії дезінформації в умовах гібридної війни, визначити основні принципи політики протидії дезінформації в ЄС та державах-членах як основи формування європейського механізму реагування на інформаційні загрози в умовах гібридної війни, дослідити безпекові інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни, вивчити інформаційно-комунікаційні інструменти реалізації європейської політики протидії дезінформації в умовах гібридної війни, розкрити роль національних моделей протидії дезінформації у формуванні віяла інструментів європейської політики протидії дезінформації, визначити роль та місце досвіду України у формування стійкості європейської політики протидії дезінформації. Сукупно використані джерела ми можемо структурувати за наступними напрямами.

Інституційна еволюція та регіональні пріоритети нами розкрито через процес формування та розширення компетенцій оперативних груп StratCom (East, South, Western Balkans), які детально висвітлений у брифінгах Н. Бентзен [звітах EEAS. Діяльність флагманського проєкту EUvsDisinfo та розвиток Системи швидкого сповіщення (RAS) аналізуються як практичні механізми операційної координації та верифікації. Окремо досліджено питання взаємодії ЄС та НАТО у регіональному вимірі, зокрема на Балканах. Дискусії щодо концептуальних розбіжностей у підходах країн-членів до відносин із РФ висвітлені у працях Б. Роггевеен. Перехід від боротьби з окремими фейками до протидії іноземним маніпуляціям та втручанням (FIMI) обґрунтований у серії спеціалізованих звітів EEAS за 2023–2025 рр. Ці документи дають змогу ідентифікувати тактики ворожих акторів, включаючи використання «сірих зон» у внутрішньоєвропейському дискурсі, що підтверджується кейсами протестів

фермерів. Регіональні особливості російського впливу, зокрема на прикладі Грузії, висвітлені у науковій розвідці Н. Нечаєвої-Юрійчук.

Концептуальне підґрунтя для розробки стратегічних наративів та моделей стійкості, зокрема психологічних її аспектах, сформовано у наукових працях М. Вігелла, Н. Карпчук, А. Шуляк і Н. Шуляка, присвячених проблемам інформаційної безпеки. Психологічна дієвість спростувань та ризики ефекту «зворотного удару» досліджені у мета-аналізі М.-П. Чан. Також цінним джерелом для дослідження психологічних аспектів формування національної стійкості стало дослідження В. Бурдяк, що розкриває проблематику методів маніпулювання ЗМІ суспільною свідомістю та співвіднесення цих явищ. Проблематика «позитивного сторітелінгу» та протидії дезінформації щодо санкцій і енергетичного шантажу розкривається через аналітику Ж. Борреля та спеціалізовані роз’яснення Європейської Ради.

Для фундаментального розуміння масової комунікації у цифрову добу було опрацьовано статтю І. Макух-Федоркової. В статті науковиці ґрунтовно описано, яку важливу роль зіграли соціальні мережі у зміні традиційних механізмів комунікації, що спрощує шлях дезінформації до цільової аудиторії.

Фундаментом для аналізу правових засад формування стратегічних комунікацій стали висновки Європейської Ради (2015), які зафіксували політичну волю щодо створення спеціалізованих структур протидії дезінформації. Стратегічне планування та подальша інституціоналізація сфери простежуються через Плани дій ЄС та резолюції Європейського Парламенту. Важливим у контексті предметного поля нашого дослідження є План дій з європейської демократії (2020), де стратегічні комунікації визначені критичним елементом захисту демократичних процесів. Окрему групу нормативних джерел складають роз’яснення щодо посилення комунікаційних зусиль ЄС як відповіді на російську пропаганду.

Критичний погляд на фінансове забезпечення та фрагментарність зусиль ЄС представлено у звітах Європейського суду аудиторів та бюджетних звітах Європарламенту. Порівняльний аналіз фінансування російської пропаганди

наведено у розвідках «Репортерів без кордонів». Загальний рівень інформаційної резильєнтності в регіональному розрізі верифіковано за даними Disinformation Resilience Index 2024. Окремі виклики сучасної дипломатії, зокрема у контексті заяв Д. Трампа, розглянуто за актуальними медіа-матеріалами та спростуваннями ЦПД.

Джерельне забезпечення системи цифрових безпекових інструментів протидії дезінформації нами структуровано за наступними векторами: феноменологія цифрових впливів, нормативне регулювання новітніх цифрових технологій (ШІ, цифрові послуги) та прикладні технологічні рішення на наднаціональному і національному рівнях.

Розуміння сутності сучасних дезінформаційних загроз базується на концепції «обчислювальної пропаганди», розкритій у працях С. Вуллі та П. Говард. Механізми функціонування бот-мереж та їх роль у маніпулюванні трендами детально досліджено у звітах DFRLab, NATO StratCom COE та наукових розвідках Е. Феррара. Психологічний вимір цифрових операцій та особливості використання психографічного профілювання аналізуються у роботах В. Бакір. Окрему увагу приділено загрозам «синтетичної» дезінформації, зокрема діпфейкам, на основі аналізу кейсу з дискредитацією керівництва України, а також теоретичних напрацювань Р. Чесні та Д. Сітрон.

Щодо нормативно-правового регулювання, центральне місце у цій групі джерел займає Акт про штучний інтелект (AI Act), що оперує ризик-орієнтованим підходом та означує вимоги до маркування контенту. Процеси імплементації цих норм та їх вплив на нормотворчість в ЄС досліджено у працях Дж. Баєр та М. Маккарті. Регуляторну роль Акту про цифрові послуги (DSA) у забезпеченні алгоритмічної прозорості та протидії шкідливому контенту висвітлено у документах Єврокомісії та спеціалізованих дослідженнях. Досвід національного впровадження та узгодження цих стандартів, зокрема в Ірландії, аналізується через діяльність Coimisiún na Meán та відповідне законодавство.

Технологічне наповнення політики інформаційної безпеки ЄС простежується через грантові програми Horizon Europe. Діяльність консорціумів

VERA.ai та AI4TRUST демонструє перехід до використання мультимодального аналізу та «гібридного інтелекту» для виявлення дезінформації. Безпековий потенціал технологій розподіленого реєстру (Blockchain, KSI) у захисті державних даних висвітлено на прикладі естонського досвіду та її співпраці з ЄС і НАТО. Вітчизняну практику імплементації цих рішень проаналізовано через розвиток системи «Трембіта».

ЄС, як наднаціональна структура діє також і через зусилля окремих країн-членів. Специфіку державно-центричного підходу Франції досліджено через мандат служби VIGINUM та викриття мережі «Portal Komba. Гібридну модель Литви досліджено через архітектуру платформи Debunk.org та її синергію з волонтерськими спільнотами. Український сегмент джерел фокусується на деконструкції мереж анонімних Telegram-каналів як інструменту гібридної агресії. Роль інформаційної гігієни в умовах глобальних викликів узагальнено в монографії Н. Шуляк і А. Шуляк, а загальна рамка мережевої оборони – у звітах EEAS та працях Дж. Паммента.

Використані для дослідження створення онлайн-екосистеми як перспективного інструменту політики протидії дезінформації нами структуровано в межах наступних напрямів: теоретико-методологічні засади екосистемного підходу, нормативно-правове регулювання онлайн-екосистеми в ЄС, національні моделі (Франція, Естонія) та прикладний досвід побудови цифрової стійкості в Україні.

Розуміння екосистеми як складного техно-економічного простору базується на працях П. К. Сеньйо, К. Лю та Дж. Еффаха, які розробили рамку цифрових бізнес-екосистем. Доповіді McKinsey & Company та дослідження стратегії Apple надали базу для розуміння мережевих ефектів та моделі «замкненого саду», що сьогодні трансформуються у безпекові цифрові мережі. Питання економічних і політичних аспектів функціонування платформ, а також їх роль у цифровій трансформації розглядаються крізь призму напрацювань Спільного дослідницького центру (JRC) Єврокомісії у працях Е. Гомес-Еррери та Б. Мартенса.

Важливим джерелом аналізу фіксації переходу від саморегулювання платформ до жорсткого правового контролю є Акт про цифрові послуги (DSA), який запровадив вимоги алгоритмічної прозорості та інститут «довірених скаржників». Процес формування етичних та юридичних зобов'язань простежено через Посилений кодекс практики щодо дезінформації та рішення Єврокомісії 2025 року про його інтеграцію в правове поле. Емпіричним підтвердженням дієвості цих механізмів виступають звіти Центру прозорості та публікації технологічних гігантів, зокрема TikTok. Аналіз діяльності EDMO та її регіональних хабів (зокрема BENEDMO) здійснено через їхні координаційні функції та звіти щодо захисту демократичних виборів.

Національні архітектури інформаційної безпеки та європейські стандарти розглянуто на прикладі окремих кейсів. Французький сегмент екосистеми представлений аналізом профільного законодавства 2018 року та декретів про створення служби VIGINUM та супер-регулятора Arcom. Дослідження Ж.-Б. Жанжена Вільмера (CAPS/IRSEM) та діяльність AFP Factuel демонструють синергію між державою та незалежним медіасередовищем у протидії маніпуляціям. Естонський досвід цифрової стійкості досліджено через стратегію «Цифрове суспільство 2030», систему X-Road та концепцію Data Embassies, відображені у наукових розробках А. Кітта і М. Магі. Вплив лобіювання Big Tech на формування цих правил розглянуто у працях Л. Боуза Гарсія та А. Олеарт.

Український вимір відображає унікальний досвід побудови «держави у смартфоні» як інструменту стійкості, що підтверджується звітами ОЕСР та аналітикою Hybrid CoE. Роль Міністерства цифрової трансформації, застосунку «Дія» та воєнних чат-ботів («єВорог») аналізується як приклад прямої цифрової взаємодії держави та громадянина. Специфіку використання мобільних застосунків (зокрема «Повітряна тривога») для оперативного інформування та медіаграмотності висвітлено у наукових працях О. Кошелюк та Н. Благовірної. Критичним викликом для екосистеми визначено монополію Telegram, що досліджено через дані Internews щодо медіаспоживання українців у 2025 році та звіти DFRLab і NATO StratCom COE щодо зброєзації цієї платформи.

Для визначення особливостей формування системи засобів верифікації інформації як інструменту протидії дезінформації нами використано джерела, що фокусуються на теоретико-методологічних засадах дослідження «інформаційного розладу», нормативно-стратегічному регулюванні на рівні ЄС та України, а також технологічних й інституційних інструментах практичного фактчекінгу.

Аналіз інституційних засад верифікації в ЄС представлений у праці О. Звоздецької. Науковиця фокусується на діяльності структур StratCom та Системи швидкого оповіщення (RAS) як важливих елементів протидії гібридним впливам. Фундаментальне значення для розуміння природи сучасних інформаційних загроз має концепція «інформаційного розладу» (information disorder), розроблена К. Вордл та Х. Дерашханом. Автори пропонують відмовитися від спрощеного терміну «fake news» на користь трирівневої класифікації (місінформація, дизінформація, малінформація), що дозволяє диференціювати методи верифікації залежно від наміру заподіяти шкоду. В контексті національної безпеки ці розробки доповнюються монографією В. Горбуліна. Дослідник розглядає верифікацію як критичний компонент протидії у «п’ятому вимірі» гібридної війни. Методологічну глибину процесу перевірки забезпечують праці з інженерії систем, зокрема дуалістичний підхід Р. Прессмана, С. Андрьоля та настанови Global Harmonization Task Force щодо розмежування «верифікації» та «валідації», що дозволяє трактувати перевірку інформації як інструмент стратегічного управління ризиками. Розвиток європейської політики верифікації простежується через еволюцію стратегічних документів. Вихідною точкою інституціоналізації стали висновки Європейської Ради від березня 2015 р., які сформували основу для створення робочих груп StratCom. Подальша деталізація механізмів відображена у «Плані дій проти дезінформації» та Спільних рамках протидії гібридним загрозам. Важливим компонентом нашого дослідження є аналіз правового регулювання механізмів та інструментів протидії дезінформації на рівні держав-членів та країн-кандидатів, де концептуальні рамки дій ЄС уточнюються у звітах Н. Бентзен, J. Pamment та

аналітиці B. Immenkamp. Окрему увагу приділено концепції FIMI у документах Європейської служби зовнішніх справ та Ради ЄС. Український сегмент представлений профільним законодавством, зокрема Законом «Про верифікацію та моніторинг державних виплат» та постановами Кабінету Міністрів.

Окрему групу джерел становлять матеріали щодо технологічної спроможності верифікації. Праці К. Бончевої та П. Накова, а також дослідження А. Зубіаги фокусуються на ролі штучного інтелекту в автоматизації фактчекінгу. Практичний інструментарій описано в документації проєкту InVID/WeVerify, що став джерелом оновлення дискурсу протидії дезінформації. Діяльність флагманських інституцій, таких як EUvsDisinfo та EDMO, розглядається через призму встановлення єдиних стандартів та операційних процедур фактчекінгу в кризових ситуаціях. Додатково нами залучено розробки Bellingcat (Е. Гіггінс) та посібники з верифікації цифрового контенту К. Сільвермана.

Важливим джерелом для дослідження є Кодекс принципів Міжнародної мережі фактчекінгу (IFCN), що визначає етичні рамки діяльності верифікаторів. Регіональні особливості досліджуються на прикладі чеської платформи Demagog.cz, звітів CEDMO та наукових розвідок Н. Карпчук. Глобальні тренди та статистичні дані щодо розвитку політичного фактчекінгу містяться у дослідженнях L. Graves та звітах Duke Reporters' Lab (E. Ryan). Стан стійкості інформаційного простору до маніпуляцій у Центральній та Східній Європі, включаючи Україну, відображено у Disinformation Resilience Index, а практичні аспекти розслідувань висвітлено у науковій праці О. Гороховського.

В наукових розвідках присвячених медіаграмотності та медіаосвіті як компетентністним інструментам протидії дезінформації, означені категорії розглядаються не лише як освітні, а й як стратегічні елементи превентивної інформаційної безпеки. Наукові джерела, використані для аналізу цих проблем класифіковано наступним чином: офіційні документи ЄС, національні стратегії країн-членів, нормативно-правова база України, а також теоретичні розробки у сфері когнітивної психології та стратегічних комунікацій.

Першу групу джерел складають документи Європейського Союзу, які визначають нормативний каркас медіаосвіти. Пріоритетне місце посідає Директива про аудіовізуальні медіапослуги (AVMSD), яка закріплює юридичні зобов'язання держав-членів у цій сфері. Стратегічні орієнтири аналізуються через План дій з європейської демократії (2020) та План дій у галузі цифрової освіти (2021–2027), де медіаграмотність визначено фундаментом стійкості проти іноземних маніпуляцій. Загальні засади політики ЄС у цифрову епоху доповнюються офіційними роз'ясненнями щодо формування цифрового майбутнього Європи. Наукова праця В. Бурдяк пропонує обґрунтування політичної складової медіаграмотності як інструменту протидії дезінформації. Завдяки залученню системно-функціонального підходу та методів статистико-порівняльного моніторингу, авторка забезпечує високий рівень верифікації емпіричного матеріалу, що дозволяє чітко визначити політико-психологічні детермінанти когнітивної стійкості суспільства в сучасному інформаційному просторі.

Аналітичний складник базується на звітах EEAS (2025) та Європейської обсерваторії цифрових медіа (EDMO) за 2022–2025 рр., що дозволило простежити реакцію європейської спільноти на воєнну дезінформацію РФ. Емпіричне порівняння стійкості різних суспільств реалізовано через дані Media Literacy Index 2025, які фіксують рівень захищеності від епохи «постправди». Додатково залучено праці Д. Стельмаха щодо досвіду ЄС у протидії російським кампаніям.

Друга група сформована джерелами, що описують успішні кейси країн ЄС. Дослідження досвіду Фінляндії базується на політиці Національного аудіовізуального інституту (KAVI), а німецька модель аналізується через діяльність Федерального агентства громадянської освіти (bpb) та мережі Landesmedienanstalten. Фундаментальне значення для обґрунтування методу пребанкінгу мають праці Дж. Розенбека, С. ван дер Ліндена та Т. Нюгрена, які заклали основу «теорії інокуляції». Технологічний аспект реалізації цього

підходу висвітлено у практичних настановх Jigsaw та ігрових інструментах ВООЗ «Go Viral!».

Специфіку шведської моделі «психологічного захисту» та її радикальної прозорості досліджено на основі наукових праць Н. Карпчук, Н. Піпченко та офіційних платформ Агентства психологічного захисту Швеції. Роль медіаінститутів у підтримці демократії аналізується на прикладі Fojo Media Institute. Питання суспільної стійкості та переосмислення українського досвіду для європейського контексту розглянуто крізь призму розвідок О. Луцевич (Chatham House) та критичного аналізу природи терміну «fake news», представленого у працях Е. Тандока.

Окрему групу складають нормативні та стратегічні документи України. Автором аналізував концепцію «Нової української школи» (НУШ) та меморандуми між МОН та IREX щодо інтеграції медіаграмотності в освітній процес. Практична імплементація неформальної освіти вивчалася через державні проєкти «Фільтр» (МКІП), платформу «Дія.Освіта» та спільні ініціативи Google, Jigsaw і Центру протидії дезінформації.

Вивчення ролі інститутів громадянського суспільства у реалізації європейської політики протидії дезінформації, дозволило визначити суб'єктність недержавного сектору як чинника формування суспільної стійкості. Залучені джерела класифіковано за тематичними блоками: теоретичні засади гібридного протистояння, досвід країн Балтії та Центральної Європи, мережеві ініціативи цифрового спротиву та діяльність провідних українських неурядових організацій.

У працях В. Горбуліна розуміння ролі громадянського суспільства базується на концептуалізації гібридних загроз, а інформаційне протистояння розглядається як «п'ятий вимір» війни. Глобальний контекст еволюції воєнних конфліктів та специфіка російських стратегій висвітлені у розвідках M. Galeotti та F. Hoffman, що дозволяє локалізувати місце дезінформації у загальній архітектурі гібридної агресії.

Окрему групу джерел складають матеріали, присвячені аналізу балтійської моделі стійкості (Baltic way of resilience). Дослідження ICDS, CEPA та звіти міністерств оборони Литви і Латвії демонструють синергію між державними структурами та громадськими ініціативами у сфері кіберзахисту й стратегічних комунікацій. Рівень готовності інфраструктури та відповідність стандартам НАТО верифіковано за даними Міжнародного індексу кібербезпеки та працями Є. Гарькавого.

Особливий сегмент джерельного забезпечення дослідження складає науковий та експертно-аналітичний доробок, у межах якого висвітлено особливості самоорганізації громадян у цифровому середовищі. Аналітика NATO StratCom COE та розвідки B. Kartous розкриває діяльність литовських та чеських «ельфів» як відповідь на активність інтернет-тролів. Трансформація локальних рухів у глобальні спільноти, зокрема роль руху NAFO, підтверджена офіційними заявами оборонних відомств, що свідчить про визнання ефективності гумору та сатири як інструментів контрпропаганди.

Процеси інтеграції систем протидії дезінформації простежуються через міждержавні декларації та програми співпраці. Аналіз 27 кейсів країн ЄС від EDMO доповнюється звітами про естонсько-українську програму «Стійка Україна» та домовленості про спільний інформаційний захист між Україною та державами-членами ЄС. Нормативні обмеження щодо пропагандистських ресурсів, зокрема досвід Латвії, демонструють правовий вимір захисту публічної сфери.

Окрема група джерел детально описує інституціоналізацію українського досвіду. Діяльність ГО «Детектор медіа» та проєкту MediaSapiens аналізується через дослідження інформаційного споживання та впливу пропаганди. Роль фактчекінгових платформ представлено з допомогою аналізу стратегії StopFake, VoxCheck та інноваційних розробок Ґвара Медіа. Сучасний етап державно-громадського партнерства верифіковано через меморандуми про співпрацю між Центром протидії дезінформації при РНБО та аналітичними центрами, а також спільні ініціативи з Google та Jigsaw.

Здійснений аналіз джерельної бази дослідження вказує на те, що сучасна політична наука сформувала комплекс наукових досліджень, які можуть бути використані для предметного вивчення сукупності та функціональності механізмів та інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни, який одночасно забезпечений релевантним набором нормативно-правових та веріфікованих даних.

Висновки до розділу 1

Методологічний потенціал неоінституціоналізму в дослідженні інструментів та механізмів протидії дезінформації полягає в тому, що політичні інститути регулюючи формальні процеси, формують культурні норми, когнітивні рамки та очікування, які впливають на сприйняття інформаційних загроз. Використання неоінституціонального підходу дозволяє: по-перше, зрозуміти, чому одні держави демонструють високий рівень стійкості до дезінформаційних атак, тоді як інші залишаються вразливими; по-друге, аналізувати взаємозв'язок між інституційною довірою, легітимністю політичних рішень та здатністю суспільства мобілізувати ресурси для протидії маніпуляціям; по-третє, оцінювати ефективність формальних механізмів протидії та неформальних практик спротиву дезінформації, які закріплюються у суспільстві та впливають на його стійкість в умовах гібридної війни.

Механізм протидії дезінформації у методології неоінституціоналізму можна визначити як комплекс інституційних практик, правил та структур, що забезпечують легітимність, стійкість і результативність політичних інститутів у динамічному інформаційному середовищі. У його змісті поєднуються три ключові виміри: історичний, який пояснює формування та трансформацію інституційних рамок у довготривалій перспективі; раціонально-вибірковий, що розглядає протидію дезінформації як систему стимулів і санкцій, які спрямовують поведінку акторів у межах встановлених правил; та соціологічний, який акцентує на когнітивних, нормативних і регулятивних структурах, що формують легітимність і забезпечують довіру суспільства до колективних

рішень. Узагальнено, механізм протидії дезінформації у неоінституціоналізмі постає як інституційно зумовлений процес агрегування соціальних інтересів, вироблення норм і практик достовірної комунікації та створення умов для ефективної самоорганізації суспільних структур у боротьбі з інформаційними загрозами.

Застосування методології неофункціоналізму дозволяє досліджувати, як політика протидії дезінформації може зміцнювати інституційну довіру, сприяти соціальній згуртованості та формувати нові стандарти взаємодії між державою, громадянським суспільством і медіа. Неофункціоналізм також допомагає пояснити, чому боротьба з дезінформацією не може бути ізольованим завданням, а потребує комплексної інтеграції з іншими політиками, зокрема безпековою та інформаційно-комунікаційною. Використання методологічних принципів неофункціоналізму в дослідженні політики протидії дезінформації дозволяє визначати здатність суспільства створювати взаємопов'язані механізми, які посилюють одне одного, формуючи стійку систему захисту від інформаційних загроз.

Використання концепту стійкості у теоретичному вимірі дозволить проаналізувати політику протидії дезінформації в ЄС як процес балансування між свободою слова та безпекою демократичних інститутів. В сучасній політичній науці він є універсальною дослідницькою рамкою, що поєднує адаптивність соціальних систем із їхньою здатністю зберігати функціональність в умовах постійних інформаційних загроз. Ідея стійкості дозволить визначвти здатність політичних інститутів і суспільних структур трансформуватися, інтегрувати нові практики та водночас відновлювати легітимність. Теоретичне застосування концепту стійкості у дослідженні дезінформації дозволяє пояснити, чому загрози, згенеровані дезінформацією є не зовнішнім явищем до політичного поля ЄС, а постають системним викликом для європейської демократії, що потребує комплексної відповіді.

РОЗДІЛ 2
СТРУКТУРА МЕХАНІЗМУ ЄВРОПЕЙСЬКОЇ ПОЛІТИКИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

2.1. Основні принципи політики протидії дезінформації в Європейському Союзі

Формування принципів політики протидії дезінформації в ЄС набуло системності після 2014 р., коли тимчасова окупація Російською Федерацією Автономної Республіки Крим та частини Донецької і Луганської областей, виразно продемонструвала, що інформаційні операції можуть бути використані як складова стратегії «гострої сили» в системі інструментів гібридної війни [235]. Саме тоді стало очевидним, що дезінформація перестає бути лише інструментом пропаганди і перетворюється на технологію стратегічного впливу, здатну змінювати політичні реалії.

Важливим маркером цього зсуву стала позиція, озвучена російським генералом В. Герасимовим у 2013 р., коли він наголошував на зростанні ролі невійськових засобів у досягненні політичних цілей [44, с. 115]. Ця позиція, пізніше опублікована у військовому журналі, фактично заклала підґрунтя для доктрини, яка інтегрувала інформаційні інструменти у військово-політичну стратегію Росії та стало відображенням переходу держави-агресора від класичних форм «жорсткої сили» до комбінованих методів, коли інформаційні кампанії стають не менш ефективними за військові дії. Координація цих процесів Федеральною службою безпеки свідчила про інституціоналізацію інформаційної війни як окремого напряму державної неоімперської політики Росії. Б. Німмо описав російську дезінформаційну стратегію через категорії «4Ds»: deny, distort, diminish, distract [80], що вказує на системність і багатовимірність інформаційних операцій як засобу ведення гібридної війни. На нашу думку, ця дослідницька позиція стала важливим інтелектуальним ресурсом для європейських інституцій, адже дозволила зрозуміти логіку дезінформаційних кампаній і розробити механізми їх нейтралізації.

Таким чином, політика ЄС у сфері протидії дезінформації постала як відповідь на нову форму гібридної загрози, в якій інформація використовується як зброя, а боротьба з нею потребує вироблення правових і регуляторних інструментів, глибокого розуміння когнітивних та інституційних механізмів впливу. Разом з цим, перед ЄС постала необхідність виробити власну відповідь, яка б поєднувала захист демократичних інституцій із технологічними інструментами протидії дезінформації. Поступово дезінформація почала сприйматися як загроза безпеці ЄС, і саме тому була офіційно закріплена в політичних документах як різновид «гібридної загрози». Вперше це визначення прозвучало у Висновках Європейської Ради 2015 р., а вже наступного року Європейська Комісія у своєму Повідомленні деталізувала: «Масові кампанії з дезінформації, використання соціальних мереж для контролю політичного наративу або радикалізації, вербування та спрямування проксі-акторів можуть бути засобами для гібридних загроз. (...) Ініціатори гібридних загроз можуть систематично поширювати дезінформацію, в тому числі через цільові кампанії в соціальних мережах, тим самим прагнучи радикалізувати людей, дестабілізувати суспільство та контролювати політичний наратив» [167]. Наголошувалося, що поширення дезінформації може систематично підривати довіру до демократичних інститутів, дестабілізувати суспільство та змінювати політичний наратив. Включення дезінформації до категорії «гібридних загроз» означало визнання її як інструменту зовнішнього впливу на політичне поле ЄС та формування нової безпекової парадигми. Відтоді інформаційний простір перестав розглядатися як нейтральне середовище і став ареною стратегічного протистояння. Європейські інституції почали усвідомлювати, що традиційні механізми оборони не здатні протидіяти інформаційним кампаніям, які діють через когнітивні та соціальні канали, тому політика ЄС у цій сфері одразу проєктувалася як поєднання правових, комунікаційних та освітніх інструментів, спрямованих на підвищення стійкості суспільства.

Політика ЄС у сфері протидії дезінформації ґрунтується на вихідному припущенні, що дезінформація як явище не має статусу незаконного, проте вона

здатна завдавати шкоди суспільним інтересам та є фактором небезпеки в умовах гібридної війни. Правове поле у визначенні дезінформації, як простір формування принципів протидії дезінформації, упродовж останніх десяти років зазнало активного розвитку. У Повідомленні Єврокомісії «Боротьба з дезінформацією в Інтернеті: європейський підхід» [130] від 26 квітня 2018 р. було представлено комплексний підхід, що включає реагування на серйозні загрози шляхом підтримки цифрових екосистем, заснованих на принципах прозорості; розширення можливостей громадян у протидії дезінформації; забезпечення захисту демократичних процесів, зокрема у сфері формування політик. У цьому документі також було визначено термін «дезінформація», що закріпив концептуальні рамки для подальшого розвитку європейської політики у цій сфері. Єврокомісія визначила дезінформацію як неправдиву або оманливу інформацію, яка створюється, поширюється та використовується з метою отримання економічної вигоди або навмисного введення громадськості в оману, і яка може завдати шкоди суспільству [130]. При цьому підкреслювалося, що дезінформація не охоплює вже незаконні форми висловлювань, такі як наклеп, мова ненависті чи підбурювання до насильства. У тексті наголошується, що дезінформація може бути законною з точки зору права, але водночас становити серйозну загрозу для демократичних процесів, громадського порядку та суспільних цінностей, що й обґрунтовує необхідність вироблення спеціальних політичних та регуляторних механізмів для протидії її поширенню.

Наприкінці цього ж, 2018 р. було ухвалено Спільний план дій проти дезінформації (Action Plan against Disinformation, APD) [268; 269], у якому визначено чотири базові принципи діяльності ЄС у сфері протидії деструктивному інформаційному впливу. Перший принцип стосувався посилення спроможності інституцій ЄС та держав-членів у виявленні, аналізі та реагуванні на деструктивні інформаційні впливи, що передбачало створення спеціалізованих структур та використання сучасних аналітичних інструментів. Другий принцип був спрямований на зміцнення співпраці з платформами соціальних медіа та цифровими сервісами, які відіграють ключову роль у

поширенні інформації, з метою забезпечення прозорості та відповідальності їхньої діяльності. Третій принцип передбачав розвиток механізмів інформування та підвищення медіаграмотності громадян, що мало сприяти формуванню критичного мислення та здатності розпізнавати неправдиву інформацію. Четвертий принцип був пов'язаний із посиленням координації між державами-членами ЄС та міжнародними партнерами для забезпечення узгодженості дій у сфері протидії дезінформації [269]. Документ також визначив необхідність мобілізації фінансових та організаційних ресурсів для реалізації цих завдань, а його ухвалення стало важливим етапом у формуванні європейської нормативної та політичної бази, спрямованої на захист демократичних процесів, внутрішньої стабільності та суспільних цінностей від негативних наслідків поширення дезінформації.

Цей документ заклав концептуальні засади для формування європейської політики у сфері боротьби з дезінформацією, окресливши ключові напрями дій, що мають забезпечити узгодженість між державами-членами та сприяти розвитку механізмів захисту демократичних процесів і суспільних інституцій від негативних наслідків поширення неправдивої та маніпулятивної інформації [57]. Його значення полягає у тому, що він уперше закріпив узгоджені принципи та інституційні механізми, які мають забезпечити комплексну відповідь на виклики, пов'язані з поширенням неправдивої та маніпулятивної інформації. Стратегічна важливість APD полягає також у тому, що він заклав основу для подальших нормативних і політичних ініціатив у формуванні європейської стратегії, яка поєднує захист демократичних процесів, забезпечення внутрішньої стабільності та підтримку суспільних цінностей у контексті глобальної цифрової трансформації.

У 2020 р. Єврокомісією було представлено План дій щодо європейської демократії (European Democracy Action Plan) [192], який мав на меті зміцнення стійкості демократичних інституцій та розширення можливостей демократії в межах ЄС. У цьому документі визначено комплекс заходів, спрямованих на посилення окремих політик ЄС, забезпечення умов для проведення вільних і

чесних виборів, підтримку незалежних медіа та протидію дезінформації. ЄС розглядав боротьбу з дезінформацією як один із ключових напрямів захисту демократії, що пояснює включення до Плану трьох основних шляхів реалізації політики протидії дезінформації. Перший напрям стосується забезпечення цілісності виборчих процесів та сприяння демократичній участі, що включає прозорість політичної реклами, регулювання діяльності політичних партій та механізми підвищення стійкості виборчих систем. Другий напрям спрямований на зміцнення свободи та плюралізму медіа, що передбачає заходи із захисту журналістів, протидію стратегічним судовим позовам проти участі громадськості (SLAPPs), а також підтримку незалежних медіа та розвиток стандартів журналістської діяльності. Третій напрям охоплює протидію дезінформації, що включає посилення спроможності ЄС та держав-членів у виявленні та реагуванні на деструктивні інформаційні впливи, запровадження додаткових зобов'язань та механізмів відповідальності для онлайн-платформ, а також розширення можливостей громадян для прийняття обґрунтованих рішень шляхом підвищення рівня медіаграмотності та критичного мислення [192]. Таким чином, документ окреслює три стратегічні шляхи реалізації політики: захист виборчої доброчесності, забезпечення свободи та стійкості медіа, а також системну протидію дезінформації як ключовому виклику для демократичних процесів у ЄС.

Кодекс практик протидії дезінформації у своїй першій редакції, ухваленій у жовтні 2018 р., став першим інструментом ЄС добровільного характеру, спрямованим на формування рамкових зобов'язань для цифрових платформ, рекламної індустрії та інших учасників інформаційного простору у сфері протидії поширенню неправдивої та маніпулятивної інформації. Документ було розроблено Єврокомісією у співпраці з ключовими технологічними компаніями та представниками рекламного сектору, що надало йому характеру багатосторонньої угоди [168]. Його стратегічне значення полягало у тому, що він заклав основу для подальшої інституціоналізації політики ЄС у сфері боротьби з

дезінформацією, визначивши набір добровільних, але політично зобов'язуючих принципів та практик.

У першій версії Кодексу було закріплено низку ключових положень. По-перше, він передбачав зобов'язання щодо забезпечення прозорості політичної реклами, включно з чіткою ідентифікацією замовників та джерел фінансування. По-друге, документ вимагав від платформ вживати заходів для обмеження монетизації дезінформації, зокрема через рекламні інструменти, що використовуються для поширення неправдивого контенту. По-третє, Кодекс містив положення про необхідність закриття доступу до інструментів поширення дезінформації для тих суб'єктів, які систематично порушують правила. По-четверте, він наголошував на важливості співпраці між платформами та незалежними фактчекінговими організаціями, а також на розвитку механізмів, що дозволяють користувачам отримувати достовірну інформацію та перевіряти джерела. По-п'яте, Кодекс передбачав регулярне звітування компаній про виконання взятих зобов'язань, що мало забезпечити певний рівень підзвітності перед Європейською Комісією [168].

Водночас перша редакція Кодексу мала низку обмежень. Його добровільний характер означав відсутність юридично зобов'язуючих санкцій у випадку невиконання положень, що знижувало ефективність інструменту. Крім того, звітність компаній була нерівномірною та часто недостатньо деталізованою, що ускладнювало оцінку реального впливу Кодексу на зменшення поширення дезінформації. Незважаючи на ці недоліки, документ став важливим етапом у формуванні європейської політики у сфері протидії дезінформації, оскільки він започаткував практику залучення приватних компаній до виконання суспільно значущих завдань у сфері інформаційної безпеки та демократичної стійкості.

Важливим елементом у цьому контексті стали результати аудиту ефективності, викладені у спеціальному звіті «Дезінформація, що впливає на ЄС: боротися, але не приборкати» [191], який був присвячений аналізу та оцінці діяльності ЄС у сфері протидії дезінформації, зокрема виконанню положень

Спільного плану дій проти дезінформації 2018 р. У звіті було сформульовано низку рекомендацій, спрямованих на вдосконалення заходів ЄС у цій сфері, що підкреслює стратегічне значення Плану дій щодо європейської демократії як інструменту для подальшого розвитку політики протидії дезінформації та забезпечення стійкості демократичних процесів у ЄС. Звіт підкреслив, що План дій був релевантним на момент ухвалення, однак є неповним і потребує вдосконалення. Серед ключових рекомендацій було зазначено необхідність створення чітких механізмів координації між Єврокомісією та Європейською службою зовнішніх дій, оскільки відсутність узгоджених процедур ускладнювала реалізацію заходів. Було наголошено на потребі розробки системного моніторингу та звітності, адже наявна фрагментарна система не забезпечувала належної підзвітності та прозорості. Окремо акцентувалося на проблемі недостатнього та короткострокового фінансування, що обмежувало можливості для довгострокового планування та стійкої реалізації політики [191].

Звіт також звернув увагу на стратегічні комунікаційні підрозділи, які відіграють важливу роль у протидії дезінформації, але залишаються недостатньо укомплектованими кадрами та ресурсами для реагування на нові загрози. Було рекомендовано посилити кадрове та фінансове забезпечення цих структур. Крім того, зазначалося, що Система швидкого оповіщення (Rapid Alert System), створена для координації між державами-членами, не реалізувала свій потенціал у повному обсязі, і тому потребує вдосконалення для забезпечення більш ефективного обміну інформацією та спільних дій. Окремо наголошувалося, що Кодекс практики ЄС щодо дезінформації, хоча й став важливим кроком, має обмежену ефективність через добровільний характер зобов’язань платформ. У звіті рекомендувалося посилити механізми контролю та відповідальності для цифрових платформ, щоб забезпечити реальне виконання взятих ними зобов’язань [371].

Таким чином, рекомендації звіту зводилися до необхідності: посилення координації між інституціями ЄС, створення системного моніторингу та звітності, забезпечення довгострокового фінансування, зміцнення кадрового та

ресурсного потенціалу стратегічних комунікаційних підрозділів, вдосконалення Системи швидкого оповіщення та посилення зобов'язань цифрових платформ. Ці рекомендації підкреслили стратегічне значення Плану дій щодо європейської демократії як інструменту для подальшого розвитку політики протидії дезінформації та забезпечення стійкості демократичних процесів у ЄС.

Результати звіту стимулювати до оновлення редакції Кодекс практик протидії дезінформації, яка була представлена у червні 2022 р. [382]. Цей документ мав стратегічне значення для принципів політики протидії дезінформації ЄС, оскільки перетворив попередній добровільний інструмент на більш комплексну систему співрегулювання, що передбачала чіткіші зобов'язання для цифрових платформ, рекламної індустрії та інших учасників інформаційного простору. Оновлений Кодекс було розроблено у тісній співпраці між Єврокомісією та понад тридцятьма підписантами, серед яких великі технологічні компанії, рекламні організації та представники громадянського суспільства.

У змістовному плані Посилений Кодекс практик протидії дезінформації закріпив низку нових положень, які значно розширили рамки попередньої редакції (Додаток Б). По-перше, було введено більш деталізовані зобов'язання щодо прозорості політичної реклами, включно з вимогою створення спеціальної бібліотеки політичних оголошень, доступної для громадськості. По-друге, документ передбачив посилені заходи для обмеження монетизації дезінформації, зокрема через суворіші правила для рекламних мереж та платформ, які повинні запобігати використанню їхніх сервісів для поширення неправдивого контенту. По-третє, Кодекс встановив вимогу до платформ щодо регулярного надання стандартизованих звітів про виконання зобов'язань, що дозволяє Єврокомісії здійснювати більш системний моніторинг та оцінку ефективності. По-четверте, було закріплено положення про необхідність співпраці з незалежними фактчекінговими організаціями та науковими інституціями, що має забезпечити більш високий рівень достовірності інформації та підвищити якість перевірки контенту. По-п'яте, документ передбачив створення механізмів для підтримки

користувачів у розпізнаванні дезінформації, включно з інструментами підвищення медіаграмотності та критичного мислення [382].

Важливою новацією стало запровадження чіткіших механізмів підзвітності, які передбачають можливість застосування санкцій у випадку невиконання взятих зобов'язань. Це означало, що оновлений Кодекс набув більшої ваги у правовому та політичному вимірах, наближаючись до моделі співрегулювання, в якій добровільні зобов'язання поєднуються з елементами контролю та відповідальності. Посилений Кодекс практик протидії дезінформації також врахував нові виклики, пов'язані з розвитком цифрових технологій, зокрема автоматизованих систем поширення контенту та алгоритмічних методів його посилення, що раніше залишалися поза увагою процесу вироблення політики протидії дезінформації [382].

Наступним кроком у формуванні принципів політики протидії дезінформації стало ухвалення Закону про цифрові послуги (Digital Services Act, DSA) 19 жовтня 2022 р. як фундаментального нормативного акту ЄС, що встановлює єдину правову рамку для цифрових послуг у межах внутрішнього ринку ЄС. Його стратегічне значення полягає у тому, що він замінив та оновив положення Директиви 2000/31/ЕС про електронну комерцію, створивши сучасну систему регулювання, яка відповідає викликам цифрової економіки та інформаційного суспільства. Документ визначив горизонтальні правила для постачальників посередницьких послуг, включно з онлайн-платформами, пошуковими системами та іншими цифровими сервісами, що діють на території ЄС, і встановив їхні обов'язки щодо управління контентом, прозорості та відповідальності перед користувачами. Його значення для політики протидії дезінформації буде проаналізоване нижче в контексті національних механізмів держав-членів ЄС.

Здійснений аналіз дозволяє визначити основні принципи політики протидії дезінформації в ЄС, що є основою для узгоджених дій інституцій ЄС, держав-членів та приватних суб'єктів у сфері інформаційної безпеки: перший принцип полягає у визнанні дезінформації як явища, що не завжди має ознаки

незаконності, але яке здатне завдавати шкоди суспільству, демократичним процесам та інституціям, що потребує спеціальних політичних і регуляторних заходів; другий принцип стосується забезпечення прозорості, зокрема у сфері політичної реклами та діяльності цифрових платформ, що має запобігати прихованому поширенню неправдивих повідомлень та маніпуляцій; третій принцип передбачає обмеження монетизації дезінформації, тобто створення умов, за яких економічна вигода від поширення неправдивого контенту стає неможливою, що мало зменшити стимули для його продукування; четвертий принцип полягає у розвитку співпраці між платформами, державними інституціями та незалежними фактчекінговими організаціями, що забезпечить багаторівневу перевірку достовірності інформації та підвищує її якість; п'ятий принцип спрямований на розширення можливостей громадян, зокрема через підвищення рівня медіаграмотності та розвиток критичного мислення, що дозволить суспільству самостійно розпізнавати неправдивий контент; шостий принцип стосується створення механізмів підзвітності та регулярного звітування цифрових платформ про виконання взятих зобов'язань, що забезпечує контроль з боку Єврокомісії та громадськості; сьомий принцип полягає у посиленні координації між державами-членами ЄС та міжнародними партнерами, що має забезпечити узгодженість дій у глобальному інформаційному просторі та підвищити ефективність протидії транснаціональним кампаніям дезінформації.

Разом з тим, питання координації цих принципів з принципами політики протидії дезінформації, що реалізується в державах-членах ЄС, європейська політика не узгоджує достатньою мірою. У серпні 2020 р. було проведено опитування національних регуляторних органів у сфері аудіовізуальних засобів у 27 державах-членах ЄС, яке мало на меті з'ясувати, чи існують у національних правових системах спеціальні положення, що визначають поняття дезінформації, або ж нормативні акти, які можуть бути застосовані до цього явища. На основі порівняльного правового аналізу та узагальнення результатів відповідей було здійснено дослідження законодавства 11 держав-членів ЄС, серед яких Австрія, Хорватія, Кіпр, Чехія, Франція, Греція, Угорщина, Литва, Мальта, Румунія та

Словаччина. Отримані дані засвідчили, що частина держав має нормативні положення, які прямо або опосередковано стосуються регулювання дезінформації, проте найбільш дискусійним аспектом у контексті забезпечення свободи вираження поглядів залишаються положення кримінального права, що передбачають можливість застосування покарання у вигляді позбавлення волі у випадку засудження за відповідними статтями [103].

Литва є єдиною державою-членом ЄС, яка у своєму законодавстві містить чітку заборону на дезінформацію та закріплює визначення цього терміну. Відповідно до статті 19 Закону «Про надання інформації громадськості» забороняється поширення дезінформації, а також інформації, що має наклепницький або образливий характер щодо особи, яка принижує її гідність і честь [103]. У законі наведено визначення дезінформації як умисного поширення неправдивої інформації, яке корелює з підходом Єврокомісії, оскільки включає три ключові елементи: неправдивість інформації, наявність наміру та заподіяння шкоди. Водночас воно обмежується шкодою, що завдається конкретній особі, і не охоплює суспільну шкоду, а також не містить положення про економічну вигоду, як це передбачено у визначенні ЄС. Крім того, акцент робиться на процесі поширення дезінформації, тоді як аспект її створення залишається поза межами правового регулювання.

Хоча Литва залишається єдиною державою-членом ЄС, яка у своєму законодавстві містить чітке визначення терміну «дезінформація» та закріплює його як окрему категорію, низка інших держав-членів ЄС мають нормативні положення, що фактично узгоджуються з європейським та академічним визначенням дезінформації, проте не використовують сам термін «дезінформація» у правових текстах. Найпоширенішими правовими інструментами, які застосовуються до цього явища, є положення кримінального законодавства, що регулюють питання «неправдивих новин» або «неправдивої інформації». Такі норми функціонують у правових системах Австрії, Хорватії, Кіпру, Чехії, Франції, Греції, Угорщини, Мальти, Румунії та Словаччини. Вони передбачають відповідальність за умисне поширення неправдивих відомостей,

що можуть завдати шкоди окремій особі, соціальній групі, організації чи державі, і, таким чином, виконують функцію правового регулювання дезінформаційних практик, навіть якщо термінологічно це не визначено як «дезінформація» [81, p. 130]. Ці дані узгоджуються з повідомленням Єврокомісії, оприлюдненим у період пандемії Covid-19 у 2020 р., де було зазначено, що окремі держави-члени ЄС мають положення кримінального законодавства, які застосовуються до явища дезінформації [176]. У цьому документі окремо була названа Угорщина, яка запровадила нову кримінальну норму щодо поширення дезінформації під час надзвичайного стану. Але в інших державах-членах ЄС існує значна кількість законів, які також регулюють питання дезінформації, хоча вони не завжди визначають її як окрему категорію. Ці нормативні акти можна класифікувати на кілька груп: положення кримінального та некримінального законодавства, що стосуються неправдивих новин або неправдивої інформації; спеціальні закони, ухвалені у період пандемії Covid-19 для протидії поширенню неправдивих відомостей; а також законодавчі акти, спрямовані на запобігання поширенню неправдивих новин та неправдивої інформації у виборчий період. Така класифікація дозволяє простежити різні підходи до правового регулювання дезінформації в межах ЄС та оцінити їхній вплив на баланс між забезпеченням інформаційної безпеки та дотриманням принципів свободи вираження поглядів як основних принципів протидії дезінформації.

До групи кримінального регулювання дезінформації належить Мальта, в якій ст. 82 Кримінального кодексу встановлює кримінальну відповідальність за поширення неправдивих новин, визначаючи злочином «зловмисне розповсюдження неправдивих новин, які можуть викликати занепокоєння громадської думки, порушити громадський порядок чи громадський спокій або спричинити заворушення серед населення чи окремих соціальних груп» [138]. Санкція за таке діяння може передбачати до трьох місяців позбавлення волі. Це положення узгоджується з концептуальним визначенням дезінформації, оскільки включає три ключові елементи: наявність неправдивої інформації, умисний характер дії та заподіяння шкоди, що може проявлятися у впливі на

громадську думку чи порушенні суспільного порядку. Водночас воно лише частково співвідноситься з визначенням дезінформації, запропонованим Єврокомісією, де йдеться про неправдиву або оманливу інформацію, створену, представлену та поширену з метою отримання економічної вигоди чи навмисного введення громадськості в оману, яка може завдати шкоди суспільству. У мальтійському законодавстві відсутній елемент економічної вигоди, проте акцент робиться на умисному поширенні неправдивих відомостей та їхньому потенційному впливі на соціальну стабільність.

У Франції стаття 27 «Закону про свободу преси», хоча й не належить до кримінального законодавства, забороняє поширення неправдивих новин, приписуваних третім особам, якщо вони створені недобросовісно та призводять до порушення громадського порядку або можуть його порушити, і передбачає можливість накладення штрафу у розмірі 45 000 євро [284]. Це положення відповідає визначенню дезінформації, оскільки включає неправдивість інформації, наявність наміру та заподіяння шкоди у вигляді порушення громадського порядку. У Хорватії «Закон про правопорушення проти громадського порядку та спокою» визначає поширення неправдивих новин як правопорушення, що порушує мир і спокій громадян, і передбачає можливість 30-денного ув'язнення [387, p. 24]. У Греції стаття 191 Кримінального кодексу містить положення, яке криміналізує поширення неправдивих новин, що викликають страх у невизначеної кількості осіб або певних груп, змушуючи їх здійснювати незаплановані дії чи відмовлятися від них, що може завдати шкоди економіці, туризму, обороноздатності або міжнародним відносинам країни [141]. Це положення акцентує увагу на конкретних діях, які є наслідком поширення неправдивих відомостей, а не лише на впливі на переконання чи думки. У Словацькій Республіці стаття 361 Кримінального кодексу передбачає кримінальну відповідальність за умисне створення небезпеки серйозного занепокоєння серед населення певної території шляхом поширення неправдивих тривожних новин, що може призвести до дворічного позбавлення волі [143]. У Чеській Республіці стаття 357 Кримінального кодексу також встановлює

кримінальну відповідальність за умисне спричинення загрози серйозного занепокоєння серед населення шляхом поширення тривожних новин, які не відповідають дійсності, і передбачає можливість дворічного ув'язнення [140]. На Кіпрі стаття 50 Кримінального кодексу визначає злочином поширення неправдивих новин або відомостей, які можуть завдати шкоди громадському порядку чи довірі суспільства до держави та її органів, викликати страх чи занепокоєння серед населення або будь-яким чином порушити цивільний мир і порядок, і передбачає покарання у вигляді двох років позбавлення волі.

З точки зору законодавчих актів щодо дезінформації, ухвалених в державах-членах ЄС у період пандемії Covid-19, найбільш дискусійним прикладом є законодавство Угорщини. Відповідно до спеціальних положень, внесених до розділу 337(2) Кримінального кодексу, що регулює питання «розпалювання страху», було встановлено, що оприлюднення заяви, яка завідомо є неправдивою або поширюється з необережним ігноруванням її достовірності чи хибності під час особливого правового режиму з наміром перешкодити або знизити ефективність захисних заходів, кваліфікується як тяжкий злочин і карається позбавленням волі на строк від одного до п'яти років [142]. Це положення передбачає наявність трьох ключових елементів: неправдивої інформації, умисного характеру дії та конкретної шкоди, пов'язаної із заходами протидії Covid-19. Крім того, стаття 338 Кримінального кодексу Угорщини встановлює кримінальну відповідальність за поширення будь-якого неправдивого факту, який може порушити громадський спокій, і передбачає можливе покарання у вигляді позбавлення волі строком до трьох років [142]. У Румунії президентський указ 2020 р. надав регулятору комунікацій повноваження вимагати видалення онлайн-контенту, що поширює неправдиві новини про Covid-19 та заходи профілактики, передбачені у відповідних нормативних актах [341]. Таким чином, приклади Угорщини та Румунії демонструють різні підходи до правового регулювання дезінформації у кризових умовах, де акцент робиться як на кримінально-правових санкціях, так і на адміністративних механізмах контролю за поширенням неправдивих відомостей.

До окремої групи нормативного регулювання дезінформації в державах-членах ЄС правові норми, що стосуються неправдивої інформації у виборчому процесі, які також відповідають визначенню дезінформації. Найбільш показовим прикладом є Франція, де відповідно до закону 2018 року про боротьбу з маніпулюванням інформацією передбачено, що протягом тримісячного періоду до виборів суддя має право ухвалювати будь-які пропорційні та необхідні заходи для припинення поширення «будь-якої інформації, твердження або звинувачення, що є недостовірним або вводить в оману, яке може вплинути на щирість майбутнього голосування та яке поширюється навмисно, штучно або автоматизовано та масово через публічну онлайн-службу комунікації» [94]. Це положення передбачає наявність трьох ключових елементів: умисного характеру дії («навмисно»), неправдивої інформації («неточний або оманливий факт») та потенційної шкоди («факт, що може змінити щирість майбутнього голосування»), а також додатково визначає спосіб поширення: штучний, автоматизований та масовий. Таким чином, воно обмежується потенційною шкодою для виборчого процесу, не охоплюючи інші аспекти, такі як громадський порядок чи суспільна шкода чи безпека. Визначення також звужене до конкретного методу поширення, що відрізняє його від більш загальних положень. Крім того, в Австрії Кримінальний кодекс містить норму, яка визначає злочином поширення неправдивих новин у період виборів, якщо вони можуть вплинути на виборців [139]. Таким чином, приклади Франції та Австрії демонструють різні підходи до правового регулювання дезінформації у виборчому контексті, де акцент робиться на забезпеченні достовірності та прозорості виборчого процесу.

На підставі проведеного аналізу можна сформулювати низку узагальнень щодо визначень дезінформації у правових системах держав-членів ЄС. По-перше, у більшості випадків простежуються три базові елементи, які повторюються у різних формулюваннях: наявність неправдивої інформації, її поширення з конкретним наміром, що має зловмисний або недобросовісний характер, та заподіяння певної шкоди. Водночас, хоча ці елементи є спільними,

деталі визначень істотно відрізняються, зокрема щодо того, чи шкода полягає у зміні поведінки, чи у використанні специфічних методів поширення. У різних країнах згадуються різні види шкоди: економічна шкода, шкода громадському порядку, шкода окремій особі, шкода гідності, шкода виборчому процесу або шкода заходам охорони здоров'я, як у випадку з регулюванням, пов'язаним із Covid-19. Значна частина визначень акцентує увагу на акті комунікації з громадськістю, а не лише на дії творця контенту. У деяких випадках, як у Франції, додатковим елементом є спосіб поширення неправдивої інформації, який має бути штучним, автоматизованим та здійснюватися у великих масштабах. Таким чином, визначення дезінформації у законодавстві держав-членів ЄС демонструють як спільні риси, так і суттєві відмінності, що відображають різні підходи до правового регулювання цього явища.

Зважаючи на те, що основним принципом правового регулювання дезінформації в ЄС є принцип дотримання прав і свобод людини, визначимо, наскільки цей принцип дотримується в правовому регулюванні дезінформації в державах-членах ЄС. Насамперед, питання стосується співвідношення національного законодавства, яким регулюється дезінформація, європейському принципу права на свободу вираження поглядів, гарантованого європейським законодавством про основні права [131] та міжнародним правом у сфері прав людини [258]. Європейська комісія у своєму повідомленні наголосила, що кримінальні положення щодо дезінформації, ухвалені під час пандемії Covid-19 і спрямовані на визначення злочинів, пов'язаних із дезінформацією, можуть спричинити явище самообмеження у висловлюваннях та викликати особливе занепокоєння щодо дотримання свободи вираження поглядів [176]. У цьому контексті міжнародне право прав людини чітко визначає, що подібні закони не узгоджуються з принципами свободи вираження поглядів. Чотири міжнародні спеціальні мандати у сфері свободи вираження поглядів заявили, що законодавчі акти, які містять заборону на поширення «неправдивих новин» і мають розпливчастий та двозначний характер, є несумісними з міжнародними стандартами свободи вираження та повинні бути скасовані [132]. Спеціальний

доповідач ООН з питань свободи вираження поглядів підкреслив, що концепція дезінформації є надзвичайно складною для точного визначення у правових актах і створює ризик надання органам виконавчої влади надмірних дискреційних повноважень у визначенні того, що є дезінформацією, а що є помилкою, та у встановленні критеріїв істинності [132]. Таким чином, покарання за дезінформацію визнається непропорційним відповідно до міжнародного права прав людини. Крім того, Комітет ООН з прав людини у своєму рішенні зазначив, що кримінальне переслідування за «злочин публікації неправдивих новин» лише на підставі того, що новини були неправдивими, становить явне порушення права на свободу вираження поглядів [253].

Подібна позиція простежується і в практиці європейського права у сфері прав людини щодо законодавчих положень, які стосуються недостовірної інформації. Європейський суд з прав людини у справі «Салов проти України» (2005) одноголосно постановив, що переслідування за «розповсюдження неправдивої інформації» відповідно до виборчого законодавства України порушує право на свободу вираження поглядів, гарантоване статтею 10 ЄКПЛ. Суд наголосив, що стаття 10 ЄКПЛ «як така не забороняє обговорення або поширення отриманої інформації, навіть якщо існують серйозні підозри щодо її неправдивості» [387, p. 26]. У подібному форматі Суд виніс три одностайні рішення щодо положень виборчого законодавства Польщі, які дозволяли кандидатам звертатися до суду з вимогою заборонити публікацію агітаційних матеріалів або заяв, що містять «неправдиві дані чи інформацію», причому суд мав розглянути такі заяви протягом 24 годин [387, p. 30]. У всіх цих випадках Суд визнав, що застосування відповідних положень порушує статтю 10 ЄКПЛ, оскільки національні суди «негайно кваліфікували заяви як неправдиві», зроблені місцевим політиком під час виборів, або беззастережно кваліфікували всі заяви як такі, що не мають фактичної основи», і таким чином фактично позбавили його захисту, гарантованого статтею 10. У світлі наведених рішень можна констатувати наявність суттєвих проблем щодо відповідності положень

національного законодавства, які застосовуються до дезінформації, європейським принципам стандартам свободи вираження поглядів.

Різні національні підходи до правового регулювання дезінформації можна розглядати як складову ширшої тенденції на рівні держав-членів ЄС щодо ухвалення нормативних актів, які стосуються впливу цифрових платформ соціальних медіа на функціонування національних медіа-систем та демократичні процеси [360]. У відповідь на появу та розмаїття таких національних підходів наприкінці 2020 р. Був ухвалений DSA [177], який запровадив комплекс нових уніфікованих правил для цифрових платформ і підлягав прямому застосуванню в усіх 27 державах-членах ЄС. Однією з ключових цілей DSA є гармонізація різних національних підходів до регулювання, що пояснює вибір Єврокомісією саме Регламенту як форми правового акту, а не Директиви.

Важливим аспектом DSA є центральне поняття «незаконний контент», яке у статті 2 визначено як «будь-яку інформацію, яка сама по собі або через посилання на діяльність, включаючи продаж продуктів чи надання послуг, не відповідає законодавству ЄС або законодавству держави-члена, незалежно від конкретного предмета чи характеру цього закону» [177]. Це визначення охоплює всі випадки дезінформації, які були закріплені у національних правових актах, розглянутих вище. Посилання на національне законодавство означає, що DSA фактично інтегрує різні національні підходи, які концептуалізують дезінформацію як «незаконний контент», у загальноєвропейську систему регулювання. З точки зору функціонування внутрішнього ринку можна передбачити, що DSA не усуне наявні відмінності між державами-членами, а навпаки може посилити їх, оскільки національні правові системи залишаються ключовим орієнтиром для визначення того, що вважатиметься «незаконним контентом» у межах європейського правового простору.

У DSA міститься низка положень, які потенційно можуть бути застосовані до явища дезінформації. Зокрема, стаття 26 встановлює вимогу для «дуже великих онлайн-платформ» (VLOP) здійснювати оцінку ризиків, пов’язаних із «значними системними ризиками», що виникають у процесі функціонування

їхніх сервісів. До таких ризиків віднесено «навмисне маніпулювання їхніми послугами» шляхом «неавтентичного використання або автоматизованого використання сервісу, яке має фактичний або передбачуваний негативний вплив на захист здоров'я населення, неповнолітніх, громадський дискурс, а також фактичний або передбачуваний вплив, що стосується виборчих процесів та громадської безпеки» [177]. Елементи цієї норми положення відображають ключові характеристики визначення дезінформації, характерні для держав-членів ЄС та інтегрованих до опосередкованого нормативного регулювання дезінформації в ЄС. У статті 57 DSA наведено додаткові приклади навмисного маніпулювання сервісами платформи, серед яких «створення підроблених облікових записів, використання ботів та інші автоматизовані або частково автоматизовані дії, що можуть призвести до швидкого та широкого поширення інформації, яка є незаконним контентом або суперечить положенням та умовам онлайн-платформи» [177]. Таким чином, концепція «навмисної маніпуляції», закріплена у DSA, додає новий вимір до розуміння дезінформації, оскільки охоплює не лише змістовний аспект неправдивої інформації, але й форму її поширення, що здійснюється через неавтентичне або автоматизоване використання цифрових платформ.

Згідно зі статтею 35 DSA, Єврокомісія разом із консультативною структурою Європейською радою з цифрових послуг сприятимуть розробленню кодексів поведінки, спрямованих на усунення «системних» ризиків. У пояснювальних положеннях DSA зазначено, що до таких ризиків можуть належати явища дезінформації, а також маніпулятивні та образливі практики, включаючи «скоординовані операції, спрямовані на поширення інформації, зокрема дезінформації, наприклад використання ботів або підроблених облікових записів для створення неправдивої чи оманливої інформації, іноді з метою отримання економічної вигоди, яка є особливо шкідливою для вразливих користувачів» [177]. Передбачено, що кодекси поведінки включатимуть обов'язок застосування конкретних заходів зі зменшення ризиків і підлягатимуть регулярному моніторингу та оцінці з боку Єврокомісії та Європейської Ради. У

декларативних положеннях також зазначено, що кодекси поведінки відповідно до статті 35 DSA можуть слугувати основою для вже існуючих механізмів саморегулювання, зокрема для Кодексу поведінки ЄС щодо дезінформації [177]. Таким чином, хоча у DSA прямо не подано визначення дезінформації, нові положення щодо системних ризиків та кодексів поведінки фактично охоплюють її як явище, що підлягає регулюванню. Водночас, у DSA містяться два додаткові положення, які потенційно можуть суттєво змінити політику ЄС у сфері протидії дезінформації.

По-перше, це стаття 8 DSA, що встановлює чіткий правовий механізм для національних судових та адміністративних органів, які отримують право видавати накази онлайн-платформам «вживати заходів» щодо конкретного користувацького контенту, який кваліфікується як «незаконний контент» [177]. Відповідно до статті 8(2), платформи зобов'язані повідомляти національний орган «без зайвої затримки» про наслідки виконання наказу та про заходи, які були вжиті [177]. Важливо підкреслити, що поняття «незаконного контенту» у DSA має досить широке визначення, що охоплює всі національні положення держав-членів ЄС, які стосуються дезінформації, неправдивих новин та неправдивої інформації. Таким чином, стаття 8 DSA створює спільне правове поле ЄС та відповідний механізм, який дозволяє національним судовим та адміністративним органам видавати накази платформам щодо видалення контенту відповідно до національних норм, що регулюють дезінформацію. Це має значні наслідки для свободи вираження поглядів у цифровому середовищі, оскільки у випадках, коли особи переслідуються за національними законами за їхні онлайн-висловлювання, стаття 8 DSA фактично полегшує можливість національних органів влади вимагати від платформ видалення такого контенту. Як результат, платформи можуть бути інструменталізовані для реалізації національних правових норм у цифровому просторі, що, своєю чергою, може опосередковано стимулювати їх до запровадження більш суворих практик модерації контенту у відповідь на такі вимоги.

По-друге, стаття 14 DSA встановлює механізм повідомлення та реагування на випадки «незаконного контенту» [177]. Відповідно до неї, онлайн-платформи повинні забезпечити наявність процедур, які дозволяють будь-якій фізичній чи юридичній особі інформувати їх про існування у їхніх сервісах певних елементів інформації, що вважаються «незаконним контентом». При цьому платформи зобов'язані обробляти всі отримані повідомлення та ухвалювати рішення «вчасно, старанно та об'єктивно» [177]. З огляду на широке визначення «незаконного контенту» у DSA та враховуючи, що окремі держави-члени ЄС криміналізують поширення дезінформації, механізми повідомлення та видалення контенту поширюються також на випадки дезінформації [178]. Це означає, що DSA фактично екстраполює національні правові норми, які забороняють дезінформацію, та надає їм чинності у відносинах із цифровими платформами, створюючи єдиний правовий інструмент для їхнього застосування у загальноєвропейському контексті.

Здійснений аналіз основних принципів політики протидії дезінформації в ЄС, який ґрунтувався на правовому визначенні дезінформації в правовому полі ЄС та правовому полі держав-членів ЄС у контексті фундаментального права на свободу вираження поглядів дозволяє стверджувати, що, визначення дезінформації, запропоноване Єврокомісією, може бути піддане критиці через його надмірну широту та нечіткість, що ускладнює його застосування як юридичного визначення з точки зору правової визначеності, ефективності та дотримання свободи вираження поглядів. Деякі елементи цього визначення є особливо проблематичними, наприклад, включення категорії «інформації, що вводить в оману», яка потребує суб'єктивної оцінки. Відтак, таке визначення може функціонувати виключно як політичне, а не як юридичне. Здійснений аналіз засвідчив значні відмінності між національними підходами до регулювання дезінформації у державах-членах ЄС, а також виявив тенденцію до криміналізації цього явища, що свідчить про обмежений вплив поточної політики ЄС на процес гармонізації.

Ухвалений Закон про цифрові послуги спрямований на гармонізацію національних підходів до регулювання незаконного контенту в Інтернеті, може мати протилежний ефект і фактично посилити національні відмінності, а отже лише частково досягти заявленої мети гармонізації. Це пояснюється тим, що визначення «незаконного контенту» у DSA безпосередньо відсилає до законодавства держав-членів ЄС, охоплюючи всі національні положення, які застосовуються до дезінформації, що було предметом аналізу. Загалом DSA прагне уніфікувати процедури, за якими платформи повинні реагувати на поширення дезінформації у своїх сервісах, проте виникають сумніви щодо того, наскільки цей акт здатний усунути бар'єри для вільного обігу інформації, що виникають унаслідок різних національних підходів до боротьби з дезінформацією.

Як показало порівняння національних практик, більшість держав-членів, що регулюють дезінформацію, розглядають її крізь призму питань національної безпеки, громадського порядку та суспільного миру, і значна частина таких положень закріплена у кримінальному праві. Важливо також враховувати, що компетенції Єврокомісії у цій сфері залишаються обмеженими. Це створює ризик ігнорування тих національних рішень, які важко узгодити з фундаментальними європейськими цінностями, зокрема зі свободою вираження поглядів. У будь-якому випадку, регулювання дезінформації демонструє наростання напруги між національними та європейськими компетенціями, а також між різними регуляторними цілями у сфері дезінформації та цифрової економіки. Таким чином, хоча DSA створює єдину рамку для платформ, які повинні боротися з незаконною дезінформацією, при детальному аналізі стає очевидним, що він мало сприяє усуненню відмінностей між національними підходами та не пропонує єдиної моделі того, як платформи мають узгоджуватися з цими відмінностями.

2.2. Особливості національних моделей політики протидії дезінформації в державах-членах ЄС

Актуальність дослідження особливостей національних моделей політики протидії дезінформації в державах-членах ЄС є надзвичайно високою та багатовимірною з огляду на сучасні геополітичні, інформаційні та безпекові реалії. ЄС сьогодні знаходиться в умовах постійного впливу зовнішніх і внутрішніх деструктивних інформаційних потоків, які спрямовані на підрив демократичних інституцій, посилення політичної поляризації, втручання у виборчі процеси та послаблення єдності між державами-членами. Дезінформація, яка поширюється через цифрові платформи, соціальні мережі та медіа, стає інструментом гібридного впливу, який активно використовують як державні, так і недержавні суб'єкти. У цьому контексті національні моделі протидії дезінформації в межах ЄС набувають особливої ваги, оскільки, попри спільні стратегічні рамки, сформовані на рівні Єврокомісії, кожна держава має унікальні політичні, історичні, культурні передумови, що визначають її підхід до даної проблеми. Вивчення національних моделей реагування на дезінформаційні виклики дає змогу зрозуміти, які стратегії є найбільш адаптованими до нових типів загроз, як забезпечується демократичний контроль за циркуляцією дез(інформації), і яка роль громадянського суспільства у цьому процесі.

Вибір країн для аналізу національних інструментів протидії дезінформації ґрунтується на парадигмі інформаційної безпеки та необхідності охопити різні рівні вразливості та інституційної реакції на гібридні загрози з боку Росії. Дослідження включає кейси з ключових геополітичних кластерів: Східний фланг НАТО, Центральна Європа, західноєвропейські економічні лідери та Східне партнерство. Нами охоплені різні геополітичні, історичні та економічні контексти в межах ЄС та держав його безпосереднього східного сусідства. Така диверсифікація дозволяє провести комплексне порівняльне дослідження ефективності механізмів реагування на іноземні дезінформаційні впливи.

До групи країн із високим рівнем геополітичної вразливості та історичним досвідом тривалого зовнішнього інформаційного тиску включено держави Балтії

(Латвію, Литву та Естонію), які об’єднані спільним пострадянським бекграундом і безпосередньою територіальною близькістю до РФ. Додатковим фактором, що ускладнює їхній інформаційний простір, є присутність значної російськомовної меншини, яка часто стає цільовою аудиторією російських дезінформаційних кампаній. Таким чином, їхній досвід є критично важливим для вивчення інтегрованих державних та суспільних стратегій захисту національної інформаційної стійкості. Окрему увагу приділено Чеській Республіці як прикладу країни колишнього соціалістичного табору, яка здійснила успішну демократичну трансформацію. Чехія займає активну проукраїнську позицію і демонструє активність та ініціативу у реагуванні на російські дезінформаційні впливи як на державному рівні, так і через громадянське суспільство. Зокрема, прикладом ефективної низової протидії є діяльність «руху ельфів» (Czech Elves), що є унікальною моделлю самоорганізації громадянського суспільства для моніторингу та деконструкції дезінформаційних наративів. Дослідження також включає Францію та Німеччину як приклади потужних європейських країн Західної та Центральної Європи. Вони є основними економічними та політичними центрами ЄС, що робить їх ключовими мішенями для гібридних загроз, спрямованих на підрив європейської єдності. Вибір Німеччини особливо важливий з огляду на її статус «локомотива економіки ЄС» та наявність значних фінансових ресурсів для впровадження інноваційних та високотехнологічних механізмів протидії дезінформації. Аналіз їхніх стратегій дозволить виявити найкращі практики, які можуть бути імплементовані в країнах із меншими ресурсами. Окремим, але не менш важливим кейсом, є Республіка Молдова. Як країна-сусідка України та держава з невирішеним конфліктом на власній території, Молдова є об’єктом постійних та інтенсивних дезінформаційних атак з боку Росії. Аналіз її досвіду дозволяє оцінити зусилля, спрямовані на захист суверенітету та демократичного вибору. Зокрема, нещодавні парламентські вибори слугували ареною, на якій Росія задіяла значні ресурси та заходи у межах масштабних дезінформаційних кампаній, спрямованих на проросійський реванш. Вивчення цього контексту надає критично важливе розуміння

інструментів, необхідних для підтримки стійкості в умовах прямої конфронтації з агресивним зовнішнім інформаційним впливом [59]. Таким чином, комбінація цих країн забезпечує широкий та репрезентативний зріз інструментів, механізмів та рівня стійкості до дезінформації.

Для забезпечення системного та науково обґрунтованого порівняння, аналіз обраних національних моделей буде проведено за чотирма ключовими критеріями. По-перше, це нормативно-правова база кожної країни, зокрема наявність спеціалізованих законів (NetzDG в Німеччині та закон 2018 р. у Франції) та стратегічних документів («План дій» в Чехії та «Концепція національної безпеки» в Латвії). По-друге, це критерій інституційної архітектури, тобто наявність та повноваження спеціалізованих державних органів, відповідальних за протидію (наприклад, BIS, VIGINUM, Arcom). По-третє, це роль та інструменти громадянського суспільства, включаючи діяльність незалежних фактчекінгових організацій (AFP Factuel) та низових рухів («ельфи»). По-четверте, це загальний регуляторний підхід та ступінь державного втручання, що варіюється від прямих заборон мовлення (країни Балтії) до стимулювання онлайн-платформ до співпраці.

Держави Балтії є єдиними державами-членами ЄС, що в минулому мали статус республік СРСР, і на сьогодні є країнами проживання кількісно значної російської етнічної меншини, що сприяє проєкції стратегічних інтересів Москви в цьому європейському регіоні, незважаючи на вступ трьох країн до ЄС і НАТО в 2004 році [241]. Країни Балтії, як і інші європейські держави, стикаються з серйозною проблемою поширення дезінформації. Їхнє географічне розташування на східному кордоні ЄС робить їх особливо вразливими до російської пропаганди та дезінформаційних кампаній. Але на тлі Західноєвропейських та навіть Центральноєвропейських держав-членів ЄС, політика протидії дезінформації держав Балтії, на нашу думку, є не достатньо проактивною. Сильними сторонами держав Балтії у розумінні небезпек російської дезінформації, що є перевагою у виробленні рішень з протидії дезінформаційним наративам, можна вважати: опанований історичний досвід

травматичної російсько-радянської окупації; сусідство та прикордонні конфлікти з РФ; неприховувана агресивна риторика ЗМІ РФ проти «фашистської Прибалтики»; політичне визнання урядами російської загрози та відкрита солідарність з Україною в російсько-українській війні; членство в ЄС та НАТО.

У 1999 р. російський уряд вперше оприлюднив Закон «Про державну політику щодо співвітчизників за кордоном», який згодом був включений до Стратегії національної безпеки Росії [241]. Закон був покликаний «захистити» інтереси співвітчизників, до яких відносили російськомовних, вірних ідеям «руского міра» за мовою, історією та культурною ідентичністю, або тих, хто народився в СРСР і живе на території колишньої радянської республіки [399]. Будучи невід'ємним складником зовнішньої політики Росії, цей закон спрямовувався на використання російськомовних діаспор для розвитку мережі громадських організацій. У державах Балтії потенційними об'єктами такої політики були російські етнічні меншини, що компактно проживали на східних кордонах ЄС, зокрема у Нарві (Естонія) та Даугвапілсі (Латвія).

Російська стратегія поширення дезінформаційних наративів в державах Балтії пов'язана з геополітичною стратегією історичного ревізіонізму, яка заперечувала радянську окупацію держав Балтії, маркуючи анексію як акт політичної волі еліт Литви, Латвії та Естонії після звільнення від нацизму [296]. Таким чином, про радянська ностальгія була обрана як інструмент збереження російської соціальної пам'яті в Балтійському регіоні. Як наслідок, російська меншина в державах Балтії вимагала формування медійного середовища, здатного задовольнити її інформаційні потреби. У цьому контексті як прагматичний політичний крок варто оцінити створення проєвропейських російськомовних ЗМІ (онлайн-портал Балтійських новин Delfi [147], російська версія латвійського сайту RUS.LSM [294]), які одночасно були простором інклюзії для російської меншини та важливим інструментом протидії російській пропаганді. Зважаючи на складний процес соціальної інтеграції російськомовних жителів держав Балтії, через, насамперед, їх вікову структуру в якій домінували групи старшого вікового сегменту, створення

російськомовних ЗМІ було важливою ініціативою та альтернативою російським пропагандистським каналам. Варто відзначити, що на платформі RUS.LSM є розділи присвячені вивченню латиської мови [293], медіа грамотності [295], об'єктивному висвітленню російсько-української війни, що позитивно впливає на громадську думку. З іншого боку це призводить о *капсулювання* російської меншини в своєму російськомовному середовищі, проте плюсів більше ніж мінусів. Зауважимо, що про небезпеки «капсулювання» у форматі анклавів, влучно зазначала українська дослідниця Н. Ротар, наголошуючи на небезпеках відсутності дієвих інтеграційних стратегій національних держав, в яких є місця компактного проживання національних меншин [54, с. 174-179].

28 вересня 2023 р. латвійський парламент схвалив «Концепцію національної безпеки», в якій чітко визначено зміст стратегічних комунікацій та боротьби з деформацією як ключових елементів формування поля національної безпеки Латвії [384]. У документі наголошується, що заходи стратегічних комунікацій та боротьби з деформацією мають спрямовуватися на запобігання впливу іноземних держав, зокрема Росії, на внутрішню політику Латвії та латвійське суспільство засобами поширення дезінформації. Документ неодноразово вказує на Росію як на основне джерело загроз національній безпеці Латвії, включаючи інформаційну сферу. Зазначається, що повномасштабне військове вторгнення РФ в Україну, розпочате 24 лютого 2022 р. є ключовим фактором, що змушує переглядати Концепцію національної безпеки та рухатися в напрямі забезпечення того, що з 1 січня 2026 р. весь «контент, створений суспільними ЗМІ, має бути лише латиською мовою та мовами, що належать до європейського культурного простору» [384]. Цей крок фактично унеможливить для Латвійського телебачення та Латвійського радіо продовжити створювати контент російською мовою через припинення державного фінансування, що згідно з Концепцією, сформує «єдиний інформаційний простір» [384]. Тому він викликав неоднозначну реакцію. До прикладу, ряд журналістських спілок виступили проти такої ініціативи: «Ми стурбовані тим, що ця нова пропозиція буде означати, що російськомовні жителі Латвії більше не матимуть регулярного

доступу до достовірної та перевіреної інформації, що залишить їх сприятливими для дезінформації, фейкових новин та пропаганди. Здатність суспільних ЗМІ надавати життєво важливу інформацію та зв'язуватися з усім суспільством є особливо важливою з огляду на агресію Росії в Україні. Російською мовою розмовляє щонайменше третина населення Латвії, включаючи не лише етнічних росіян (які складають близько чверті населення), але й багато інших меншин, таких як українські біженці. Якщо пропозицію буде прийнято, вона підірве основні права громадян, закріплені в міжнародному, європейському та європейському законодавстві про права людини, на «доступ до ЗМІ та поширення й отримання інформації, зокрема рідною мовою» [270]. Зважаючи на те, що подібні принципи знайшли відображення в Законі Латвії про суспільні електронні засоби масової інформації та адміністрування, Комітет захисту журналістів, Європейський мовний союз, Європейська федерація журналістів, Міжнародна федерація журналістів, Фонд «Справедливість для журналістів», «Репортери без кордонів», Медіа-організація Південно-Східної Європи, закликали уряд переглянути свою позицію [280]. Цей приклад демонструє всю складність організації процесу протидії дезінформації, коли рішучість національної держави йти на радикальні кроки в протидії російській політиці дезінформації супроводжується критикою ініціатив уряду з боку противників російського геополітичного ревізіонізму та ідеології «руского міра».

В латвійській «Концепції національної безпеки 2023» [384] дезінформація визначена як серйозна загроза. Латвія не просто реагує на цю загрозу, а вибудовує комплексну стратегію, яка включає підвищення медіаграмотності населення, розвиток власного якісного інформаційного простору та активну стратегічну комунікацію. Що стосується заборони російських медіа, документ не використовує прямих формулювань заборони, але вказує на стратегічні кроки, які фактично призводять до виключення російської дезінформації з латвійського інформаційного простору. Це включає припинення ретрансляції пропагандистських програм та боротьбу з нелегальним доступом до них з паралельним активним розвитком національних медіа, що є альтернативою

російським впливам. Така політика відображає глибоке усвідомлення Латвією інформаційної війни та її деструктивного впливу на національну безпеку.

Литва була однією з перших держав ЄС, яка заборонила мовлення російських державних телеканалів, вважаючи їх основним джерелом дезінформації. Ще у 2020 р. Литва заборонила мовлення російського державного телеканалу RT [262]. Через невеликий відсоток російськомовних громадян у Литві, поширення російської дезінформації та маніпуляцій серед литовців є не таким інтенсивним. Комісія з радіо і телебачення Литви у 2022 р. призупинила мовлення 32 телевізійних програм, контрольованих Газпром Медіа, та шести державних мовних каналів [162], що узгоджувалося зі спільною європейською політикою протидії дезінформації, адже 2 березня 2022 р. ЄС зупинив мовлення російських державних ЗМІ Sputnik та Russia Today на території ЄС у зв'язку з початком масштабної агресії Росії проти України [14]. У вересні 2023 р. LRTK прийняла рішення про заблокування 53 IP-адрес, які забезпечували он-лайн поширення російських пропагандистських телепрограм [291]. У червні 2024 р. Литва продовжила заборону на трансляцію російських та білоруських телеканалів на невизначений термін, посилаючись на те, що ці країни становлять загрозу національній безпеці згідно з Національною стратегією безпеки [298]. Ці заходи свідчать про послідовну політику Литви щодо протидії російській пропаганді та дезінформації у форматі проактивної стратегії.

Держави Балтії активно використовують інструментарій та підходи ЄС та НАТО, є підписантами більшості європейських ініціатив спрямованих на протидію дезінформації. Тут важливим для України є досвід Естонії, за ініціативою якої НАТО у 2004 р. розробив концепцію центру передового досвіду в сфері кіберзахисту [368]. 14 травня 2008 р. за участі Естонії Німеччини, Італії, Латвії, Литви, Словаччини та Іспанії був створений Центру кіберзахисту (Cooperative Cyber Defense Center of Excellence, CCDCOE). Північноатлантична рада ініціювала його розміщення в Таллінні та надала Центру повну акредитацію та статус Міжнародної військової організації у жовтні того ж року. До 2025 р.

CCDCOE виросла та розширилася, об’єднавши 39 держав-союзників по НАТО та однодумців-партнерів поза межами Альянсу, включаючи Україну.

Зауважимо, що досвід держав Балтії у протидії дезінформації був покладений в основу вироблення національної моделі в Молдові. У 2017 р. парламент цієї держави зробив спробу обмежити поширення російських новин, ухваливши відповідні зміни до законодавства. Однак тодішній президент Молдови І. Додон, відомий своїми проросійськими поглядами, ветував цей закон, назвавши його загрозою демократії. Президентка Молдови М. Санду в 2022 р. підписала закон про інформаційну безпеку, який забороняє поширення новинного та аналітичного контенту з країн, які не ратифікували Конвенцію про транскордонне телебачення. Зокрема це означає, що в Молдові заборонили російські інформаційні програми. Під дезінформацією в законі мається на увазі «навмисне поширення хибної інформації, створеної для заподіяння шкоди особистості, соціальній групі, організації чи безпеці держави» [12]. За її поширення передбачено штрафи від 40 до 100 тисяч леїв (від 2 до 5 тисяч євро), а також зупинення ліцензії на мовлення терміном до 7 днів. Контроль за виконанням закону покладено на Раду з телерадіомовлення.

Отже, досвід держав Балтії вирізняється комплексним і водночас адаптивним характером реагування. Усі три держави розвинули національні стратегічні рамки інформаційної безпеки, в яких дезінформація розглядається як складова гібридної загрози, що вимагає технологічної, аналітичної відповіді, й посилення стійкості суспільства. Важливу роль відіграє законодавче забезпечення, наприклад, Литва посилила механізми регулювання інформаційного простору, включно із санкціями щодо медіа, які поширюють прокремлівську пропаганду, обмеженням доступу до російських каналів, блокуванням інформаційних ресурсів, що становлять загрозу для національної безпеки. Держави Балтії демонструють високий рівень стратегічного мислення в інформаційній політиці, адже дезінформація розглядається ними як загроза фактичній точності повідомлень та інструмент підриву довіри до демократичних інституцій, дискредитації євроатлантичної інтеграції та впливу на демократичні

політичні процеси. Саме тому інформаційна політика тісно інтегрована з оборонною стратегією та політикою національної ідентичності та стійкості до загроз (Додаток В). Особливо важливо те, що ці держави здійснюють політику інтеграції російськомовного населення, поєднуючи заходи з протидії дезінформації із програмами інклюзивної комунікації, навчання державної мови та посилення громадянської освіти. У європейському вимірі держави Балтії відіграють роль ініціаторів посилення загальноєвропейської політики протидії дезінформації, виступаючи за більш жорстке регулювання цифрових платформ, прозорість алгоритмів поширення інформації, відповідальність соціальних мереж за контент. Вони послідовно підтримують ініціативи Єврокомісії у сфері цифрових сервісів, закликаючи до посилення контролю над платформами, які дозволяють маніпулятивне поширення деструктивного контенту.

Ще одна національна модель протидії дезінформації була сформована в Чехії, державі, яка активно допомагає Україні зброєю, дипломатичною підтримкою та прийомом біженців в умовах російсько-української війни. Державною інституцією, що відповідає за інформаційну безпеку в Чехії є Служба Інформаційної безпеки Чехії (Bezpečnostní informační služba, BIS) [104]. На основі сортування та аналізу отриманої розвідувальної інформації вона виконує дві основні функції: по-перше, інформаційну, що означає інформування осіб та установ, визначених законом, про діяльність, інтереси та плани іноземних держав на території Чеської Республіки; по-друге, превентивну, пов’язану з розробкою та впровадженням заходів, які ускладнюють проведення розвідувальних дестабілізуючих операцій іноземних держав на території Чехії. Завданням BIS як контррозвідувальної служби є виявлення, моніторинг та збір інформації про діяльність іноземних держав та фізичних і юридичних осіб, що діють в інтересах та на благо іноземних держав на території Чеської Республіки. Метою інформаційно-превентивної діяльності BIS є: запобігання витоку секретної або конфіденційної інформації в розпорядження іноземної держави; відкрите або приховане втручання в діяльність розвідувальних служб з боку

іноземної держави; виявлення та перешкоджання операціям впливу іноземної держави (дезінформація, маніпуляції, обман, пропаганда) [104].

BIS не обмежується фактчекінгом або написанням звітів, маючи законні інструменти агенти служби викривають та карають суб'єктів поширення дезінформації. До прикладу у вересні 2023 р. BIS викрила російського агента, який поширював дезінформацію [105], з приводу чого Голова служби М. Куделка зауважив: «Деякі дезінформаційні вебсайти запозичують контент і з російських джерел та російських державних ЗМІ, а це означає, що деякі прокремлівські наративи досягають чеського інформаційного середовища … » [133]. За словами М. Куделки, поле дезінформації в Чехії є фрагментарним, для якого характерним є прийняття наративів, що відповідають російській пропаганді, напади на належність Чехії до політичного поля ЄС та безпекового поля НАТО, ідеалізація Росії та вербальна агресія щодо США.

У звіті за 2023 р. аналітики BIS наголосили, що російська війна проти України стала каталізатором системних змін у багатьох аспектах функціонування чеської держави, зокрема в секторі інформаційної безпеки та протидії дезінформації [106]. Зокрема, 15 листопада 2022 р. був ухвалений «План дій Чеської Республіки щодо протидії дезінформації» [328], підготовлений Урядовим уповноваженим з питань ЗМІ та дезінформації на період 2023–2025 рр. В плані доволі критично оцінювалася здатність Чехії протистояти масованим дезінформаційним атакам, тому пропонувалося оновлення національної моделі протидії дезінформаційним загрозам за такими напрямами. По-перше, це напрям системних змін, який розгортався через: призначення Урядового уповноваженого з питань медіа та дезінформації; створення експертно-консультативного органу для Урядового уповноваженого, що об'єднав державний, неурядовий, академічний, медійний та приватний сектори; посилення кадрових та технічних можливостей для моніторингу дезінформації та стратегічної комунікації в органах державної влади; розробку та реалізацію довгострокової стратегії використання комунікації для зниження негативного впливу дезінформації на суспільство.

По-друге, це напрям посилення стійкості чеського суспільства, в рамках якого планувалися: вирішення проблеми відсутності прозорої та стратегічної фінансової підтримки неурядових організацій, що протидіють дезінформації; т розробка концепції державної підтримки незалежних ЗМІ; демонетизація дезінформаційного середовища.

По-третє, це напрям міжнародної співпраці щодо соціальних медіа через активну підтримку поточних та майбутніх ініціатив ЄС; розробка національної стратегії для уможливлення впливу на європейські ініціативи.

По-четверте, це напрям розробки законодавчої бази щодо державного регулювання процесу блокування он-лайн контенту, що становить загрозу національній безпеці, включаючи чіткі процедури та контрольні механізми; внесення змін до кримінального законодавства про встановлення відповідальності за умисне поширення дезінформації, яка має особливо серйозні наслідки, наприклад, загрожує демократичному характеру чеської держави чи її безпеці.

По-п’яте, це напрям забезпечення фінансових та кадрових ресурсів, зокрема, створення відповідних кадрових можливостей в інфраструктурному полі Уряду Чехії шляхом розширення відділу стратегічних комунікацій до департаменту стратегічних комунікацій та протидії дезінформації; формування організаційних можливостей для централізованого планування реклами з протидії дезінформації з метою забезпечення прозорого та ефективного використання державних коштів.

Оновлення чеської національної моделі протидії дезінформації у 2023–2024 рр. здійснювалося в рамках політичного дискурсу про криміналізацію явища поширення дезінформації. Представник чеського уряду з питань ЗМІ та дезінформації М. Кліма наголошував: «Точиться багато експертних дискусій щодо того, чи достатньо чинного кримінального законодавства для боротьби з випадками дезінформації» [233]. Негайне закриття вебсайтів, які уряд класифікує як дезінформаційні, кримінальне правопорушення за поширення дезінформації, сотні мільйонів крон для ЗМІ та окремих організацій, що

розслідують дезінформацію були означені як ефективні елементи національної моделі протидії дезінформації.

Свої переваги має французька національна модель протидії дезінформації. За ініціативою президента Франції Е. Макрона у 2018 р. був ухвалений закон «Закон про боротьбу з маніпуляціями інформацією» [288], спрямований на протидію російській дезінформації. Цей закон став відповіддю на відкрите втручання Росії у французькі виборчі процеси і уможливив обмеження мовлення російських пропагандистських телеканалів. За рішенням суду можна було вимагати видалення контенту, якщо він мав дезінформаційну складову, масово та штучно поширювався і міг вплинути на чесність виборів або громадський порядок. Закон також накладав на онлайн-платформи зобов'язання щодо прозорості та співпраці. Е. Макрон публічно заявив, що «Russia Today та Sputnik не функціонували як органи преси, вони діяли як органи впливу та пропаганди, і навіть брехливої пропаганди» [16]. Зауважимо, що за цим законом Вища аудіовізуальна рада (CSA) отримувала право припиняти мовлення будь-якого медіа, яке під час виборів поширювало небезпечну інформацію, що могла бути пов'язана з впливом іноземних держав.

13 липня 2021 р. у Франції була створена «Служба пильності та захисту від іноземного цифрового втручання» (далі – VIGINUM» [287] під керівництвом Генерального секретаря оборони та національної безпеки. VIGINUM – це технічна та операційна служба французької держави, відповідальна за моніторинг та захист від іноземного цифрового втручання, зокрема і засобами дезінформації. Діяльність VIGINUM організована навколо операцій захисту певних суспільно значущих тем, довкола яких потенційно може генеруватися дезінформація. До таких тем були віднесені інституційні, демократичні, політичні, суспільні, історичні, спортивні події, заплановані чи поточні події, що відбуваються у Франції або впливають на громадські дебати в країні.

Це стимулювало формування у Франції розвиненої мережі фактчекерів. Зокрема, агентство AFP Factuel є одним із найбільших у світі [74], а VIGINUM співпрацює з ініціативами з перевірки фактів, такими як Objectif Désinfox, який

є спільним проєктом Agence France-Presse та Google, запущеним у 2017 р. [75]. AFP Factuel, як служба цифрової верифікації, а згодом, провідна організація з перевірки фактів глобального рівня, здійснює неперервний моніторинг он-лайн контенту національними мовами ЄС, враховуючи культурні, мовні та політичні особливості держав-членів ЄС. AFP Factuel є підписантом Кодексу принципів Міжнародної мережі перевірки фактів [260], що гарантує незалежність, прозорість та неупередженість їхньої роботи.

Згідно з французьким законодавством про протидію дезінформації від 1 січня 2022 р. діє Орган регулювання аудіовізуального і цифрового зв'язку (ARCOM) [88]. Його поява в системі інструментів політичного управління політикою протидії дезінформації є результатом злиття CSA та органом, що контролює розповсюдження творів і захист прав власності в Інтернеті (HADOPI). ARCOM гарантує свободу комунікацій та контролює фінансування аудіовізуальної творчості та захист прав авторів. Його регулювання поширюється на он-лайн платформи, соціальні мережі та пошукові системи, зокрема контролю за тим, як сервіси впроваджують інструменти та ресурси для досягнення основних цілей державної політики протидії дезінформації. ARCOM також є інституцією, яка входить до системи довірених структур, відповідальних за виявлення та повідомлення про підозрюваний незаконний контент на он лайн платформах у Франції, відповідно до Закону ЄС про цифрові послуги. Зауважимо, що в рамках своїх компетенцій ARCOM збирає інформацію щодо конкретних засобів, застосованих платформами для боротьби з ризиками маніпуляції інформацією в період, що передує президентським та парламентським виборам, однак він не має повноважень розглядати конкретні справи поширення дезінформаційних наративів.

Дотичним інструментом реалізації політики протидії дезінформації у Франції є Національне агентство з безпеки інформаційних систем (ANSSI), яке діє виключно в сфері кібербезпеки та є національною інституцією з питань кібербезпеки та кіберзахисту. Міжвідомче агентство, відповідальне за створення

та організацію захисту країни від кібератак, сприяє зміцненню загального рівня кібербезпеки та стабільності кіберпростору [289].

Отже, французька національна модель протидії дезінформації поєднує демократичні принципи, правову регламентацію та інституційну відповідальність. Французький підхід спирається на чітке законодавче розмежування дезінформації та свободи слова, орієнтуючись на захист виборчої легітимності, державного суверенітету та громадської довіри. Франція в протидії дезінформації рухається до формування сталої інфраструктури інформаційної стійкості, яка опирається на інституційний розвиток фактчекінгу, прозорість алгоритмів цифрових платформ та партнерство з недержавними акторами. Водночас державна політика залишається вразливою до низки викликів, насамперед, до технологічної складності інформаційних операцій, нерівномірної участі платформ у виконанні регуляторних вимог. Для України французька модель протидії дезінформації може бути прикладом цілеспрямованої державної політики, яка поєднує безпекові потреби та демократичні цінності.

Національна модель протидії дезінформації в Німеччині є багаторівневою, правовою та орієнтованою на довгострокове формування стійкого інформаційного середовища. Німеччина була однією з перших держав, яка прийняла у 2017 р. «Закон про забезпечення дотримання мережевих правил» (NetzDG) [107], який зобов’язав соціальні мережі видаляти незаконний контент протягом 24 годин: соціальні мережі, у яких зареєстровано понад 2 мільйони користувачів із Німеччини, мають на місцевому рівні видаляти «очевидно незаконний контент» (допис, зображення чи відео) упродовж 24 годин після сповіщення. Якщо законність важко визначити одразу, постачальник інформаційної послуги має розглянути запит упродовж семи днів. Цей процес може тривати довше лише в окремих випадках, наприклад якщо залучено авторів контенту або рішення приймає спільний галузевий орган, акредитований як саморегульована організація. Відповідно до закону NetzDG, контент, що має бути видалений, має порушувати одну з визначених законом статей Кримінального кодексу. Найбільші сервіси враховують вимоги німецького

національного законодавства та співпрацюють з урядом. Разом з тим, Німеччина, як одна з провідних демократій ЄС, сформувала національну модель, яка базується не стільки на криміналізації дезінформації як окремого правопорушення, скільки на інтеграції вже існуючих правових норм, що стосуються мови ворожнечі, наклепу, підбурювання до насильства та захисту виборчих процесів. Замість запровадження спеціального антисуб'єктного закону проти дезінформації, як у випадку Франції, Німеччина зробила ставку на нормативну рамку, в якій центральне місце займає закон NetzDG, що зобов'язує великі соціальні платформи видаляти незаконний контент у встановлені терміни. Це положення стало частиною ширшого процесу посилення відповідальності цифрових платформ та створення нормативної моделі співрегуляції.

Інституційний ландшафт німецької політики протидії дезінформації є фрагментарним, але водночас гнучким. До протидії маніпуляціям залучені різні міністерства та федеральні служби: МВС, МЗС, агентства кібербезпеки, а також спеціалізовані структури (ZEAM), покликаний координувати виявлення і нейтралізацію зовнішніх інформаційних впливів. Втім, одним із головних викликів для німецької національної моделі протидії дезінформації залишається відсутність єдиного координаційного центру, що уповільнює реагування на складні, скоординовані інформаційні атаки. Також існує брак правових механізмів для впливу на «сірі зони» дезінформації, яким є маніпулятивний контент, який формально не є незаконним, але має руйнівний ефект для політичного дискурсу. У цьому контексті особливо небезпечною є нова хвиля технологічних загроз, пов'язаних з використанням бот-мереж, генеративного штучного інтелекту та діпфейків. Ще однією потенційною вразливістю є обмежене фінансування ZEAM, що ставить під сумнів його довгострокову ефективність.

Отже, німецька національна модель протидії дезінформації є прикладом прагматизму, коли держава, суспільство та цифрові гравці формують взаємозалежну систему інформаційної безпеки, ефективність якої залежатиме від здатності адаптуватися до нових технологічних умов, посилити міжвідомчу

координацію та зміцнити інституційну спроможність без ризику для відкритого інформаційного простору. У майбутньому ця модель має потенціал стати однією з провідних у межах ЄС, задаючи стандарт відповідального, але водночас ліберального підходу до інформаційних викликів цифрової доби.

Отже, здійснений порівняльний аналіз національних моделей протидії дезінформації засвідчив, що попри наявність загальноєвропейських рамок для всіх держав-членів ЄС та Молдови як держави Східного партнерства, політика протидії дезінформації залишається значною мірою гетерогенною та національно-специфічною. Спільним для всіх досліджених кейсів є чітке усвідомлення російської дезінформації як прямої загрози національній безпеці, що призвело до повсюдного посилення нормативно-правової бази та інституціоналізації протидії через створення та адаптацію спеціалізованих державних інституцій. Водночас, нами виявлено кардинальні відмінності у підходах, зумовлені історичним досвідом та політичною культурою. держави Балтії, Чехія та Молдова, маючи травматичний досвід прямого зовнішнього тиску, демонструють найбільш жорстку та проактивну модель організації національної політики протидії дезінформації, що включає прямі заборони мовлення та активний контррозвідувальний компонент. Натомість Німеччина та Франція, здійснюючи пошук балансу між безпекою та свободою слова, сформували м’які реактивні моделі, відмінність між якими полягає в тому, що Німеччина розгортає протидію дезінформації через правову кримінальну відповідальності платформ, а Франція – через інституційний захист демократичних процесів. Таким чином, кожна проаналізована країна сформувала унікальну конфігурацію інструментів протидії дезінформації, адаптуючи загальні європейські принципи до власних безпекових реалій.

2.3. Перспективи наближення політики протидії дезінформації України до принципів та стандартів ЄС

Проведений компаративний аналіз національних моделей протидії дезінформації держав-членів ЄС засвідчив, що в його межах сформувалася

розгалужена, але водночас гетерогенна система протидії дезінформації, де кожна країна адаптує загальні європейські директиви до власних геополітичних та історичних реалій. Україна, виступаючи сьогодні фактичною складовою загальноєвропейської системи інформаційної безпеки та надаючи унікальний досвід безпосередньої протидії агресору, переходить від фази ситуативної взаємодії до етапу глибокої нормативної та інституційної сумісності з ЄС. У цьому контексті логічним постає перехід до детального розгляду конкретних напрямів та стратегічних перспектив наближення української політики протидії дезінформації до принципів ЄС, що є вимогою євроінтеграційного процесу та спільною безпековою необхідністю для захисту демократичних цінностей. Шляхом адаптації європейського досвіду, Україна прагне створити стійку систему протидії дезінформації. Це досягається за допомогою широкого спектру інструментів, які надають міжнародні організації, зокрема ЄС, ОБСЄ, ЦЄІ та НАТО [41, с. 42-43].

Наближення України до європейських принципів у сфері інформаційної безпеки є процесом, що охоплює політичну, правову та інституційну площини. Міжнародна співпраця у цьому контексті виступає інструмент запозичення досвіду в процесі створення стійкої національної системи, здатної функціонувати в спільному безпековому полі з ЄС [166]. Взаємодія між Україною та ЄС у сфері інформаційної безпеки сьогодні вийшла за межі консультативної допомоги. Ми спостерігаємо створення інтегрованої моделі, в якій український досвід «польової» протидії дезінформації поєднується з інституційною матрицею протидії дезінформаційним загрозам в ЄС. Взаємодія між Україною та ЄС у сфері протидії дезінформації реалізується через кілька ключових рамок.

По перше, це секторальна інтеграція України до європейського простору протидії дезінформації. На початок 2026 р. секторальна інтеграція в європейську структуру протидії дезінформації визначена прагненням України стати повноправною частиною Єдиного цифрового ринку ЄС, що вимагає фундаментальної реформи медіасфери відповідно до правової системи acquis ЄС

[186]. Україна вже досягла значного прогресу на цьому шляху, впровадивши ключові закони про електронні комунікації та наблизивши загальну правову базу до європейських стандартів [186]. Головним інструментом цієї гармонізації став рамковий Закон «Про медіа», який є основою для створення прозорого та стійкого медіаландшафту, здатного ефективно протистояти зовнішнім маніпуляціям [47].

Секторальне зближення охоплює і безпековий вимір, зокрема через поступову конвергенцію зі Спільною зовнішньою та безпековою політикою ЄС [187]. Це партнерство є взаємовигідним, оскільки дозволяє поєднувати інституційну потужність ЄС з унікальним досвідом України в протидії агресії. Важливим етапом цієї інтеграції стало підписання двосторонньої безпекової угоди у червні 2024 р., яка вперше на такому високому рівні закріпила спільні заходи проти іноземних інформаційних маніпуляцій та втручань (FIMI) [218]. Україна також активно долучається до європейських оборонних ініціатив та місій, таких як EUMAM та EUAM, що зміцнює загальноєвропейську систему інформаційної безпеки. Таке глибоке залучення до проєктів та спеціалізованих кібердіалогів свідчить про те, що Україна вже стала невід'ємною складовою європейської системи захисту демократичних цінностей [187].

По-друге, операційна співпраця та інформаційний обмін через пряму взаємодію українських структур із Системою швидкого оповіщення (Rapid Alert System, RAS) та Агентством ЄС з кібербезпеки (ENISA) [130]. Цей напрям є найбільш динамічним компонентом секторальної інтеграції, оскільки він забезпечує практичну синхронізацію оборонних зусиль у цифровому середовищі [203]. Фундаментом операційної взаємодії є прямий обмін даними про інформаційні загрози через RAS, яка координується Європейською службою зовнішніх дій (EEAS). Участь України в цій системі дозволяє національним структурам, зокрема Центру протидії дезінформації при РНБО та Центру стратегічних комунікацій при МКІП, синхронізувати свої реакції з державами-членами ЄС. Це забезпечує можливість одночасного виявлення, маркування та

нейтралізації транскордонних дезінформаційних кампаній ще на етапі їхнього зародження. Важливим кроком у посиленні технічної сумісності стало підписання у грудні 2023 р. Робочої угоди між Агентством Європейського Союзу з кібербезпеки (ENISA) та українськими профільними відомствами [163] Цей документ відкрив шлях до глибокої операційної співпраці у сфері аналізу гібридних загроз, включаючи спільний моніторинг інцидентів, обмін розвідувальними даними про кібератаки, що супроводжують дезінформаційні операції, та участь українських фахівців у європейських кібертренінгах. Особливе місце в операційній структурі посідає впровадження спільної методології FIMI. Україна фактично стала головним майданчиком для апробації нових європейських стандартів виявлення маніпулятивних дій іноземних акторів. Завдяки цьому український «польовий» досвід безпосередньо впливає на формування «Гібридного інструментарію» ЄС (EU Hybrid Toolbox), дозволяючи ЄС швидше адаптувати свої алгоритми захисту до мінливих тактик ворога. Юридичне закріплення цієї операційної моделі відбулося у червні 2024 р. через підписання Спільних безпекових зобов'язань, які передбачають постійну координацію зусиль у сфері протидії іноземним інформаційним маніпуляціям як обов'язковий елемент спільної архітектури безпеки. Таким чином, операційна співпраця перетворила Україну на суб'єкта європейського безпекового простору, що забезпечує сталий розвиток колективної стійкості [135].

По-третє, технічна та фінансова підтримка. Цей напрям співпраці полягає у системному ресурсному забезпеченні українського інформаційного та безпекового секторів. Технічна та фінансова підтримка спрямована на досягнення двох цілей: забезпечення життєздатності незалежних медіа як альтернативи пропаганді та надання високотехнологічного інструментарію для кіберзахисту критичної інфраструктури [187]. Фактично, це створення «матеріального щита», який дозволяє переводити теоретичні стратегії протидії дезінформації у практичну площину оперативної роботи [218]. У практичній площині технічна підтримка реалізується через поглиблену участь України в оборонних проєктах Постійного структурованого співробітництва (PESCO), що

розгортається через залучення українських фахівців до Команд швидкого реагування на кіберзагрози (CRRT) [336]. Така інтеграція забезпечує оперативний обмін технологіями захисту державних реєстрів від цифрових диверсій, що супроводжують дезінформаційні операції. Фінансовий вимір співпраці у 2025 р. було суттєво розширено через програму «EU4IndependentMedia», яка отримала додаткові 10 млн євро для підтримки регіональних редакцій та впровадження інструментів верифікації контенту на основі ШІ [165]. Окремим механізмом виступає Європейський фонд миру (EPF), ресурси якого у 2024–2025 рр. почали спрямовуватися на закупівлю спеціалізованих систем моніторингу та автоматизованої нейтралізації масштабних бот-мереж [135].

По-четверте, стратегічні комунікації, а саме інституційна координація та спільна атрибуція загроз. Цей аспект полягає у створенні спільного політичного та доктринального фундаменту для протидії гібридним загрозам. Стратегічні діалоги є майданчиком для узгодження «правил гри», визначення спільних цінностей та формування правових рамок, що дозволяють Україні та ЄС виступати єдиним фронтом. Їх розгортання відображає перехід від простого консультування до спільного формування європейської політики у сфері когнітивного та цифрового суверенітету. Практична реалізація цього напряму базується на регулярних форматах, таких як Кібердіалог Україна-ЄС, третя ітерація якого у липні 2024 р. зафіксувала перехід до фази повної операційної сумісності у сфері боротьби з дезінформацією як елементу гібридних атак. Фундаментальним документом у цьому процесі є Спільні безпекові зобов’язання, підписані 27 червня 2024 р., які офіційно закріпили FIMI як обов’язковий елемент безпекового співробітництва на наступні десять років [136]. У межах стратегічного діалогу Україна також була інтегрована у новий санкційний механізм ЄС, запроваджений у жовтні 2024 р. спеціально для протидії дестабілізуючій діяльності РФ за кордоном [217]. Такий рівень координації дозволяє сторонам використовувати спільну методологію атрибуції інформаційних загроз, що детально описано у третьому щорічному звіті EEAS

щодо загроз FIMI, опублікованому у березні 2025 року [204]. Крім того, діалог охоплює питання захисту демократичних процесів та когнітивної стійкості, що передбачає впровадження спільних стандартів захисту виборчих систем від маніпулятивних втручань [137].

І по-п’яте, це актуальні сьогодні, безпекові гарантії, тільки в контексті інформаційної безпеки та протидії дезінформації. Спільні зобов’язання та довгострокова стійкість є метою взаємних гарантій. Ця площина співпраці позначає фундаментальний перехід від формату партнера, який надає підтримуючу допомогу до формату колективної інформаційної оборони. Безпекові гарантії в інформаційній сфері означають, що ЄС офіційно визнає дезінформацію та гібридні атаки на Україну загрозою для власної безпеки. Суть аспекту полягає у юридичному закріпленні обов’язків ЄС підтримувати Україну у виявленні, атрибуції та відбитті маніпулятивних втручань протягом тривалого часу, що забезпечує стабільність ресурсів та політичну невідворотність покарання для агресора. Практичним втіленням цієї площини стало підписання 27 червня 2024 р. Спільних безпекових зобов’язань між Україною та ЄС, в яких уперше на такому високому рівні було деталізовано заходи FIMI [137]. У межах цих гарантій Україна отримала повний доступ до «Гібридного інструментарію ЄС» [203], що дозволяє синхронізувати національні заходи реагування з європейськими стандартами атрибуції загроз. Важливим юридичним кроком у межах цих зобов’язань стало впровадження у жовтні 2024 р. нового санкційного режиму ЄС, який дозволяє запроваджувати обмежувальні заходи проти фізичних та юридичних осіб, причетних до дестабілізації інформаційного простору України. У звіті Європейської Комісії за 2025 р. зазначається, що такий підхід дозволив створити «захисну парасольку» над українським медіапростором, поєднуючи моніторинг у реальному часі з політичним тиском на технологічні платформи для блокування ворожих мереж. Окремим напрямом підвищення стійкості, згідно з третім звітом EEAS за березень 2025 р., стало спільне розроблення сценаріїв реагування на масове використання дипфейків під час виборчих циклів, що забезпечує готовність інституцій до нових технологічних

викликів. Таким чином, безпекові гарантії інтегрували інформаційний суверенітет України у спільний безпековий периметр Європи [136].

Розвиток співпраці України та ЄС у сфері протидії дезінформації пройшов шлях від тактичного реагування на окремі інциденти до створення цілісної колективної стійкості [187]. Цей процес був зумовлений необхідністю постійної адаптації до мінливих форм гібридної агресії, що вимагало поступового переходу від моніторингу контенту до системного аналізу маніпулятивної поведінки іноземних акторів [218]. Системний розгляд етапів цього процесу дає змогу простежити, як український досвід безпосередньої протидії дезінформації став каталізатором для вдосконалення європейських механізмів захисту демократичного простору [203].

Перший етап можна назвати реактивним, він тривав у 2014–2018 рр. Суть цього етапу полягає у переході ЄС від стратегічного заперечення проблеми до перших кроків інституційного маркування загроз. На цьому етапі всі рішення ухвалювалися як термінова відповідь на шоковий вплив російської агресії проти України та окупацію Криму. Головна метою було вивчення методів ворога, створення бази даних дезінформації та спроба налагодити першу комунікацію з аудиторіями країн Східного партнерства через спростування маніпуляцій. Початковою точкою інституціоналізації протидії дезінформації стало рішення Європейської Ради від березня 2015 р., яке закликало Високого представника ЄС розробити план дій щодо стратегічних комунікацій для протидії російським кампаніям [188]. Результатом цього стало створення у квітні 2015 р. в межах Європейської служби зовнішніх справ (EEAS) оперативної групи East StratCom Task Force (EStratCom), яка стала першим у світі офіційним підрозділом такого типу [216]. Основним інструментом групи став проєкт «EUvsDisinfo», запущений наприкінці 2015 р., що започаткував системне розбирання та деконструкцію кремлівських наративів у реальному часі [332]. Завершенням цієї фази стало прийняття у грудні 2018 р. «Плану дій проти дезінформації», який вперше вивів проблему на рівень загальноєвропейської безпекової стратегії та ініціював створення Системи швидкого оповіщення (RAS) [171].

Наступний етап (2019-2021 рр.), можна описати як етап «політичної інституціоналізації». Його суть полягає у переході від тактичного реагування до системного політичного проєктування спільного безпекового простору. Якщо раніше Україна розглядалася переважно як об'єкт дослідження для East StratCom, то тепер вона перебрала на себе роль проактивного партнера. Цей період характеризується перенесенням питання дезінформації з суто «медійного» поля у площину дипломатії та секторальної інтеграції, в якій українські кейси стають драйверами для створення нових інституційних вузлів у самому ЄС. Поворотним моментом у переході до цієї фази став візит віце-прем'єра Д. Кулеби до Брюсселя у 2019 р., який заклав фундамент для включення питань інформаційної безпеки до спільного дискурсу України та ЄС, в якому українська сторона досягла принципової домовленості про поглиблення секторальної інтеграції, зокрема у сферах цифрового ринку, юстиції та безпеки [346]. Цей візит був критично важливим, оскільки він відбувся невдовзі після запуску в ЄС (у березні 2019 р.) Системи швидкого оповіщення RAS для протидії дезінформації. Таким чином, домовленості, досягнуті Д. Кулебою, заклали політичне підґрунтя для майбутнього приєднання України до цього ключового механізму ЄС та прямої співпраці з East Stratcom, що стало практичним втіленням стратегії євроінтеграції у сфері інформаційної безпеки [310].

Саме тоді Україна вперше чітко артикулювала, що протидія дезінформації передбачає досягнення цифрової сумісності із acquis ЄС. Ця динаміка отримала логічне продовження під час 22-го Саміту Україна–ЄС у 2020 р., на якому сторони офіційно визнали дезінформацію загрозою демократії та домовилися про створення спеціалізованого формату діалогу [222]. Готовність України співпрацювати в питаннях протидії дезінформації того є року висловив Президент України під час виступу на загальних дебатах 75-ї сесії Генеральної Асамблеї ООН, у вересні 2020 р., запропонувавши створити в Києві штаб-квартиру міжнародного офісу з протидії дезінформації та пропаганді: «Україна як одна з держав, яка з 2014-го активно протидіє пропаганді та інформаційним атакам, готова ініціювати створення в Києві штаб-квартири міжнародного офісу

з протидії дезінформації та пропаганді» [60]. Справжнім інституційним проривом став 2021 р., коли Україна почала формувати власну внутрішню інфраструктуру протидії дезінформації: Центр протидії дезінформації при РНБО та Центр стратегічних комунікацій та інформаційної безпеки при МКІП [49]. Створення цих органів відбувалося у постійних консультаціях з європейськими структурами, що дозволило від самого початку закласти в їхню роботу принципи мережевої взаємодії, притаманні StratCom ЄС. У цей же період Україна стала першою державою-партнером, чий досвід горизонтальної співпраці держави та громадянського суспільства почав інтегруватися у звіти Європейської служби зовнішніх справ як модельна практика для держав-членів [222]. Таким чином, до кінця 2021 р. було сформовано «інституційний місток», який дозволив сторонам розмовляти однією мовою та готуватися до найбільш інтенсивного етапу співпраці [49].

Етап 2022–2026 рр. може бути означений як етап роботи над стратегічною сумісністю задля стійкості в умовах повномасштабної війни. Його зміст полягає у переході від партнерства до повної функціональної та нормативної однорідності принципів протидії дезінформації. Повномасштабне вторгнення 2022 р. зняло будь-які бар'єри у співпраці, перетворивши інформаційний фронт на зону спільної операційної відповідальності. Головним змістом цього етапу є формування Україною нового європейського стандарту «активної оборони» в мережі, що передбачає інтеграцію бойового досвіду OSINT-спільнот та державних центрів у безпекові доктрини ЄС. Сратегічним кроком даного етапу стала розробка у 2024 р. «Дорожньої карти» відновлення медіапростору (Додаток Д), яка заклала алгоритм переходу від воєнних обмежень до європейських стандартів плюралізму та незалежності регулятора [32]. Важливим безпековим якорем стали Спільні безпекові зобов'язання, які офіційно включили FIMI до системи спільних оборонних заходів на десятирічну перспективу [137]. У період 2025–2026 рр. співпраця зосередилася на імплементації DSA, оскільки Україна стала пілотним майданчиком для тестування механізмів відповідальності технологічних гігантів за поширення дестабілізуючого

контенту [218]. Згідно з третім звітом EEAS за березень 2025 р., українські фахівці тепер беруть безпосередню участь у роботі європейських ISAC, забезпечуючи ЄС даними для швидкої атрибуції та запровадження санкцій проти суб'єктів гібридної агресії [331]. Завершення процесу скринінгу у 2025 р. підтвердило, що Україна фактично стала невід'ємним компонентом загальноєвропейської системи інформаційної оборони, трансформувавши свій «польовий» досвід у загальноєвропейські стандарти інформаційної стійкості [187].

Динамічне поглиблення операційної взаємодії та закріплення безпекових гарантій на рівні двосторонніх угод актуалізували потребу у напрацюванні спільного правового підґрунтя співпраці. Логічним наслідком інституційної еволюції став перехід від політичних декларацій до глибокої нормативної синхронізації, що вимагає передусім узгодження понятійно-категоріального апарату, щодо протидії дезінформації. Питання нормативно-правового зближення України та ЄС сьогодні зосереджене на впровадженні дієвих захисних механізмів через гармонізацію визначень. Правова інтеграція України до європейського простору протидії дезінформації сьогодні розглядається як фундаментальна перебудова вітчизняного правового поля на засадах «стійкої демократії» [187]. Ключовим вектором цього процесу є перехід від каральних методів регулювання інформаційного простору до створення прозорих інституційних запобіжників, що відповідають стандартам acquis ЄС та практиці Європейського суду з прав людини.

Наріжним каменем правової реформи стало ухвалення та імплементація Закону України «Про медіа» [47], який дозволив синхронізувати українське законодавство з Директивою про аудіовізуальні медіапослуги (AVMSD) [47]. Правники наголошують, що цей закон запровадив спільні з ЄС правила гри для мовників та вперше на рівні закону визначив критерії обмеження контенту в умовах збройної агресії, забезпечивши правову визначеність, якої бракувало попереднім актам. Це дозволило Національній раді з питань телебачення і радіомовлення отримати статус незалежного регулятора, що є обов'язковою

вимогою для вступу до ЄС та визнається міжнародними експертними групами як успішний кейс інституційної адаптації [187].

Наступним етапом є адаптація стандартів Європейського акту про свободу медіа (EMFA) та Директиви (EU) 2024/1069 щодо захисту журналістів від зловмисних судових процесів (anti-SLAPP) [212]. Новим етапом правової інтеграції у 2025–2026 рр. стало наближення до стандартів DSA [223]. Питання правової відповідальності онлайн-платформ за поширення дестабілізуючого контенту сьогодні є предметом активних дискусій серед українських правників-медіаюристів [50]. Провідні експерти наголошують, що імплементація DSA в Україні дозволить вийти на рівень прямої комунікації з європейськими координаторами цифрових послуг для блокування транскордонних операцій впливу [186].

Згідно з Директивою (EU) 2024/1069, Україна розпочала адаптацію цивільно-процесуального законодавства для захисту журналістів-розслідувачів та громадських активістів від позовів, що мають на меті цензурування публічних дебатів про корупцію чи дезінформацію [221]. Правники зауважують, що створення таких запобіжників є критично важливим для збереження плюралізму медіа, оскільки дезінформація часто використовує судові інструменти для придушення альтернативних джерел інформації [1]. Додатково зауважимо, що тиск на медіа або переслідування журналістів, розслідувачів, лідерів думок з політичних мотивів підриває ефективність протидії дезінформації, бо навіть політична викривальна журналістика може викривати агентів російського впливу.

Нарешті, правова інтеграція охоплює і безпековий вимір через приєднання України до санкційних режимів ЄС щодо іноземних інформаційних маніпуляцій [43]. Спільні безпекові зобов’язання 2024 р. створили правову рамку для спільної атрибуції загроз, що дозволяє українським юридичним висновкам щодо ворожих операцій впливу бути підставою для запровадження обмежувальних заходів на

рівні всієї Спільноти, відтак, правова система України перестає бути локальною і стає частиною колективного механізму захисту верховенства права в Європі.

Механізм протидії дезінформації в Україні еволюціонував до формату цілісної мережевої моделі, яка дзеркально відображає структуру європейських безпекових інституцій. Ключовими у системі стратегічного аналізу став Центр протидії дезінформації при РНБО України, чия діяльність зосереджена на моніторингу та ідентифікації гібридних загроз у реальному часі [68]. Ефективність Центру підтверджується його операційною інтеграцією до RAS, що дозволило лише протягом 2024 р. виявити та передати на рівень європейських спецслужб дані про понад 2500 маніпулятивних кампаній, зокрема таких масштабних операцій, як «Doppelgänger» та «Matryoshka» [67]. Така взаємодія перетворила ЦПД на важливого донора даних для «Гібридного інструментарію ЄС», забезпечуючи ЄС верифікованою інформацією для запровадження санкційних обмежень проти суб'єктів іноземних інформаційних маніпуляцій [68].

Паралельно з безпековим вектором розвивається комунікаційний напрям, представлений Центром стратегічних комунікацій та інформаційної безпеки. Його робота фокусується на розбудові суспільної стійкості через проактивну комунікацію та розвиток медіаграмотності, зокрема через національний проєкт «Фільтр» [50]. У звітах Єврокомісії за 2024 р. цей досвід було відзначено як модельний для країн Східного партнерства, оскільки впровадження методики «пребанкінгу» (випереджального спростування) дозволило значно знизити вразливість цільових аудиторій до дезінформаційних втручань.

Регуляторний контур системи завершує Національна рада з питань телебачення і радіомовлення, яка після ухвалення Закону «Про медіа» [47] трансформувалася у незалежного регулятора з широкими повноваженнями. Отримання Нацрадою статусу спостерігача в Європейській групі регуляторів аудіовізуальних медіапослуг (ERGA) стало актом офіційного визнання українського медіазаконодавства сумісним із правом ЄС [186]. Технічну глибину

цієї інтеграції забезпечує співпраця з ENISA у межах Робочої угоди від 2023 р. [163].

Для того, щоб оцінити перспективи наближення політики протидії дезінформації України до стандартів ЄС потрібно також проаналізувати оцінки в даному питанні. За основу доречно взяти щорічні звіти Єврокомісії. Щорічно вона ухвалює «Пакет розширення», що є фундаментальним набором документів, який окреслює політику ЄС у сфері розширення. Цей пакет включає Повідомлення про розширення, яке підсумовує події минулого року, оцінює прогрес країн-кандидатів та потенційних кандидатів, ідентифікує існуючі виклики та визначає необхідні реформи, пропонуючи шляхи для подальших дій. У них служби Комісії представляють поглиблену оцінку стану реформ у кожній країні за останній рік, супроводжуючи їх конкретними рекомендаціями та пріоритетами для реформування, який дозволяє системно оцінити прогрес зокрема України у сферах, що безпосередньо впливають на інформаційну безпеку та здатність протистояти дезінформації. У звіті детально розглядаються реформи, пов’язані з демократичними інститутами, верховенством права, свободою медіа та цифровою трансформацією. Таким чином, звіт надає офіційний європейський погляд на досягнення України та визначає сфери, що потребують подальших зусиль для повного узгодження з європейськими стандартами у протидії дезінформації.

Зокрема, в звіті за 2023 р. відзначались успіхи в наближенні законодавства України в сфері протидії дезінформації до норм ЄС. Україна значно активізувала співпрацю з ЄС у боротьбі з гібридними загрозами та суттєво покращила свою кібербезпеку [348], а в звіті за 2024 р. аналізуються виклики для свободи Інтернету в Україні в умовах повномасштабної війни. Зазначається, що ці виклики значною мірою є наслідком контрзаходів, яких держава вживає для протидії російським кібератакам, хакерським діям та дезінформаційним кампаніям. У звіті фіксується, що в умовах воєнного стану блокування веб-ресурсів здійснюється Національним центром управління операціями та технологіями телекомунікаційних мереж (НКУ), який керується міркуваннями

національної безпеки. Водночас Єврокомісія наголошує, що такий підхід потребує фундаментального перегляду. У звіті прямо вказано, що обмеження доступу до інтернет-ресурсів повинні регулюватися чіткою правовою базою («належним регулюванням»), яка б відповідала міжнародним стандартам у сфері прав людини, а також acquis ЄС щодо свободи вираження поглядів, захисту даних та права на приватне життя [349].

Підсумовуючи аналіз перспектив наближення української політики протидії дезінформації до стандартів ЄС, варто констатувати перехід від етапу ситуативної взаємодії до фази глибокої нормативної та інституційної сумісності. Протягом 2014–2026 рр. співпраця еволюціонувала від реактивного маркування загроз до створення інтегрованої архітектури колективної стійкості, в якій український «польовий» досвід безпосередньо впливає на формування європейських безпекових доктрин. Цей процес охоплює п’ять ключових рамок: секторальну інтеграцію в межах Єдиного цифрового ринку, оперативний обмін даними через RAS та ENISA та спільні безпекові гарантії у сфері протидії іноземним маніпуляціям FIMI. Важливою теоретичною та практичною особливістю європейського підходу, яку переймає Україна, є свідома відмова від жорсткого юридичного визначення поняття «дезінформація» у первинному законодавстві. Така стратегічна невизначеність не є правовою прогалиною, а виступає розумним кроком задля захисту свободи слова та уникнення ризиків державної цензури. Замість статичних дефініцій, які можуть бути використані для придушення легітимної політичної критики, фокус зміщується на поведінковий аспект FIMI, що дозволяє кваліфікувати діяльність ворожих акторів не за змістом їхніх думок, а за зловмисними методами маніпулювання алгоритмами, прихованим фінансуванням та намірами. Це забезпечує необхідну правову гнучкість в умовах швидкої технологічної еволюції гібридних загроз. Інституційний контур цієї інтеграції базується на діяльності Центру протидії дезінформації та Центру стратегічних комунікацій, які стали важливими донорами даних для «Гібридного інструментарію» ЄС. Регуляторна сумісність забезпечується через Нацраду з питань телебачення і радіомовлення, що

отримала статус спостерігача в ERGA, та незалежне Суспільне мовлення, яке відповідає стандартам EBU. Водночас подальший поступ потребує вирішення низки критичних завдань: забезпечення реальної фінансової незалежності медіарегулятора та Суспільного мовника, імплементація дієвих анти-SLAPP механізмів для захисту журналістів-розслідувачів та поступовий перехід від воєнних обмежень, як-от телемарафон чи блокування інтернет-ресурсів без належного регулювання, до прозорих процедур, що відповідають міжнародним стандартам прав людини. Успішна реалізація цих рекомендацій дозволить Україні остаточно закріпитися в статусі невід'ємного елементу загальноєвропейської безпекової системи.

Висновки до розділу 2

Механізм політики протидії дезінформації в ЄС може бути охарактеризований як багаторівнева та інтегрована система, що поєднує нормативні, інституційні, комунікаційні та освітні інструменти. Його сутність полягає у створенні комплексної моделі співрегулювання, в якій державні інституції, цифрові платформи, медіа-індустрія та громадянське суспільство взаємодіють у межах узгоджених принципів і процедур. Важливим елементом цього механізму є нормативна база, яка включає Спільний план дій проти дезінформації 2018 р., План дій щодо європейської демократії 2020 р., Кодекс практики ЄС щодо дезінформації у його первинній та оновленій редакціях, а також DSA. Ці документи визначають правові та політичні рамки, що регулюють діяльність цифрових платформ, забезпечують прозорість політичної реклами, встановлюють механізми моніторингу та підзвітності, а також закріплюють обов'язки щодо управління системними ризиками, пов'язаними з поширенням неправдивої інформації.

Інституційний вимір механізму охоплює діяльність Єврокомісії, Європейської служби зовнішніх справ, стратегічних комунікаційних підрозділів та спеціалізованих структур, які здійснюють моніторинг інформаційного простору, координують дії держав-членів та забезпечують взаємодію з

міжнародними партнерами. Комунікаційний компонент механізму полягає у розвитку співпраці між платформами та незалежними фактчекінговими організаціями, створенні системи швидкого оповіщення для обміну інформацією між державами-членами, а також у забезпеченні доступу дослідників до даних платформ для аналізу масштабів і впливу дезінформації. Таким чином, механізм політики протидії дезінформації в ЄС можна охарактеризувати як системну модель, що поєднує правові норми, інституційні структури, інструменти співрегулювання та освітні заходи. Разом з тим національні механізми протидії дезінформації до певної мір, будучи частиною європейського механізму, функціонують автономно.

Перспективи гармонізації національних моделей протидії дезінформації держав-членів ЄС значною мірою визначаються прагненням ЄС утвердити уніфіковані принципи цифрової відповідальності, інформаційної прозорості та демократичної стійкості. Упродовж останнього десятиліття ЄС перейшов від декларативного до нормативно зобов'язального підходу, формуючи не лише інституційні рамки, а й політичні очікування щодо того, якою має бути модель протидії інформаційним загрозам у межах спільного європейського простору. Національні держави, зокрема Франція та Німеччина, уже сьогодні демонструють прагнення синхронізувати свої законодавчі та інституційні підходи відповідно до європейських рамок. Це виявляється у впровадженні принципів прозорості цифрових платформ, відповідальності за політичну рекламу, обов'язковості звітності щодо модерації контенту та кооперації з незалежними фактчекінговими структурами. Проте ці процеси не відбуваються одноманітно: існує суттєвий розрив між північноєвропейськими, західноєвропейськими і східноєвропейськими країнами як за рівнем інституційної готовності, так і за культурою інформаційної безпеки. У низці держав превалює реактивний підхід до дезінформації, що суперечить базовим стандартам свободи слова та може посилювати недовіру до владних інститутів. З іншого боку, наявність спільного правового поля створює умови для формування вертикальної інтеграції між національними й наднаціональними

рівнями. Поступово формується архітектура європейської інформаційної стійкості, в якій кожна держава має свої обов'язки та інструменти для координації, обміну найкращими практиками та уніфікованого моніторингу. Однак цей процес стикається з низкою обмежень: по-перше, відсутність чітко визначеного поняття дезінформації в правовому полі ЄС залишає місце для національних тлумачень, що може використовуватись як для захисту демократії, так і для її обмеження; по-друге, культурно-політичні відмінності між державами-членами зумовлюють різну межу терпимості до контроверсійного або альтернативного контенту.

У перспективі найбільш імовірною є модель часткової уніфікації, коли загальні зобов'язання щодо платформ, прозорості, фактчекінгу, виборчої інформації будуть імплементовані на всій території ЄС, але збережеться гнучкість у механізмах реалізації та політичних інтерпретаціях. Тому ключовим завданням найближчих років технічне забезпечення функціональності спільного підходу та політичне укорінення ідеї, що боротьба з дезінформацією є не інструментом контролю інформаційних потоків, а механізмом захисту довіри, відкритості та демократичної легітимності.

РОЗДІЛ 3
БЕЗПЕКОВІ ІНСТРУМЕНТИ РЕАЛІЗАЦІЇ ЄВРОПЕЙСЬКОЇ ПОЛІТИКИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

3.1. Стратегічні комунікації як інструмент реалізації політики протидії дезінформації

Сучасний етап розвитку міжнародних відносин характеризується фундаментальною трансформацією природи конфліктів, що вимагає перегляду базових підходів до безпеки. Ми підтримуємо позицію українських дослідників, що війна в XXI ст. починається не з кінетичних ударів, а зі змін у свідомості. Сучасні гібридні конфлікти експлуатують психологічні механізми страху, невизначеності та дезорієнтації, перетворюючи інформаційний простір з нейтрального середовища передачі даних на оперативний простір бойових дій. Відтак, комунікаційна діяльність державних та наднаціональних інституцій перестає бути суто допоміжною функцією зв'язків з громадськістю і трансформується у стратегічні комунікації. Як свідчить сучасна практика гібридних протистоянь, відсутність активної позиції та дієвої підтримки суспільства з боку наднаціональних структур (наприклад, ЄС) створює вакуум, який агресор швидко використовує для повернення держав-цілей у свою геополітичну орбіту [42, с. 137]. Саме тому в європейському безпековому дискурсі відбувся зсув у розумінні інформаційних загроз та ролі стратегічних комунікацій у протидії такому виду загроз. Проблема дезінформація почала маркуватися як маніпуляція інформацією та втручання з боку іноземних акторів (FIMI). Ця позиція, закріплена у стратегічних документах ЄС, вказує, що загрозою є не просто неправдивий контент, а скоординована діяльність інших держав чи політичних акторів, що становить пряму небезпеку національній безпеці та демократичним інститутам ЄС та державам-членам [155, p. 14, 201].

На відміну від традиційного інформування, стратегічні комунікації передбачають синхронізацію меседжів та дій з метою досягнення довгострокових безпекових цілей. До певної міри стратегічні комунікації є

проєкцією м’якої сили, що має чітко визначений оборонний характер, метою якого є захист інформаційного суверенітету держави (об’єднання держав) та просування власних наративів у середовищі противника. Для ЄС точкою біфуркації та поштовхом до інституціоналізації цієї сфери стала агресія Росії проти України у 2014 р. Відтак у грудні 2014 р. Комісар ЄС з питань європейської політики сусідства Й. Ган публічно заявив про «посилені комунікаційні зусилля» з боку Росії [239], спрямовані проти європейської демократії. Обмежена здатність інструментів класичної дипломатії ефективно протистояти масованим дезінформаційним атакам спричинила створення спеціалізованої інфраструктури протидії дезінформації. Інституційним ядром цього механізму стала Європейська служба зовнішніх справ (EEAS), в структурі якої була сформована Оперативна робоча група зі стратегічних комунікацій (StratCom Task Forces) [189, p. 5]. Важливо, що створення StratCom як одного з безпекових інструментів ЄС було внутрішньою потребою європейської системи безпеки, що знайшла вираження у політичній волі європейського політикуму, зафіксованій у висновках засідання Європейської Ради 19–20 березня 2015 р. [189].

Створення StratCom можна означити як період функціональної адаптації ЄС до умов гібридної війни. Тогочасний Президент Європейської Ради Д. Туск та Висока представниця ЄС із питань закордонних справ і політики безпеки Ф. Могеріні виступили каталізаторами цього процесу, адже саме їхня ініціатива щодо створення спеціалізованої групи протидії дезінформаційним кампаніям Російської Федерації стала відображенням спільного інтересу держав-членів ЄС до вироблення спільної реакції на зовнішні виклики та проявом «spillover»-ефекту, коли потреба у безпеці та захисті інформаційного простору стимулює поглиблення співпраці на рівні інституцій ЄС. Дискусії між групою радикально налаштованих держав (держави Балтії, Польща, Велика Британія) та більш поміркованим державами (Німеччина, Франція) відображають класичний конфлікт між функціональною необхідністю та політичною обережністю. Вимога жорсткої протидії дезінформації (держави Балтії, Польща, Велика Британія) демонструвала прагнення до посилення наднаціональних механізмів,

тоді як обережна позиція Німеччини та Франції в інституціоналізації стратегічних комунікацій ЄС відображала певну залежність від російських ресурсів, що стримувало швидке ухвалення політичних рішень [354, p. 4-6]. Проте саме ця напруга у неофункціоналізмі розглядається як рушійна сила: економічні інтереси та політичні цінності вступають у взаємодію, створюючи нові сфери компетенцій для ЄС. Тому процес вироблення відповіді на російську дезінформацію не можна розглядати як балансування між вигодою та безпекою, оскільки створення StratCom відображає інституціоналізацію нового безпекового інструменту, призначеного для координації стратегій протидії дезінформації держав-членів ЄС.

Предметом дискусії були і принципи функціонування StratCom. Радикальний підхід передбачав створення «інституту контрпропаганди», який мав би спростовувати кожен факт дезінформації у режимі реального часу. Однак, з огляду на ціннісні орієнтири ЄС, була обрана модель м'якого стратегічного наративу, що опиралася на три принципи: по-перше, формування сталої системи ефективної комунікаційної політики ЄС у регіоні Східного партнерства; по-друге, підтримці незалежного медіасередовища в ЄС та регіоні Східного партнерства; по-третє, підвищенні рівня медіаграмотності у громадян ЄС та держав Східного партнерства [205, p. 2-3]. Такий підхід дозволяв зберігати баланс між безпековими функціями StratCom та відданістю принципам свободи слова, уникаючи перетворення дипломатичних інституцій на «інститут контрпропаганди».

Практичне застосування StratCom як безпекового інструменту було розпочато у квітні 2015 р. у форматі East StratCom Task Force (ESTF) та супроводжувалося організаційними та фінансовими складнощами, оскільки діяльність ESTF не була забезпечена окремим бюджетним забезпеченням, а персонал складався переважно з відряджених національних експертів держав-членів ЄС, які мати тимчасовий статус [213]. Брак ресурсів змушував команду зосереджуватися на вузьких пріоритетах, що викликало критику з боку Європейського Парламенту. Депутати неодноразово вказували на те, що

протидія політиці російської дезінформації силами 15 експертів без належного фінансування є суто символічним кроком [100, p. 5], що можна оцінювати як відображення інституційної напруги між формальними структурами та очікуваннями політичних акторів. Тільки в 2018 р. ситуація почала змінюватися у бік системної інституціоналізації та виділення мільйонних грантів на розвиток верифікаційних платформ [184], що стало свідченням інституціоналізації ESTF через формалізацію ресурсів, створення процедур та розширення компетенцій.

Мандат ESTF є одночасно проактивним та реактивним. Проактивний аспект полягає у посиленні комунікацій ЄС у країнах Східного партнерства (Вірменія, Азербайджан, Білорусь (членство призупинене), Грузія, Молдова, Україна) з метою підтримки демократичних реформ та їх європейського вибору. Реактивний аспект мандату передбачає спрямованість на виявлення, аналіз та викриття російських дезінформаційних наративів. Реактивний аспект мандату ESTF конкретизований в діяльності проєкту EUvsDisinfo, що станом на 15 січня 2026 р. виявив та спростував 19592 фактів дезінформації [225]. Це єдина структура ЄС, яка має мандат прямо називати Росію джерелом загрози.

Функціонування ESTF як вузькоспеціалізованої групи східного спрямування поклало початок формуванню більш складної моделі даного безпекового інструменту [100] та створення інших регіональних підрозділів StratCom, що стало логічним завершенням процесу інституційного закріплення та розширення компетенцій м’якої моделі стратегічних комунікацій ЄС. Аналогічні робочі групи були створені для Західних Балкан (Western Balkans Task Force, WBTF) та країн Магрибу та Близького Сходу (South StratCom Task Force, SSTF) [206]. Така розгалужена структура дозволила ЄС закривати «сірі зони» в інформаційному просторі на своїх кордонах, перетворивши StratCom із тимчасової робочої групи на постійний та багатовекторний інструмент протидії зовнішнім інформаційним загрозам, що формує нові правила споживання інформації, закріплює очікування та створює довготривалі рамки для політики протидії дезінформації.

Формування SSTF було зумовлене необхідністю реагувати на інформаційні кампанії ісламського радикалізму та діяльність терористичних угруповань, зокрема ІДІЛ, що створювали загрозу стабільності та безпеці в регіоні Близького Сходу та Північної Африки (MENA). Важливим є те, що ця структура від самого початку набула статусу інструменту безпеки в системі європейського механізму протидії дезінформації, який поступово набував легітимності через практику протидії наративам, що розпалювали ненависть та антизахідні настрої в арабському світі [199]. Згодом мандат групи розширився, охопивши протидію російському та китайському впливу в Африці, де ці країни активно використовували чутливі антиколоніальні наративи для дискредитації європейської присутності. Така трансформація свідчить про інституційну здатність до адаптації та розширення компетенцій. SSTF не залишилася обмеженою первинним завданням, а поступово інтегрувала нові функції, закріплюючи свою роль у ширшій архітектурі інформаційної безпеки ЄС. Важливим аспектом стало використання арабської мови та адаптація меседжів ЄС до культурного контексту регіону, що вказує на сталу інституційну практику врахування локальних норм та очікувань, без чого неможливе закріплення легітимності контрдезінформаційних меседжів [209, p. 8].

WBTF був створений для комунікаційної взаємодії з державами-кандидатами та потенційними кандидатами на вступ до ЄС, серед яких Албанія, Боснія і Герцеговина, Косово, Чорногорія, Північна Македонія та Сербія. Його стратегічна мета полягала у підтримці процесу розширення ЄС, що має особливе значення для регіону, який історично був джерелом нестабільності та конфліктів. Балкани є тим політичним простором, де перетинаються інтереси ЄС, Російської Федерації, Китаю та Туреччини, що створює ґрунт для одночасної циркуляції варіативних наративів щодо змісту та сутності європейської інтеграції. Особливої уваги заслуговує Сербія, яка завдяки традиційно сильним проросійським настроям стала головним майданчиком поширення антизахідних наративів у регіоні. Високий рівень довіри громадян до РФ та активна діяльність локальних підрозділів російських державних медіа, зокрема «Sputnik»,

перетворили Сербію на інформаційний хаб, що ретранслює кремлівські меседжі на сусідні Боснію і Герцеговину та Чорногорію [101]. Це змусило інституції ЄС посилити роботу WBTF, зосередивши увагу на викритті маніпуляцій, які опираються на спільну історичну пам'ять та релігійну ідентичність для дискредитації європейського курсу регіону [214]. Група протидіє наративам, що ставлять під сумнів надійність ЄС як партнера, зокрема концепції «втоми від розширення», а також тим, що роздмухують міжетнічну напругу. Важливою особливістю діяльності є тісна співпраця з місцевими фактчекерами, які забезпечують захист демократичних інститутів регіону та сприяють формуванню довіри до європейських структур [324].

Таким чином, ESTF, WBTF та SSTF мають спільну риси: (1) всі вони є інституційними інструментами ЄС, створеними для протидії дезінформації засобами стратегічних комунікацій; (2) їхня діяльність спрямована на захист інформаційного простору, формування довіри до європейських інституцій та нейтралізацію зовнішніх впливів, які використовують маніпулятивні наративи для підриву стабільності; (4) вони працюють із локальними контекстами, адаптуючи меседжі ЄС до культурних, мовних та політичних особливостей регіонів; (4) зазнали процесу поступової інституціоналізації, який розгортався від тимчасових форматів до стійких алгоритмів, які стали невід'ємною частиною європейського механізму протидії дезінформації. Відмінність між ESTF, WBTF та SSTF полягає у специфіці регіональних викликів та пріоритетів (Малюнок 3.1.1), зокрема ESTF була створена як відповідь на масштабні дезінформаційні кампанії Росії, що мали на меті дискредитацію ЄС та підрив довіри до європейських інституцій в умовах гібридної війни, розпочатої Росією проти України. Її головним завданням стало викриття кремлівських наративів та формування системи інформаційного захисту на східному напрямку. Діяльність SSTF спрямована проти інформаційних кампаній ісламського радикалізму та діяльності ІДІЛ, відтак, зосереджена на боротьбі з наративами ненависті та антизахідними настроями у країнах Близького Сходу та Північної Африки, зокрема й тими, що генеруються Росією та Китаєм. WBTF мало іншу стратегічну

мету, спрямовану на формування сталої підтримки процесу розширення ЄС у регіоні, який історично був джерелом нестабільності.

Малюнок 3.1.1. Спрямованість діяльності ESTF, WBTF та SSTF

Дані Малюнку 3.1.1 дозволяють стверджувати, що спільним для всіх трьох груп є їхня роль у формуванні архітектури стратегічних комунікацій ЄС як інструменту протидії дезінформації, тоді як відмінності визначаються конкретними регіональними викликами: російська пропаганда на сході, радикальні ісламістські та антиколоніальні наративи на півдні, проросійські інформаційні впливи та міжетнічна напруга на Балканах. Це вказує на багатовекторність європейської політики протидії дезінформації та варіативність засобів діяльності, в яких відображена проактивний та реактивний статус їх мандату.

Обмежуючим фактором ефективності функціонування ESTF, WBTF та SSTF в реалізації європейської комунікаційної політики у сфері протидії дезінформації є дефіцит ресурсів. Попри те, що після 2022 р. інституції ЄС здійснили суттєвий перегляд фінансових пріоритетів, асиметрія можливостей у порівнянні з агресором лише посилилася. Якщо у 2021 р. бюджет Відділу стратегічних комунікацій Європейської служби зовнішніх справ становив

близько 11,1 млн євро, то вже у 2023 р. операційне фінансування заходів з протидії дезінформації було збільшено до 15,4 млн євро [211]. Однак навіть ці показники залишаються неспівмірними з фінансовими можливостями Російської Федерації. Згідно зі звітами про виконання російського бюджету, у 2022 р. витрати на державні медіа, позначені як «масові комунікації», зросли на рекордні 40 %, досягнувши 143 млрд рублів, що еквівалентно приблизно 1,9 млрд доларів США [350]. Це означає, що на кожен євро, витрачений ЄС на стратегічні комунікації, Росія інвестує понад 100 євро у реалізацію політики дезінформації. Європейський суд аудиторів у спеціальному звіті №09/2021 наголосив, що заходи ЄС залишаються фрагментарними, а сама проблема дезінформації є «tackled, but not tamed» (під контролем, але не приборкана). Аудитори підкреслили, що без чіткої фінансової стратегії та збільшення кадрового потенціалу оперативних груп зусилля ЄС ризикують залишитися радше символічними, ніж дієвими, особливо на тлі динамічної еволюції гібридних загроз, які потребують системної та масштабної відповіді [191].

Важливим аспектом, що визначає ефективність функціонування ESTF, WBTF та SSTF є розв’язання правової та етичної дилеми визначення межі між боротьбою з дезінформацією та дотриманням фундаментального права на свободу вираження поглядів. Для демократичної європейської спільноти створення механізмів блокування контенту без ризику перетворення їх на інструменти цензури є питанням політичної легітимності. Забезпечення безпеки інформаційного простору в демократичному суспільстві не може здійснюватися ціною відмови від засадничих ліберальних цінностей. Головна складність полягає у визначенні критеріїв пропорційності: де закінчується необхідний захист від деструктивного зовнішнього впливу і де починається цензура, що підриває довіру громадян до державних інституцій. Легітимність стратегічних комунікацій ЄС прямо залежить від здатності інституцій діяти в межах правового поля, що виключає довільне обмеження свободи слова [70, с. 37–38]. Важливим кроком у вирішенні цієї проблеми стало впровадження концепції Foreign Information Manipulation and Interference (FIMI), яка змістила фокус

аналізу в протидії дезінформації з оцінки змісту повідомлень (суперечливий підхід «правда проти брехні») на виявлення маніпулятивної та скоординованої діяльності іноземних акторів. Такий підхід базується на принципі «аналізу методів, а не меседжів», що дозволяє ідентифікувати втручання за технічними ознаками (використання бот-мереж, штучне посилення наративів, приховане фінансування), не втручаючись у суть політичної дискусії [199]. Проте на практиці зберігаються «сірі зони», де зовнішнє втручання тісно переплітається з внутрішнім політичним дискурсом. Прикладом такої «сірої зони» є протести аграріїв у країнах ЄС (зокрема у Польщі та Німеччині) у 2023–2024 роках [151; 352]. У цьому кейсі автентичне незадоволення фермерів економічною політикою (внутрішній дискурс) було штучно посилене зовнішніми акторами через цифрову інфраструктуру маніпуляцій. Використання бот-мереж для масштабування антиукраїнських закликів та дискредитації «Зеленого курсу» ЄС створило ситуацію, коли технічне припинення маніпулятивної діяльності ризикує бути інтерпретованим як обмеження законного права громадян на протест та вільне висловлення думок [109; 203]. Оскільки іноземні актори часто використовують реальні внутрішні суперечності європейських суспільств для їх посилення, відокремити автентичну критику дій інститутів влади чи політичних рішень від скоординованої операції впливу залишається надскладним завданням [180]. Це створює постійні ризики для дотримання європейського принципу організації політичної діяльності – політичного плюралізму, оскільки будь-яка спроба обмеження таких гібридних наративів може бути інтерпретована як тиск на свободу висловлювання, діяльність політичної опозицій або обмеження демократичних дебатів [215].

Перешкодою для формування єдиного безпекового периметра ЄС засобами протидії дезінформації є інституційна асиметрія та фрагментація підходів до означеної правової та етичної дилеми на рівні держав-членів ЄС. Аналіз показує чіткий поділ на дві основні моделі реагування. Країни Балтії, Польща та Скандинавські держави інтегрували стратегічні комунікації у систему «тотальної оборони» (Total Defence), в якій протидія дезінформації

розглядається як невід'ємний елемент національної стійкості, а координація між військовими, спецслужбами, медіа та громадянським суспільством створює комплексний механізм захисту [398, p. 10, 34–36]. Такий підхід, однак, ставить питання про ризик надмірного втручання держави у сферу свободи слова, адже межа між захистом інформаційного простору та обмеженням права на вільне висловлення може бути розмитою. Натомість низка держав Західної та Південної Європи (Італія, Іспанія, Греція, Португалія, Бельгія) продовжує дотримуватися традиційних, суто регуляторних моделей, в якій боротьба з маніпуляціями покладається переважно на медіарегулятори та незалежні ради з етики [191]. Цей варіант виглядає більш обережним у правовому сенсі, адже намагається уникати прямого втручання держави у комунікаційний простір, проте водночас створює безпекові прогалини, які гібридні актори активно використовують для транскордонних операцій впливу, таргетуючи найбільш вразливі сегменти європейського інформаційного простору. Така ситуація породжує ефект «клапттикової ковдри» інформаційної безпеки ЄС, що відображає небезпеки відсутніості уніфікованих етичних та правових стандартів, створюваних відсутністю нормативно-правового визначення дезінформації на рівні ЄС. Це дозволяє противнику використовувати правові та організаційні відмінності між країнами для легітимізації дезінформаційних наративів у межах всього ЄС, маскуючи зовнішнє втручання під локальний політичний дискурс [191]. У цьому контексті дилема свободи вираження поглядів та боротьби з дезінформацією стає центральною: надмірна регуляція може поставити під загрозу демократичні принципи, тоді як недостатня координація відкриває шлях для масштабних інформаційних атак. На нашу думку, визначення моделі балансу між цими двома вимірами впливатиме на легітимність та ефективність європейських стратегічних комунікацій як інструменту протидії дезінформації, що здійснюється ESTF, WBTF та SSTF.

Розуміючи потребу розгортання більш оперативних стратегічних комунікацій в протидії дезінформаційним загрозам, в ЄС був запущений закритий механізм оперативної координації Система швидкого сповіщення

(Rapid Alert System, RAS) [171]. Цей інструмент стратегічних комунікацій був створений у березні 2019 р. в рамках імплементації Плану дій проти дезінформації, що стало відповіддю на необхідність забезпечення більшої узгодженості між державами-членами ЄС у сфері інформаційної безпеки. RAS функціонує як захищена цифрова платформа, яка об'єднує контактні точки у всіх 27 державах-членах ЄС, а також в його інституціях, включно з Єврокомісією та EEAS. Його створення мало на меті подолати проблему фрагментації та асиметрії підходів, забезпечивши можливість оперативного обміну інформацією про дезінформаційні кампанії, їхні джерела та методи поширення (Додаток Ж). У цьому контексті RAS виступає субінструмент стратегічних комунікацій, що уможливив формування нових стандартів взаємодії між державами-членами та міжнародними партнерами, створюючи основу для колективної стійкості до гібридних загроз. Його закритий характер дозволив поєднати потребу у швидкому реагуванні з гарантіями конфіденційності, що є критично важливим для збереження довіри між учасниками та ефективності спільних дій у сфері протидії дезінформації.

Оскільки ключова мета RAS полягає у забезпеченні обміну даними про дезінформаційні кампанії в режимі реального часу, створюючи «situational awareness» для всіх учасників, алгоритм його діяльності досить простий (Малюнок 3.1.2, складено автором).

Малюнок 3.1.2. Алгоритм RAS

На відміну від відкритої бази даних EUvsDisinfo, RAS надає можливість урядам поширювати непублічну інформацію про методи розповсюдження дезінформації, координовану неавтентичну поведінку ботоферм та здійснювати атрибуцію атак до конкретних іноземних акторів. Це дозволяє державам-членам

ЄС переходити від ізольованого реагування до колективної відповіді, що значно підвищує рівень стійкості інформаційного простору. Наприклад, якщо російська інформаційна операція фіксується у Литві, завдяки RAS про неї миттєво отримують повідомлення в Іспанії, що створює можливість превентивно «вакцинувати» іспанський інформаційний простір ще до того, як відповідний наратив набуде вірусного поширення [269]. Такий алгоритм RAS вказує, що стратегічні комунікації ЄС опираються на адекватне ситуації застосування реактивних та проактивних протоколів протидії дезінформації.

Після початку повномасштабної агресії Росії проти України у 2022 р., функціонал RAS зазнав суттєвого розширення та набув статусу основного каналу координації у сфері стратегічних комунікацій та реалізації санкційної політики проти російських пропагандистських медіа, таких як RT та Sputnik. Система стала платформою для обміну доказами їхньої деструктивної діяльності, що дозволило інституціям ЄС оперативно узгоджувати заходи у відповідь та забезпечувати правову легітимність обмежувальних рішень. Важливим нововведенням стало відкриття спеціальних каналів комунікації в рамках RAS для партнерів, зокрема для України. Це надало можливість українському Центру стратегічних комунікацій у режимі реального часу передавати європейським колегам дані про нові російські інформаційні операції безпосередньо з епіцентру подій [207]. Така інтеграція посилила ефективність реагування ЄС та продемонструвала новий рівень інституційної взаємодії між ЄС та Україною як державою-кандидатом, на якому обмін інформацією став основою для посилення стійкості до інформаційних загроз в умовах гібридної війни.

Для оцінки ефективності інструментів протидії дезінформації в ЄС актуальним є питання вироблення універсальних показників ефективності стратегічних комунікацій. У сучасних практиках, що реалізуються ЄС в межах та засобами стратегічних комунікацій, домінують кількісні індикатори, що пов’язано з можливістю підрахунку кількості викритих дезінформаційних повідомлень у базі EUvsDisinfo (Додаток З) [225] чи охоплення постів у

соціальних мережах, проте надзвичайно складно оцінити реальний вплив цих спростувань на когнітивні установки та поведінкові патерни аудиторії [191]. Це вказує на необхідність вироблення інструментів вимірювання розриву між «виходом» (output), тобто кількістю виробленого контенту, що спростовує дезінформацію засобами наративів стратегічних комунікацій ЄС та «результатом» (outcome), тобто зміною рівня стійкості громадян ЄС, спільнот та держав-членів до дезінформаційних наративів. У науковій спільноті тривають гострі дискусії щодо доцільності класичного спростування (debunking) дезінформації, адже є ризики виникнення ефекту «зворотного удару» (backfire effect) дезінформації, коли її публічне викриття призводить до парадоксальних наслідків: повторення дезінформаційного наративу під час його спростування лише посилює його «знайомість» та запам’ятовуваність у свідомості громадян (familiarity backfire effect) [125, p. 1541]. Тобто, аудиторія може краще запам’ятати саму дезінформацію, ніж її спростування інструментами стратегічних комунікацій, особливо якщо вона відповідає внутрішнім установкам чи упередженням. Це створює складне завдання для стратегічних комунікацій ЄС, що полягає у виробленні моделі реактивної комунікації, не перетворюючись на ретранслятора дезінформаційних наративів і водночас, не порушуючи право на свободу вираження поглядів. Експерти схиляються до того, що спростування має бути максимально лаконічним, фокусуватися на фактах і супроводжуватися візуалізацією, яка заміщує дезінформаційну картинку у пам’яті аудиторії, проте впровадження таких стандартів в діяльність ESTF, WBTF та SSTF все ще триває.

На нашу думку, технічне (кількісне) викриття дезінформації є лише однією складовою моделі протидії дезінформації. Ефективність стратегічних комунікацій ЄС в умовах гібридної війни визначається змістовим виміром, оскільки критично важливим стає поряд із спростуванням неправдивих повідомлень, формування власного наративу, здатного конкурувати з дезінформацією та перемагати її. Українська дослідниця Н. Карпчук окреслює цей процес як перехід до політики «стратегічного наративу», підкреслюючи, що

ЄС прагне вибудувати єдину публічну сферу, в якій комунікація одночасно виконує функції просування позитивного іміджу євроінтеграції та захисту ціннісних основ ЄС від зовнішніх автократичних моделей. Ефективність цього механізму залежить від здатності ЄС вести діалог зрозумілою мовою, застосовуючи стратегію «позитивного сторітелінгу», яка передбачає заповнення інформаційного вакууму власним порядком денним, заснованим на демократичних принципах, замість постійного реагування на атаки агресора [26. с. 38–39]. Такий підхід дозволяє нейтралізувати деструктивні наративи, зміцнювати довіру до європейських інституцій, формуючи стійкість європейського політичного поля до маніпуляцій.

Згідно зі звітами EEAS про загрози маніпулювання інформацією [199; 201; 202; 203; 204; 209], російська політика дезінформації реалізується не хаотично, а просуває чітко структуровані майстер-наративи, які ретельно адаптовані до проблем ЄС. Це означає, що ефективність стратегічних комунікацій залежить від здатності зрозуміти системну логіку їхнього створення і поширення та інтегрувати стратегічний наратив ЄС в проактивні стратегії протидії дезінформації. Аналіз результатів діяльності StratCom [200; 209] дозволив виокремити три ключові вектори атак, на нейтралізацію яких спрямовані зусилля ЄС, і саме ця спрямованість визначає вектори розгортання «позитивного сторітелінгу» з метою посилення стійкості ЄС до дезінформації.

Перший вектор дезінформаційних атак, який став особливо потужним у 2022–2023 рр., був пов’язаний із темою енергетичного шантажу та соціально-економічного колапсу. Центральний наратив будувався на тезі «Європа замерзне без Росії», що мало на меті створити атмосферу паніки серед населення ЄС, спровокувати соціальні протести та посилити тиск на уряди з вимогою зняти санкції [111]. У цьому контексті ефективність стратегічних комунікацій ЄС проявилася у здатності перетворити ворожий наратив на інструмент власного «позитивного сторітелінгу». Єврокомісія винесла в публічне поле фактичні дані про заповнені газосховища та диверсифікацію поставок, що трансформувало російські прогнози у маркер некомпетентності кремлівських стратегів. Такий

підхід показав, що проактивні стратегічні комунікації, формуючи позитивний порядок денний, зміцнюють довіру до європейських інституцій та підвищує стійкість суспільства до маніпуляцій.

Показовим є й феномен публікацій Президента США Дональда Трампа у соціальній мережі «Х», в якій він «радив» Україні приймати ультимативні вимоги мирного плану, аргументуючи це тим, що «ця зима буде холодною» [62]. Хоча подібні заяви західних лідерів, які дисонують із загальною риторикою підтримки України, проти якої здійснюється агресія, є предметом окремого політологічного аналізу, цей кейс яскраво ілюструє небезпеку «дружнього вогню» в інформаційному просторі. Подібні висловлювання, навіть якщо вони продиктовані внутрішньополітичною логікою, можуть резонувати з російськими наративами про енергетичну вразливість, ускладнюючи реалізацію скоординованої комунікаційної політики ЄС. Саме тому розгортання «позитивного сторітелінгу» стає ключовим інструментом, оскільки дозволяє посилювати власні наративи, що базуються на демократичних цінностях, солідарності та довгостроковій стратегії стійкості.

Другий вектор дезінформаційних атак був спрямований на дискредитацію санкційної політики ЄС, що отримав назву «ефект бумеранга». Основний наратив будувався на твердженнях про те, що «санкції не працюють» або «шкодять ЄС більше, ніж Росії» [110]. Агресор активно використовував маніпулятивну статистику та окремі голоси євроскептиків для просування ідеї про марність економічного тиску, намагаючись підірвати довіру до європейських інституцій та створити відчуття внутрішньої слабкості. У відповідь стратегічні комунікації ЄС розгорнули кампанію, яка стала прикладом розгортання «позитивного сторітелінгу». Замість того щоб постійно виправдовуватися перед критиками, ЄС змістив акцент із миттєвих ефектів на довгострокові результати, пояснюючи суспільству, як санкції поступово підривають російський військово-промисловий комплекс та економіку загалом [17]. Такий підхід дозволив перетворити негативний наратив на позитивний порядок денний, коли санкції подаються не як тягар для ЄС, а як стратегічний

інструмент протидії агресору та захисту демократичних цінностей. Отже, «позитивний сторітелінг» виконує функцію інформаційної відповіді та формування стійкості європейців через стратегічні наративи, які консолідують громадян навколо ідеї довготривалої безпеки та солідарності.

Третій вектор дезінформаційних атак, який має найбільш небезпечний довгостроковий характер, пов'язаний із формуванням наративу «Втома від України» та дискредитацією біженців. Його стратегічна мета полягає у поступовій ерозії солідарності всередині ЄС. Цей наратив включає поширення дезінформації про «невдячних біженців», «тотальну корупцію в Києві», «розпродаж західної зброї на чорному ринку» та твердження про те, що «війна затягується через допомогу Заходу» [66]. За даними першого звіту EEAS про FIMI, Україна та її представники стали мішенню у понад 50% усіх проаналізованих випадків інформаційних маніпуляцій у світі, що свідчить про системність і масштабність цього вектору атак [203]. У відповідь стратегічні комунікації ЄС мають розгортати «позитивний сторітелінг», який полягає у постійній демонстрації успіхів українського опору та чіткому поясненні прямого зв'язку між європейською допомогою і безпекою самих європейців. Окремим викликом для інформаційної безпеки є використання політичними лідерами агресивної, емоційно забарвленої риторики, яка може мати ознаки деструктивного впливу на стратегічне партнерство ЄС, США та України. Яскравим прикладом є заяви Президента США Д. Трампа щодо примусу України до мирних переговорів, які містять елементи ультимативності та публічного тиску [61]. Подібні меседжі, тиражовані медіа, можуть бути використані ворожою пропагандою як доказ «втоми» партнерів або відсутності суб'єктності України. Це не відповідає принципам скоординованих стратегічних комунікацій ЄС і створює додаткові ризики для європейської інформаційної стійкості. Саме тому розгортання «позитивного сторітелінгу» ЄС є важливим засобом демонстрації єдності та закріплення легітимності європейського курсу в умовах гібридної війни.

Узагальнюючи проведений аналіз, можна зробити висновок, що стратегічні комунікації ЄС у період 2014–2026 рр. перетворилися з допоміжного інструменту публічного інформування на безпековий інструмент реалізації політики протидії дезінформації. Цей процес супроводжувався зміною розуміння природи загрози та предмету протидії: від боротьби з окремими «фейковими новинами» до системної протидії іноземним інформаційним маніпуляціям та втручанням (FIMI), що дозволило зосередитися на виявленні скоординованої діяльності іноземних акторів. Формування регіонально адаптованих оперативних груп (Task Forces) стало логічним етапом розвитку стратегічних комунікацій, який враховує лінгвістичні та культурні вразливості різних стратегічних напрямків, від Східного партнерства до регіону MENA, і водночас створює ефект взаємного підсилення між національними інституціями та відповідними політиками безпеки.

Разом із тим, ефективність субінструментів стратегічних комунікацій залишається обмеженою через фінансову асиметрію, порівняно з ресурсами Росії як держави-агресора, та інституційну фрагментацію всередині ЄС, де розрив між моделлю «тотальної оборони» прикордонних держав і суто регуляторними підходами держав Західної Європи породжує небезпечний ефект «клаптикової ковдри». Подолання цих викликів потребує вироблення нових показників ефективності, здатних враховувати психологічні ризики, зокрема ефект «зворотного удару», а також синхронізації стратегічних наративів із реальними політичними діями. Лише за умови посилення горизонтальної координації через Систему швидкого сповіщення стратегічні комунікації зможуть виконати свою головну функцію, яка полягає, зокрема і в забезпеченні захисту цінностей ліберальної демократії на європейському континенті.

3.2. Формування системи цифрових безпекових інструментів протидії дезінформації в ЄС

Сучасна модель європейської безпеки перебуває у стані глибокої трансформації під тиском гібридних загроз. У цих умовах традиційні

дипломатичні та нормативні механізми виявляються недостатніми, адже швидкість поширення дезінформації, її вірусність та технологічна складність, включно з використанням бот-мереж та штучного інтелекту, вимагали від ЄС відповіді, яка була б симетричною за технологічним рівнем та оперативністю. Як слушно зазначає дослідниця А. Шуляк, проблема протидії дезінформації тісно пов'язана з технологічною революцією 4.0, що розмиває межі між безпосередніми бойовими діями та політикою, а також між військовими та цивільними особами. У цьому контексті цифрові інструменти стають ключовими безпековими активами: нейромережі для розпізнавання обличь, супутникова розвідка, мережі зв'язку на кшталт Starlink, а також безпілотні літальні апарати, які виконують функції фізичного ураження та постійного психологічного тиску. Особливого значення набувають інформаційно-комунікаційні «війська», руйнівний потенціал яких щодо державних інститутів, інфраструктури, культури та психіки населення є співмірним із потужністю традиційних родів військ [72, с. 189–190]. Саме тому цифрові інструменти протидії дезінформації перестають бути допоміжними технічними елементами і набувають статусу критично важливих безпекових інструментів політики ЄС. Логіка розвитку цієї політики диктує перехід від загального інституційного виміру до практичного використання конкретного цифрового інструментарію протидії дезінформації (програмних комплексів, платформ верифікації та алгоритмічних систем), які формують основу інформаційної безпеки ЄС та забезпечують стійкість до гібридних загроз [199].

Відповідно, формування цифрових інструментів протидії дезінформації, опиралося на констатацію здійсненого переходу від традиційних методів медійного впливу до явища, яке в сучасному науковому дискурсі визначається С. Воллей та П. Говардом як «обчислювальна пропаганда» [400, p. 3–6] (computational propaganda), тобто вплив, що здійснюється засобами цифрових технологій. Як наголошують дослідники, сучасна дезінформація більше не обмежується ресурсом комунікаційної риторичної майстерності конкретних пропагандистів, а використовує обчислювальні потужності для експоненційного

масштабування впливу. Це поняття описує конвергенцію трьох ключових факторів: алгоритмічної автоматизації, використання великих даних (Big Data) та соціальних мереж для маніпулювання громадською думкою у глобальному масштабі [152]. Якщо раніше поширення дезінформації було обмежене кількістю залучених пропагандистів, то нині цифрові інструменти дозволяють масштабувати цей процес експоненційно, перетворюючи інформаційний простір на арену автоматизованих «бойових» дій. Відтак, політика протидії дезінформації в СЄ потребувала розгортання безпекових інструментів, які здатні відповідати на виклики технологічної революції, інтегруючи алгоритмічні системи верифікації, програмні комплекси моніторингу та платформи стратегічних комунікацій.

Для забезпечення ефективності цифрових інструментів в ЄС здійснювалося системне дослідження найбільш небезпечних цифрових інструментів поширення дезінформації. Одним із найбільш небезпечних, що неперевно генерує безпекові виклики, була визнана діяльність автоматизованих бот-мереж, які визначаються як алгоритмічно керовані програми, здатні поширювати контент та імітувати людську поведінку в онлайн-просторі. У політичному контексті вони застосовуються для реалізації тактики «астротурфінгу» (astroturfing), тобто штучного створення ілюзії масової підтримки або обурення певним наративом [226, p. 101]. Дослідження підтверджують, що такі мережі здатні «управляти трендами» (commanding the trend), виводячи маргінальні дезінформаційні повідомлення у топ обговорень завдяки масованому постингу в короткі проміжки часу, що вводить в оману алгоритми соціальних мереж і реальних користувачів [320]. У звіті «Industrialized Disinformation» була зафіксована діяльність організованих «кібервійськ» у 81 країні світу, що свідчить про глобальний характер загрози та її системність [114, p. 10–12]. Ці структури часто інтегровані у державний апарат, фінансуються з офіційних бюджетів і діють як складова національної безпекової стратегії або військової доктрини. Основними тактиками таких підрозділів є просування проурядових агресивних наративів за допомогою агресивної антидемократичної

та антиєвропейської риторики, що спрямовано на придушення демократичної участі та підрив довіри до ЄС за його межами.

До небезпечних цифрових інструментів поширення дезінформації була віднесена технологія тролінгу, який, на відміну від автоматизованих бот-мереж, базується на залученні реальних операторів. Тролями є акаунти, керовані людьми, часто організованими у професійні структури, як-от відоме «Агентство інтернет-досліджень» у Санкт-Петербурзі, завданням яких є поширення дезінформації, агресивне інформаційне переслідування опонентів, використання мови ворожнечі та навмисна емоційна дестабілізація дискусій. У безпековому вимірі тролінг є засобом психологічного тиску, що використовується для залякування журналістів та активістів, змушуючи їх до самоцензури та підриваючи демократичні процеси [334, p. 34–35], але в умовах гібридної війни він перестає бути проявом індивідуальної агресії в мережі, а набуває ознак засобу впливу на систему політичних орієнтацій, що визначає спрямованість політичних дій. Саме тому стратегічні комунікації ЄС розглядають протидію тролінгу як критично важливий елемент політики інформаційної безпеки, створюючи алгоритмічні системи моніторингу, платформи верифікації та спеціалізовані аналітичні підрозділи для виявлення координованих атак.

Статус небезпечних цифрових інструментів поширення дезінформації в ЄС набув алгоритмічний мікротаргетинг, що опирається на використання індивідуалізованих та психологічних інструментів. Використовуючи масиви персональних даних, зокрема демографічні показники, історію пошуку, лайки та інші цифрові сліди, зловмисники створюють детальні психологічні портрети користувачів, що дозволяє доставляти індивідуально адаптовані маніпулятивні повідомлення у форматі «dark ads» [91, p. 5, 11]. Ці повідомлення експлуатують специфічні страхи, упередження чи емоційні вразливості конкретної людини, перетворюючи інформаційний простір на поле цілеспрямованого психологічного впливу. Така тактика замикає користувача в «інформаційній бульбашці» (filter bubble), де він отримує лише ті повідомлення, що підсилюють його переконання, роблячи його несприйнятливим до контраргументів та

фактчекінгу [91, p. 5]. У безпековому вимірі це означає руйнування базових механізмів демократичної участі, адже вибір громадян формується не на основі відкритої дискусії, а через приховані маніпуляції. Саме тому ЄС розглядає протидію алгоритмічному мікротаргетингу як критично важливий інструмент політики інформаційної безпеки, інтегруючи системи прозорості цифрової реклами, алгоритмічні механізми верифікації та регуляторні рамки для обмеження використання персональних даних у маніпулятивних цілях Додати посилання про документи ЄС.

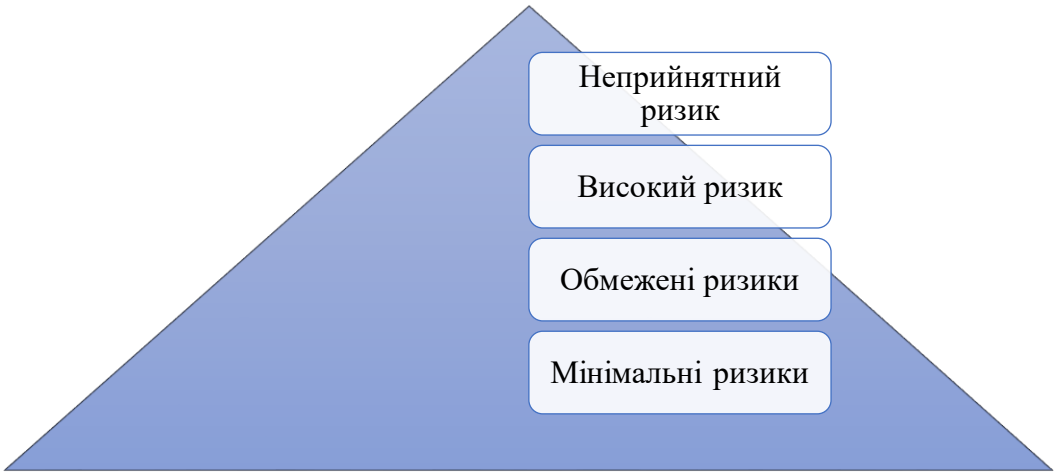
Якісно новим викликом для безпекової архітектури ЄС стала поява генеративного штучного інтелекту (ШІ) та технології глибоких фейків (Deepfakes), які перетворилися на інструменти системної дестабілізації інформаційного простору (Додаток К). Йдеться про цифрові маніпуляції аудіо, зображеннями та відео, створені за допомогою нейромереж, зокрема генеративно-змагальних мереж (GANs), що дозволяють видавати синтетичний контент за реальні записи подій чи виступи конкретних осіб. Небезпека діпфейків полягає у тому, що вони атакують фундаментальну довіру до аудіовізуальних доказів, яка є основою сучасного сприйняття реальності та легітимності політичних процесів. Хрестоматійним прикладом використання цієї технології як зброї в умовах війни став інцидент у березні 2022 р., коли хакери транслювали діпфейк-відео Президента України В. Зеленського із закликом до капітуляції. Тоді російська сторона виходила з припущення, що опір України тримається виключно на авторитеті Президента, демонструючи власний патерналізм і нерозуміння менталітету українців [351]. Через низьку технічну якість цей фейк був оперативно викритий та спростований, однак він став стратегічним сигналом про настання нової ери синтетичної дезінформації, де бар’єр входу для створення фейків стрімко знижується, а їхня переконливість зростає. Відповідно, ЄС мав інтегрувати нові інструменти протидії дезінформації, які виходять за межі класичного фактчекінгу. Йдеться про створення алгоритмічних систем верифікації аудіо- та відеоконтенту, розробку платформ для маркування синтетичних матеріалів, а також формування

спеціалізованих підрозділів стратегічних комунікацій, здатних оперативно реагувати на появу діпфейків. Важливим елементом стало залучення інтелектуального потенціалу незалежних дослідницьких центрів держав-членів ЄС, здатних забезпечити багаторівневу експертизу та підвищити довіру суспільства до офіційних повідомлень.

У відповідь на нові технологічні виклики ШІ, що набули екзистенційного характеру для інформаційної та політичної безпеки, ЄС здійснив перехід від ситуативного реагування до формування комплексної системи цифрових інструментів регулювання, які стали невід'ємною складовою політики протидії дезінформації. Основоположним документом у цій сфері є Акт про штучний інтелект (Artificial Intelligence Act, AI Act), який набув чинності у 2024 р. [347] За даними Європарламенту, ключові положення щодо маркування контенту, створеного за допомогою ШІ, почали застосовуватися від початку 2025 р., що передбачало перехідний період для адаптації медіа-ринку та технологічних платформ [173]. Це перший у світі комплексний регламент щодо ШІ, який визначив чіткі правила, засновані на ризик-орієнтованому підході, для розробників та користувачів ШІ у конкретних сферах його застосування.

AI Act є частиною ширшого пакету політичних заходів, спрямованих на підтримку розвитку надійних технологій, які водночас забезпечують захист від їхнього деструктивного використання. У пункті 4 документа подається визначення ШІ як «сімейство технологій, що сприяє широкому спектру економічних, екологічних та соціальних переваг у всьому спектрі галузей промисловості та соціальної діяльності. Завдяки покращенню прогнозування, оптимізації операцій та розподілу ресурсів, а також персоналізації цифрових рішень, доступних для окремих осіб та організацій, використання ШІ може забезпечити ключові конкурентні переваги для підприємств та підтримувати соціально та екологічно корисні результати, наприклад, у сфері охорони здоров'я, сільського господарства, безпеки харчових продуктів, освіти та навчання, медіа, спорту, культури, управління інфраструктурою, енергетики, транспорту та логістики, державних послуг, безпеки, юстиції, ресурсної

ефективності та енергоефективності, моніторингу навколишнього середовища, збереження та відновлення біорізноманіття та екосистем, а також пом'якшення наслідків зміни клімату та адаптації до них» [210]. Попри таке оптимістичне визначення, регуляція виходить із усвідомлення небезпеки деструктивного використання нових технологій, зокрема у сфері створення синтетичного контенту, маніпуляцій громадською думкою та підриву довіри до демократичних інститутів. Регулювання штучного інтелекту в СЄ вибудуване на багаторівневій моделі оцінки ризиків, яка стала основою для формування безпекових інструментів цифрової політики. Чотирирівневий підхід дозволяє класифікувати технології за ступенем потенційної загрози для суспільства, політичних процесів та демократичної легітимності (Малюнок 3.2.1).



Малюнок 3.2.1. Багаторівнева модель оцінки ризиків застосування ШІ

Відповідно до малюнку 3.2.1, на найнижчому рівні знаходяться технології ШІ з мінімальним ризиком, які можуть використовуватися без додаткових обмежень, проте навіть вони підлягають базовим вимогам прозорості та маркування, щоб унеможливити приховане маніпулювання. Вони не становлять безпосередньої загрози для здоров’я, безпеки чи фундаментальних прав громадян і тому не потребують спеціального регулювання. До цієї групи належить переважна більшість систем ШІ, зокрема такі приклади, як відеоігри чи спам-фільтри, які виконують допоміжні функції у цифровому середовищі та не мають потенціалу для системного впливу на політичні процеси чи

демократичну участь. Проте навіть у випадку мінімального ризику ЄС розглядає ці технології крізь призму політики протидії дезінформації, адже вони формують загальне інформаційне середовище, у якому відбувається взаємодія громадян із цифровими платформами. Тобто, навіть такі інструменти можуть бути використані як елементи ширших маніпулятивних стратегій, наприклад, через приховане поширення контенту або створення умов для інформаційного перевантаження, що знижує здатність користувачів критично оцінювати повідомлення [95, p. 32–37]. Саме тому політика ЄС у сфері регулювання ШІ навіть для категорії мінімального ризику інтегрує принципи прозорості та відповідальності, формуючи нові стандарти цифрової гігієни. У цьому контексті мінімальний ризик не означає повної відсутності загроз, а радше визначає рівень, на якому превентивні заходи мають бути спрямовані на підтримку інформаційної стійкості та формування довіри громадян до цифрових технологій.

Наступний рівень охоплює технології з обмеженим ризиком, для яких ключовим завданням стає забезпечення інформованої взаємодії користувачів із системами, що застосовують алгоритмічні рекомендації чи автоматизовані рішення. Обмежений ризик у системі регулювання ШІ пов’язується з категоріями технологій, що не створюють безпосередньої загрози життю чи безпеці громадян, але потребують суворої прозорості у взаємодії з користувачами, оскільки їхнє застосування може стати інструментом прихованих маніпуляцій у сфері дезінформації. До таких випадків належать системи, які забезпечують комунікацію у форматі чат-ботів, а також створення контенту за допомогою генеративних моделей, включно з глибокими фейками та публічними текстами, що можуть бути використані для підриву довіри до демократичних інститутів. Тому ЄС закріплює вимогу обов’язкового інформування громадян про взаємодію з ШІ, а також чітке маркування контенту, створеного алгоритмічними системами, щоб унеможливити його використання як інструменту прихованого впливу [210].

Третій знизу рівень визначає високоризикові застосування, які мають прямий вплив на права та свободи громадян, включно з використанням ШІ у

виборчих процесах, управлінні критичною інфраструктурою чи у сфері правосуддя. Високий ризик у системі регулювання ШІ визначається як практика його застосування, що може спричинити серйозні загрози здоров'ю, безпеці та фундаментальним правам громадян, і саме тому вони стають предметом особливо суворих вимог у політиці протидії дезінформації та забезпечення інформаційної стійкості. Саме тут ЄС інтегрує безпекові інструменти, спрямовані на аудит алгоритмів, незалежну верифікацію та суворий контроль за використанням даних. ЄС закріплює комплекс вимог для таких систем, серед яких обов'язкова оцінка ризиків, використання високоякісних даних, ведення обліку та детальна документація, постійний людський нагляд, гарантії надійності та кібербезпеки [299].

Найвищий рівень – це неприйнятні ризики, які підлягають повній забороні, зокрема технології, що створюють діпфейки для політичних маніпуляцій, системи соціального скорингу чи інструменти масового психологічного контролю. До таких практик належать шкідливі маніпуляції, спрямовані на експлуатацію вразливостей громадян, використання соціального скорингу як інструменту політичного чи соціального контролю, нецільовий скрейпінг для створення баз даних розпізнавання обличь, застосування технологій розпізнавання емоцій у робочих або освітніх середовищах, а також певні форми біометричної ідентифікації та категоризації для правоохоронних органів [210]. У безпековому вимірі ці технології становлять загрозу індивідуальним правам та колективній стійкості демократичних інститутів.

AI Act закріпив принцип обов'язкового маркування контенту, створеного за допомогою алгоритмічних систем, як ключовий безпековий інструмент політики протидії дезінформації. Його метою є убезпечення громадян від хибного сприйняття цифрових матеріалів, що можуть бути використані для маніпуляцій та підриву довіри до демократичних інститутів. У пунктах 133–137 документа детально визначено особливості маркування контенту, створеного штучним інтелектом, із виокремленням поняття «deep-fake», яке обов'язково має позначатися водним знаком («watermark») [347]. Це стосується зображень, аудіо

та відео, що були штучно створені чи здатні вводити в оману, видаючи себе за автентичні. Вимога передбачає чітке та помітне позначення таких матеріалів як синтетичних, щоб громадяни могли одразу ідентифікувати їх як продукт алгоритмічної генерації.

Водночас AI Act враховує, що контент може створюватися з мистецькою метою і не становити загрози для суспільного сприйняття, тому у таких випадках нанесення водного знаку не є обов'язковим. Проте невиконання вимог щодо маркування у випадках, коли контент може бути використаний для маніпуляцій, зокрема і інформацією, тягне за собою серйозні фінансові санкції. AI Act передбачає три рівні штрафів: найвищий (до 35 млн євро або 7% обороту компанії) застосовується за використання заборонених практик; середній рівень (до 15 млн євро або 3% обороту) застосовується за загальне невиконання вимог AI Act; найнижчий рівень (до 7,5 млн євро або 1,5% обороту) застосовується за надання недостовірної чи неповної інформації регуляторам [347]. Така система санкцій перетворює етичні норми на жорсткі фінансові зобов'язання для технологічних гігантів, змушуючи їх інтегрувати принципи прозорості та відповідальності у власні бізнес-моделі. На нашу думку, ці норми AI Act стають фундаментальним інструментом політики протидії дезінформації в ЄС, адже вони створюють превентивний бар'єр проти використання генеративних технологій в створенні та поширенні дезінформації.

AI Act передбачив чіткі зобов'язання національних урядів у сфері контролю за впровадженням та використанням систем ШІ. Це положення є ключовим у контексті політики протидії дезінформації, адже воно інтегрує національний рівень політики у сфері протидії цифровим дезінформаційним загрозам у загальноєвропейський механізм протидії дезінформації. Поруч із дефініцією технологій у документі міститься алгоритм впровадження нових систем штучного інтелекту на національному рівні, який закріплений у пункті 138 [210]. Цей алгоритм передбачає створення механізмів оцінки ризиків, формування незалежних органів моніторингу, забезпечення прозорості процесів та обов'язкове інформування громадян про використання ШІ у сферах, що мають

безпосередній вплив на їхні права та свободи. Такі зобов'язання означають, що кожна держава-член ЄС бере на себе відповідальність за контроль за використанням інструментів ШІ, що дозволяє координувати дії із протидії дезінформації, згенерованої ШІ, опираючись при цьому на національні особливості інформаційного простору.

Важливим аспектом цифрового захисту споживачів інформації в ЄС стала вимога алгоритмічної прозорості, закріплена в Акті про цифрові послуги (Digital Services Act, DSA) [223]. Протягом тривалого часу алгоритми рекомендацій соціальних мереж функціонували як «чорні скриньки», автоматично підсилюючи дезінформаційні повідомлення завдяки їхній віральності та здатності викликати сильну емоційну реакцію. Як зазначається у звітах дослідників, алгоритмічні системи платформ часто надають пріоритет поляризуючому контенту, створюючи замкнені «ехо-камери», які ізолюють користувачів від альтернативних точок зору та підривають можливість критичного мислення [395, p. 44–48]. Саме тому нова нормативна база ЄС зобов'язує дуже великі онлайн-платформи (Very Large Online Platforms, VLOPs) проводити оцінку системних ризиків своїх алгоритмів та надавати доступ до їхнього коду верифікованим дослідникам, що прямо передбачено статтею 40 DSA [223]. Це дозволило перейти від боротьби з наслідками (видалення окремих постів) до усунення причин, тобто переналаштування алгоритмів таким чином, щоб вони песимізували (знижували у видачі) неперевірений або маніпулятивний контент, а не просували його.

Такий підхід позбавив технологічних гігантів монополії на «таємницю алгоритмів», роблячи їхні внутрішні механізми підзвітними у випадках, коли вони становлять загрозу демократичній стабільності та спряв трансформації незалежного алгоритмічного аудиту на дієвий інструмент цивільного контролю, за допомогою якого суспільство, через діяльність верифікованих експертів, отримує реальні важелі нагляду за цифровим контентом, що формує громадську думку. Звіти за перше півріччя 2024 р. вказали на суттєві відмінності у готовності VLOPs до співпраці з дослідниками та регуляторами. Так, Google та YouTube

продемонстрували вищий рівень відкритості у наданні даних, тоді як Meta та TikTok продовжують створювати бар'єри для незалежних експертів, що залишається предметом постійного регуляторного тиску з боку Єврокомісії, яка розуміє, що ручна верифікація не здатна впоратися з масштабами контенту, згенерованим штучним інтелектом [127].

На нашу думку, актуальним є сформований досвід Ірландії, яку називають цифровим хабом Європи, адже в Дубліні розташовані європейські штаб-квартири більшості глобальних технологічних компаній. Ірландський регулятор Coimisiún na Meán (Комісія з медіа) фактично виконує роль головної контролюючої інституції за дотриманням положень DSA на рівні ЄС [178] . У 2022 р. Ірландія ухвалила Акт про регулювання онлайн-безпеки та медіа (Online Safety and Media Regulation Act), який надав регулятору широкі повноваження щодо моніторингу шкідливого контенту [329]. Відповідно до цього закону було створено Coimisiún na Meán, який отримав право призначати «Комісара з онлайн-безпеки» (Online Safety Commissioner), уповноваженого накладати санкції на платформи за системну бездіяльність у боротьбі зі шкідливим дезінформаційним контентом [129]. Цей орган виступає національним координатором цифрових послуг у рамках виконання DSA, забезпечуючи прямий канал комунікації між Брюсселем та штаб-квартирами технологічних гігантів. Водночас Ірландія демонструє зважений підхід до балансу між безпекою та свободою слова. Разом із Фінляндією та Швецією вона виступила ініціатором політичної позиції, що боротьба з дезінформацією не повинна призводити до надмірного блокування контенту (over-blocking), який не є однозначно незаконним [133]. Ця ідея була покладена в розробку Національної стратегії протидії дезінформації, над якою працює спеціальна міжвідомча група за участі науковців, індустрії та громадянського суспільства [314].

Одночасно ЄС інвестує значні ресурси у створення технологічного щита через програму Horizon Europe, яка фінансує розробку інструментів автоматизованої верифікації, здатних виявляти штучно створені інформаційні матеріали, маркувати їх та інтегрувати у систему стратегічних комунікацій [181].

Це дозволить повністю перейти від реактивної моделі боротьби з дезінформацією до проактивної, оскільки будуть створені максимальні умови для своєчасного розпізнавання та блокування дезінформаційного контенту. Таким чином, вимога алгоритмічної прозорості VLOPs інтегрується в систему засобів реалізації безпекових інструментів політики ЄС у сфері протидії дезінформації та підсилюється інвестиціями у власні інструменти цифрової безпеки.

Прикладом практичного використання цифрових інструментів у політиці протидії дезінформації в ЄС є проєкт Verification Assisted by Artificial Intelligence (VERA.ai) [389]. Він є флагманською ініціативою ЄС в межах програми Horizon Europe, що унаочнює перехід від пасивного фактчекінгу до активного технологічного спротиву та організаційно є консорціумом із 14 провідних дослідницьких інститутів та медіа-організацій, серед яких AFP, Deutsche Welle та University of Sheffield, які працюють над створенням «імунітету» цифрового простору. VERA.ai опирається на передову систему мультимодального аналізу, яка використовує ШІ для викриття неправдивої інформації, наділяючи цю цифрову технологію ознаками інструменту захисту демократичної стабільності. Алгоритми VERA.ai здатні здійснювати комплексну перевірку контенту, застосовуючи методи lip-sync analysis для виявлення діпфейків через аналіз узгодженості аудіо-доріжки з рухом губ спікера. Генеративні моделі часто допускають мікропомилки у синхронізації, які залишаються непомітними для людського ока, але фіксуються нейромережами VERA.ai як аномалії. Система також шукає невидимі для ока сліди цифрового втручання у відеопотік, зокрема зміни піксельної сітки, та проводить мережевий аналіз поширення наративів, що дозволяє ідентифікувати координовані інформаційні операції. Система VERA.ai використовує методи цифрової криміналістики для пошуку слідів невідповідності шумів піксельної сітки. Кожна зміна, внесена ШІ у відеопотік, залишає специфічний цифровий «артефакт», який алгоритми ідентифікують як доказ втручання [389].

Для протидії дезінформації, особливо важливим є те, що на відміну від традиційних інструментів, VERA.ai, констатуючи факт існування фейку, показує механізми його поширення. Система Cross-platform Tracking відстежує рух контенту між різними платформами, виявляючи координовану поведінку бот-мереж, тоді як алгоритм Narrative Discovery кластеризує тисячі повідомлень у єдині наративи, дозволяючи дослідникам бачити не окремі дописи, а масштабні інформаційні операції, що стоять за ними. Автори проєкту VERA.ai розвиваєють ідею «верифікації як послуги», інтегруючи свої напрацювання у популярні інструменти для журналістів, такі як розширення InVID & WeVerify [388], що робить складні технології штучного інтелекту доступними для фактчекерів у режимі реального часу.

Ще одним перспективним проєктом формування сталих цифрових інструментів протидії дезінформації в ЄС є проєкт AI4TRUST, який реалізує концепцію «гібридного інтелекту» [76]. Система функціонує за принципом лійки: ШІ здійснює первинний моніторинг мільйонів повідомлень у режимі реального часу, відсіюючи інформаційний шум та позначаючи контент із високим ризиком (high-risk content). Лише ці, вже відфільтровані випадки, передаються на розгляд людині-експерту. Такий підхід дозволяє фактчекерам не витрачати ресурси на рутинний моніторинг, а концентруватися на складних кейсах дезінформаційного впливу, що мають стратегічне значення для інформаційної безпеки. Особливістю AI4TRUST є впровадження методів пояснювального ШІ, які забезпечують виявлення маніпуляцій та надання експертам обґрунтування. Система може вказати на використання специфічних лінгвістичних маркерів, характерних для дезінформаційних кампаній певних суб’єктів, що дозволяє ідентифікувати джерела та методи інформаційних атак. Завдяки підтримці мультилінгвальних моделей AI4TRUST забезпечує моніторинг інформаційних операцій, які проводяться одночасно в різних країнах ЄС, дозволяючи виявляти транскордонні стратегії впливу, адаптовані під локальний культурний та політичний контекст [77]. На нашу думку, важливість

AI4TRUST визначається тим, що він поєднує швидкість і масштабність алгоритмічного аналізу з глибиною людської експертизи.

Окремим кластером цифрових інструментів протидії дезінформації в ЄС є технології забезпечення цілісності даних (integrity technologies), функціональність яких більшою мірою характерна для держав-членів ЄС. Показовим прикладом є технологічний досвід Естонії, в якій система е-урядування побудована на технології розподіленого реєстру KSI Blockchain [108]. Після масштабних кібератак 2007 р. Естонія усвідомила, що в умовах гібридної агресії об'єктом атаки стають не лише сервери чи технічна інфраструктура, але й довіра громадян до державних інститутів, яка є ключовим ресурсом демократичної стійкості [380]. Саме тому технологія KSI Blockchain була інтегрована як фундаментальний елемент цифрової безпеки, забезпечуючи математично доведену автентичність державних даних. На відміну від публічних блокчейнів, KSI була розроблена спеціально для потреб держави, що робить її унікальним інструментом у сфері захисту від дезінформації [279]. Вона не потребує значних енерговитрат і забезпечує миттєву верифікацію на рівні мільярдів записів, що дозволяє інтегрувати її у всі критично важливі сфери від медичних карток до систем національної оборони та механізмів протидії інформаційним атакам. Ця технологія унеможливлює непомітну фальсифікацію державних даних заднім числом, оскільки будь-яка спроба змінити запис у реєстрі (чи то про власність, судові рішення або результати виборів) миттєво фіксується системою. Такий підхід, відомий як «security by design» (безпека через архітектуру), робить державу невразливою до класичних дезінформаційних наративів про «злам системи» чи «підробку реєстрів», які традиційно використовуються для підриву довіри до демократичних процесів. Технологія розподіленого реєстру виконує роль превентивного щита, що нейтралізує ефект «дилеми брехуна», описаної Р. Чесні та Д. Сітрон, коли зловмисники намагаються поставити під сумнів справжні документи, видаючи їх за підробку [128, p. 1785]. Наявність незмінного цифрового відбитка дозволяє державі миттєво підтвердити автентичність будь-якого документа, знімаючи можливість

маніпуляцій ще на етапі їх зародження. Це означає, що інформаційна атака втрачає силу, оскільки технологічна інфраструктура сама по собі стає доказом правдивості даних. Досвід Естонії сьогодні масштабується на рівень НАТО та оборонних відомств країн ЄС як еталон цифрового суверенітету [318].

Аналізуючи цифрові інструменти протидії дезінформації, важливо констатувати, що Україна як держава-кандидат активно імплементує європейський досвід верифікації через систему е-взаємодії «Трембіта», яка є адаптованою версією естонської платформи X-Road та водночас фундаментом національної цифрової інтероперабельності [39]. Ключова перевага цієї системи полягає у її децентралізованій архітектурі, що відкидає концепцію єдиного «мега-сховища» даних, яке могло б стати критичною мішенню для масштабних кібератак. «Трембіта» організовує захищений «тунель» для обміну інформацією безпосередньо між державними реєстрами за вже згадуваним принципом «security by design». Кожна транзакція супроводжується двостороннім шифруванням та накладанням кваліфікованої е-печатки, яка гарантує цілісність та юридичну значущість даних, створюючи неспростовний цифровий доказ кожної операції. Такий підхід нівелює ефективність дезінформаційних кампаній, побудованих на фейках про «масштабні витоки» чи «підміну записів». Оскільки система забезпечує незмінність логів (журналів подій), держава отримує неспростовний аудиторський слід («цифрове алібі») для кожної транзакції, яке неможливо сфальсифікувати навіть у випадку масштабних інформаційних атак. «Трембіта» функціонально опирається європейський принцип «Once-only», за яким дані зберігаються лише в одному першоджерелі, а не дублюються, що мінімізує ризики маніпуляцій та підвищує стійкість інформаційної системи. Наголосимо, що Проєкт, реалізований у межах ініціативи EGOV4UKRAINE [23], уже продемонстрував надзвичайну стійкість, забезпечивши понад 3 мільярди успішних транзакцій за 2024–2025 рр. навіть в умовах гібридної війни [40]. Це перетворює «Трембіту» на базовий елемент національної цифрової резильєнтності, який захищає дані та відтворює довіру громадян до цифрових інструментів захисту.

Ефективність цифрових інструментів протидії дезінформації на рівні ЄС значною мірою визначається здатністю держав-членів розгортати власні цифрові інструменти виявлення та нейтралізації загроз, що доповнюють загальноєвропейські регуляторні рамки. На відміну від нормативних механізмів, які є спільними для всіх держав-членів (DSA та AI Act), технічний інструментарій часто створюється на національному рівні з урахуванням специфіки локальних викликів та характеру інформаційних атак. Саме аналіз національних моделей дозволяє виокремити два успішні, але концептуально відмінні підходи, які демонструють різні траєкторії інституціоналізації безпекових інструментів у політиці протидії дезінформації. По-перше, це державно-центричний підхід, який реалізує Франція, і який ґрунтується на посиленні ролі державних інституцій у моніторингу та контролі інформаційного простору. По-друге, гібридний підхід, який сформувався в Литві, базується на поєднанні державних інституцій та громадянського суспільства у спільному використанні цифрових інструментів протидії дезінформації.

Франція обрала шлях створення потужної державної інфраструктури технічного моніторингу як ключового безпекового інструменту у політиці протидії дезінформації [265]. У 2021 р. було створено спеціалізовану Службу пильності та захисту від іноземного цифрового втручання (VIGINUM), яка підпорядковується Генеральному секретаріату оборони та національної безпеки [287]. Унікальність цієї структури полягає у її чітко визначеному мандаті: вона концентрується виключно на технічному виявленні іноземних маніпуляцій інформацією (FIMI), принципово не втручаючись у внутрішній політичний дискурс, щоб уникнути звинувачень у цензурі та зберегти легітимність демократичних процесів. Технічне ядро VIGINUM базується на використанні алгоритмічних систем для виявлення «неавтентичної скоординованої поведінки» [390]. Система автоматично сканує відкриті дані соціальних мереж та веб-платформ, аналізуючи не зміст повідомлень, а метадані та патерни їх поширення. Алгоритми шукають аномалії, які є характерними для інформаційних операцій: синхронну публікацію однакового контенту з тисяч акаунтів, неприродно

швидке зростання охоплення або використання ідентичних IP-адрес для адміністрування сторінок, що видаються за незалежні [345].

Прикладом ефективності застосування VIGINUM у політиці протидії дезінформації стало викриття у лютому 2024 р. мережі «Portal Kombat» [345]. Технічні фахівці служби VIGINUM змогли ідентифікувати інфраструктуру, що складалася щонайменше зі 193 сайтів-клонів, які імітували локальні новинні портали в країнах ЄС, але фактично в автоматизованому режимі агрегували контент із російських Telegram-каналів. Завдяки використанню аналізу технічних індикаторів компрометації (IoC) VIGINUM вперше вдалося здійснити точну атрибуцію цієї мережі, пов'язавши її з діяльністю російської компанії TigerWeb та провайдерами у тимчасово окупованій Автономній Республіці Крим. Публікація детального технічного звіту стала інструментом оперативної нейтралізації цифрової інфраструктури, що використовувалася для поширення дезінформації [345]. Це дозволило платформам та хостинг-провайдерам миттєво заблокувати ворожі ресурси, продемонструвавши перевагу стратегії системного очищення цифрового середовища над традиційним підходом, який обмежувався спростуванням окремих наративів. Таким чином, кейс «Portal Kombat» підтвердив, що технічний моніторинг і алгоритмічна атрибуція стають ключовими безпековими інструментами політики ЄС у сфері протидії дезінформації, адже вони дозволяють виявляти джерела інформаційних атак та оперативно позбавляти їх інфраструктурної бази.

Подібну методологію технічної атрибуції та аналізу мережевих аномалій використовує українська модель протидії дезінформації, яка була адаптована до специфіки Telegram-сегменту та стала важливим елементом у формуванні європейських стандартів інформаційної безпеки. Якщо французька служба VIGINUM концентрується на виявленні загроз у вебпросторі, то Центр протидії дезінформації у тісній синергії з OSINT-спільнотами, застосовують аналогічний підхід для викриття мереж анонімних Telegram-каналів, які використовуються як інструмент гібридного впливу [64]. Ключовим елементом українського досвіду є ідентифікація проксі-ресурсів, що дозволяють обходити санкційні обмеження та

ретранслювати заборонені наративи через мережу номінально незалежних каналів, створюючи ілюзію внутрішніх джерел інформації. Спільна з європейськими партнерами матриця інформаційного інструменту протидії дезінформації полягає у деконструкції архітектури анонімності: замість спростування змісту повідомлень аналітики виявляють технічні зв'язки між каналами, які маскуються під джерела «внутрішніх інсайдів» або локальних новин [86]. Інтеграція OSINT-спільнот у систему національної розвідки дозволяє в режимі реального часу картографувати ці мережі, виявляючи ідентичні часові інтервали публікацій, спільних адміністраторів та інфраструктуру поширення контенту. Це створює можливість для оперативного реагування та стратегічного блокування інформаційних операцій ще на етапі їх розгортання. На нашу думку, такий підхід підтверджує формування єдиного європейського стандарту технічної атрибуції, який опирається на виявлення скоординованої неавтентичної поведінки стає неспростовним доказом іноземного втручання незалежно від платформи розповсюдження. Українська практика, синхронізована з досвідом Франції, демонструє, що ефективна протидія дезінформації можлива лише через поєднання алгоритмічного аналізу, мережевої криміналістики та інституційної співпраці, що в перспективі перетворить цифрові інструменти на стратегічні засоби формування інформаційної стійкості ЄС.

Литва розробила унікальну модель державно-приватного партнерства, що стала важливим безпековим інструментом у політиці протидії дезінформації в ЄС. Йдеться про платформу Debunk.org, яка позиціонується як незалежна технологічна організація, що тісно співпрацює з державними інституціями та медіа, інтегруючи їх у єдину систему інформаційної стійкості. Архітектура Debunk.org базується на синергії штучного інтелекту та спільноти волонтерів («ельфів») [87], що створює гібридну модель протидії дезінформації, в якій алгоритмічний аналіз поєднується з експертизою, що здійснюється людиною. Технічна складова системи Debunk.org здатна щодня аналізувати понад 30 тис. одиниць контенту з тисяч джерел, включно з веб-сайтами, Facebook та Telegram.

Алгоритми машинного навчання налаштовані на розпізнавання патернів ворожої пропаганди у режимі реального часу: система фіксує потенційно шкідливе повідомлення менш ніж за дві хвилини після його появи [145]. Штучний інтелект оцінює контент за низкою параметрів: емоційне забарвлення, наявність ключових слів-маркерів дезінформації, зв'язок джерела з відомими мережами ботів. Однак ключовою відмінністю литовської моделі є етап верифікації: повідомлення, позначені алгоритмами як «підозрілі» (high risk), передаються на розгляд аналітикам-людям. Це дозволяє уникнути помилкових спрацювань (false positives), властивих автоматичним системам, і водночас забезпечує високий рівень довіри до результатів аналізу. Верифікована інформація про атаку миттєво передається медіа-партнерам, які охоплюють до 90% аудиторії країни, що дозволяє реалізувати стратегію «пребанкінгу», тобто попередження суспільства про дезінформаційне повідомлення ще до того, як воно набере вірусного поширення [146].

Порівнюючи французький та литовський національні підходи до формування системи цифрових інструментів протидії дезінформації, зауважимо, що французька модель передбачає створення спеціалізованих державних структур, що здійснюють системний аналіз цифрових загроз, координують роботу з платформами та забезпечують прозорість алгоритмічних процесів. Такий підхід підкреслює інституційну відповідальність держави за захист громадян від маніпуляцій, формуючи вертикальну систему управління ризиками та інтегруючи технологічні рішення у стратегічні комунікації. Французька модель, що опирається на державно-центричний підхід, унаочнює, як держава може інтегрувати цифрові інструменти протидії дезінформації, забезпечуючи прозорість та контроль над інформаційними потоками, що походять з-за кордону. Гібридна литовська модель активно залучає незалежні медіа, фактчекінгові організації та експертні спільноти до процесу моніторингу інформаційних операцій, створюючи горизонтальну систему взаємодії у формування сукупності цифрових інструментів протидії дезінформації. Ефективність двох моделей вказує на те, що, результативність цифрової протидії

залежить від здатності держав адаптувати європейські стандарти до власних умов, створюючи багаторівневу систему захисту від дезінформації.

Таким чином, здійснений аналіз формування системи цифрових безпекових механізмів протидії дезінформації в ЄС довів, що зміст цього процесу визначається поступовим інституційним закріпленням технологічних практик у політичному та правовому просторі, що перетворює окремі інновації на стійкі елементи архітектури європейської безпеки. Від початкових регуляторних рамок, закріплених у DSA та AI Act, до національних моделей технічного моніторингу у Франції (VIGINUM), гібридних форматів державно-громадянської співпраці в Литві (Debunk.org), технологічних рішень забезпечення цілісності даних в Естонії (KSI Blockchain) та інституційного контролю за платформами в Ірландії (Coimisiún na Meán), простежується логіка поступового нарощування компетенцій цих цифрових інструментів протидії дезінформації та їх інтеграції в систему взаємопов'язаних механізмів протидії. Цей процес характеризується ефектом взаємного підсилення: технічні інструменти атрибуції та верифікації, такі як VERA.ai чи AI4TRUST, створюють умови для більшої прозорості цифрового середовища, а інституційні органи, на кшталт ірландського регулятора, забезпечують легітимність та примусовість виконання правил. Водночас національні практики, як українська модель деконструкції анонімних Telegram-мереж чи литовська стратегія «пребанкінгу», інтегруються у ширший європейський контекст, посилюючи транснаціональні стандарти технічної атрибуції та спільного реагування на інформаційні атаки.

У цьому поступі чітко простежується логіка інституційної еволюції, оскільки нові цифрові інструменти спершу виникають як реакція на конкретні загрози, але згодом закріплюються у правових актах, отримують інституційну підтримку та стають частиною системи колективної безпеки. Одночасно діє механізм функціонального розширення, який передбачає, що кожна нова сфера застосування цифрових технологій з метою протидії дезінформації створює потребу у додаткових інституційних механізмах, що забезпечують їхню легітимність і сталість. Здійснений аналіз цифрових інструментів протидії

дезінформації в ЄС вказує на те, що їх ефективність в умовах гібридної війни може бути посилена через створення онлайн екосистеми, яка здатна інтегрувати різнорівневі інституційні та технологічні практики у єдиний простір взаємодії.

3.3. Створення онлайн екосистеми ЄС як перспективного інструменту політики протидії дезінформації

Онлайн екосистема у контексті політики протидії дезінформації постає як перспективний інструмент, здатний інтегрувати різнорівневі цифрові механізми у єдиний простір взаємодії [363, p. 55]. Комерційні моделі Apple, Meta (Facebook), Amazon, Google чи Microsoft демонструють, як мережевий ефект створює стійкі платформи, в яких кожен елемент підсилює інший, що для ЄС стає актуальним референтним досвідом та концептуальним прототипом побудови безпекових цифрових мереж та інструментів, коли головним активом виступає не економічна вигода, а інформаційна стійкість суспільства [306]. Предметом спеціального вивчення в ЄС, по-перше, став досвід Microsoft із трансформації власної екосистеми в хмарно-орієнтоване середовище (Azure + Microsoft 365 + LinkedIn), який довів, що контроль над моделями взаємодії акторів є ключовим фактором у формуванні політики модерації та протидії маніпуляціям. Для ЄС це означає можливість створення власної онлайн екосистеми, в якій державні регулятори, національні безпекові структури, незалежні фактчекінгові організації та громадянські спільноти функціонують у єдиному цифровому просторі, забезпечуючи швидку атрибуцію загроз, їхню нейтралізацію та превентивне інформування суспільства [300]. Така екосистема дозволятиме уникнути фрагментації, яка виникає при використанні окремих цифрових інструментів протидії дезінформації, і забезпечує їхню сумісність, що є критично важливим у боротьбі з транскордонними інформаційними операціями. По-друге, це стратегія компанії Apple, яку в академічній літературі часто описують як модель «Замкненого саду» (Walled Garden). Її сутність полягає у глибокій вертикальній інтеграції апаратного забезпечення (iPhone, Mac), програмних оболонок (iOS, macOS) та сервісної інфраструктури (App Store,

iCloud, Apple Music), що створює замкнуте середовище, в якому кожен елемент підсилює інший. Стратегічна мета такої екосистеми полягає у формуванні високих «витрат на перехід» (switching costs) для користувача, адже дані, додатки та соціальні зв'язки особи жорстко інтегровані в єдине технологічне середовище, вихід за межі якого стає економічно та психологічно невигідним [403, p. 12–15].

Для ЄС ця логіка може бути використана у безпековому вимірі, коли онлайн екосистема виступає не як комерційний інструмент утримання користувача, а як політичний механізм забезпечення інформаційної стійкості. Якщо Apple демонструє, як контроль над архітектурою взаємодії дозволяє управляти потоками даних і поведінкою користувачів, то ЄС може використати аналогічний принцип для створення середовища, в якому цифрові інструменти протидії дезінформації інтегруються у єдину екосистему. У такій моделі кожен компонент (французький VIGINUM, литовський Debunk.org, естонський KSI Blockchain чи українська практика деконструкції анонімних Telegram-мереж) стає частиною спільної архітектури, в якій взаємопов'язаність і синергія забезпечують ефект мережевого підсилення протидії дезінформації. Така модель цифрової онлайн екосистеми ЄС може створювати новий рівень «витрат на перехід» для суб'єктів дезінформації: будь-яка спроба маніпуляції стикається з багаторівневою системою перевірки, верифікації та блокування, що робить інформаційні атаки економічно та технологічно невигідними.

У технічному звіті Об'єднаного дослідницького центру ЄС цифрова екосистема визначається як складний техно-економічний простір, у межах якого в інтегрований та взаємопов'язаний спосіб здійснюються релевантні цифрові види діяльності за участю різнорідних акторів, що переслідують власні специфічні цілі [237, p. 20-21]. У контексті політики протидії дезінформації ця характеристика набуває нового значення, адже екосистема розглядається як «локус» цифрової трансформації, що завдяки своїй горизонтальній природі перетинається з іншими секторами, трансформуючи їх зсередини, визначаючи технологічні межі функціонування інформаційного простору.

Структурними складниками такої екосистеми є три основні елементи: актори (суб'єкти, гравці), види діяльності та система взаємозв'язків між ними. До категорії акторів (суб'єктів, гравців) належать гетерогенні суб'єкти від малих стартапів та великих транснаціональних компаній до університетів, дослідницьких центрів та урядових установ, які стають частиною спільної архітектури цифрової безпеки ЄС. Діяльність у межах екосистеми диференціюється на бізнес-активність, інноваційну діяльність та науково-дослідну діяльність, що формує базу академічних знань і водночас забезпечує розвиток інструментів протидії дезінформації. Третьою фундаментальною складовою є мережа формальних та неформальних взаємозв'язків, що виникають через спільну участь у вищезгаданих видах діяльності, дозволяючи знанням та інноваціям поширюватися через екосистему та створювати ефект мережевого підсилення у сфері інформаційної безпеки та протидії дезінформації [237, p. 23]. Технологічний периметр екосистеми окреслюється через п'ятнадцять специфічних цифрових областей, таких як ШІ, кібербезпека, автономні системи, хмарні обчислення та блокчейн, які в сукупності формують інтегровану парадигму сучасного цифрового поля ЄС.

Онлайн-екосистеми постійно розвиваються, і саме ця динаміка визначає їхню роль у сучасній європейській політиці протидії дезінформації. Якщо на ранніх етапах розвитку інтернету екосистема сприймалася як сукупність непов'язаних веб-ресурсів, що функціонують за законами вільного ринку, то в умовах гібридної війни вона набуває характеру регульованого середовища з прозорими алгоритмами, відповідальністю платформ та вимірюваною активністю користувачів. Створення такої екосистеми у ЄС є відповіддю на виклик фрагментації інформаційного простору, в якому дезінформація генерується в «сірих зонах» за відсутності регулювання.

Процес формування онлайн екосистеми ЄС у сфері протидії дезінформації опирається на концепцію співрегулювання цифрових платформ, що здійснюється під наглядом інституцій ЄС. Цей підхід було інституційно закріплено в Посиленому кодексі практики щодо дезінформації 2022 р. (SCPD),

який вперше у світовій практиці об’єднав за одним столом 34 ключових гравців цифрової індустрії, зокрема технологічних корпорацій Google, Meta, Microsoft, TikTok, представників рекламного ринку та інститутів громадянського суспільства. На відміну від попередніх декларативних документів, оновлений Кодекс містив 44 зобов’язання та 128 конкретних заходів, виконання яких контролюється спеціально створеною постійною робочою групою [170]. Відтак, цифровий простір переставав бути хаотичною сукупністю платформ і мав перетворитися на регульоване середовище, в якому взаємодія ЄС та держав-членів (актори), приватного сектору (гравці) та громадянського суспільства (суб’єкти) спрямовувалася на досягнення спільної мети – унеможливлення дезінформаційного впливу іноземних держав та корпорацій на суспільно-політичні та економічні процеси в ЄС.

Ключовим інструментом перевірки ефективності створюваної онлайн екосистеми ЄС у сфері протидії дезінформації став Центр прозорості (Transparency Centre) [169]. Це унікальний механізм публічного звітування, який зобов’язує цифрові платформи розкривати дані про власні дії, тим самим інтегруючи приватний бізнес у виконання безпекових функцій, що раніше належали виключно до компетенції політичних інституцій. Відповідно, такий підхід спрямований на зміну балансу відповідальності у цифровому середовищі, адже технологічні компанії стають активними учасниками політики інформаційної безпеки, а не лише комерційними провайдерами послуг. Тобто потенційно набувають статусу не тільки гравців, але й суб’єктів. Показовим прикладом є звіт платформи TikTok за друге півріччя 2024 р., опублікований у рамках виконання SCPD. Компанія повідомила про видалення понад 36700 рекламних оголошень політичного характеру, які порушували стандарти прозорості, а також про запровадження маркування контенту, створеного штучним інтелектом, за допомогою технології C2PA (Content Credentials) [385]. Ці дані демонструють, що у межах створюваної екосистеми платформи змушені діяти в інституційно визначених рамках ЄС, здійснюючи фільтрацію токсичного контенту ще до того, як він набуває масового поширення серед користувачів.

Для формування інституційної основи онлайн екосистеми ЄС важливе значення має Європейська обсерваторія цифрових медіа (EDMO), створена у 2020 р. Її унікальність полягає в тому, що вона стала першою структурою в ЄС, яка інституціоналізувала мультидисциплінарний підхід до протидії дезінфораційним маніпуляціям. EDMO функціонує не як класичний регуляторний орган, а як незалежний координаційний хаб, що об'єднує чотири ключові групи стейкхолдерів: професійних фактчекерів, академічних дослідників, експертів з медіаграмотності та представників медіаіндустрії [193]. Сутність роботи EDMO розкривається через її децентралізовану модель діяльності, що спирається на мережу з 14 національних та регіональних хабів, які охоплюють усі держави-члени ЄС. Така структура дозволяє вирішити одну з фундаментальних проблем протидії дезінформації, пов'язану з необхідністю глибокого розуміння локального мовного та культурного контексту. Наприклад, хаб BENEDMO (Бельгія, Нідерланди) спеціалізується на аналізі фламандського та нідерландського сегментів, тоді як ADMO (Адріатичний регіон) працює з особливостями Балканського простору [97]. Це забезпечує можливість реагувати не на абстрактні інформаційні загрози, а на специфічні локальні наративи, які часто залишаються непомітними для централізованого моніторингу на рівні відповідних інституцій ЄС.

Крім того, EDMO виконує критично важливу функцію технічного посередника у формуванні онлайн екосистеми ЄС. Завдяки створенню безпечного цифрового середовища вона забезпечує дослідникам доступ до даних великих онлайн-платформ у відповідності до вимог GDPR, що раніше було практично недосяжним для окремих науковців і обмежувало можливості системного аналізу інформаційних загроз. Практичним прикладом застосування особливостей такої моделі є кампанія «Be Elections Smart» під час виборів до Європарламенту 2024 р. Завдяки створенню спеціальної цільової групи Task Force, EDMO вдалося організувати транскордонний обмін даними у режимі реального часу, що дозволило оперативно виявляти так звані «переміщені наративи» (cross-border disinformation), коли один і той самий фейк адаптувався

та запускався одночасно в різних країнах ЄС [195]. Це стало прикладом того, як онлайн екосистема здатна долати бар'єри між національними інформаційними просторами, забезпечуючи синхронізовану реакцію на загрози та формуючи новий рівень колективної інформаційної безпеки.

Законодавчим каркасом, який має утримувати складність онлайн екосистеми ЄС як інструменту реалізації політики протидії дезінформації, є згадуваний DSA. Для онлайн екосистеми ЄС однією з найбільш важливих норм є норми, закріплені у статті 22, що стосуються запровадження інституту «довірених скаржників» (trusted flaggers) [223]. Це спеціальний статус, який надається сертифікованим організаціям, зокрема державним структурам, незалежним неурядовим організаціям, що мають підтверджений експертний статус у сфері виявлення незаконного контенту або дезінформаційних матеріалів. Механізм роботи «довірених скаржників» докорінно змінює взаємодію між суспільством та платформами. Якщо раніше скарги користувачів могли залишатися без відповіді протягом тривалого часу, то повідомлення від сертифікованих організацій платформи зобов'язані розглядати у пріоритетному порядку та без невиправданих затримок. Більше того, онлайн-посередники повинні звітувати про результати розгляду таких скарг, пояснюючи свої рішення та демонструючи прозорість процесу. Статус «довіреного скаржника» надається національним Координатором цифрових послуг (Digital Services Coordinator) [27], який є незалежним органом у кожній державі-члені ЄС, що перевіряє відповідність організації критеріям незалежності та професійної компетентності.

Для громадянського суспільства, запровадження інституту «довірених скаржників» означає інституційне закріплення його ролі у політиці протидії дезінформації. Експертні громадські організації отримують своєрідний «зелений коридор» для прямої комунікації з технологічними корпораціями, що перетворює їх із пасивних спостерігачів, які раніше лише фіксували порушення у звітах, на активних учасників процесу модерації цифрового простору. Завдяки такій інтеграції вони здатні оперативно очищувати інформаційне середовище від скоординованих атак, здійснених ворожими акторами, і тим самим посилювати

стійкість демократичних інститутів. Показовим прикладом цього процесу є діяльність французького регулятора Arcom, який уже виконує функції координації на основі статті 22 DSA, збираючи дані про маніпуляції на платформах і забезпечуючи їхню підзвітність перед суспільством [84]. Така практика демонструє, що онлайн екосистема ЄС стає простором, в якому громадянське суспільство також є суб'єктом спільної відповідальності в реалізації політики протидії дезінформації.

На нашу думку, перспективи розвитку європейської онлайн екосистеми пов'язані з результатами повної інтеграції SCPD у правову структуру DSA. Офіційний старт цього процесу було дано 13 лютого 2025 р., коли Єврокомісія та Європейська рада з цифрових послуг ухвалили рішення про трансформацію Кодексу у статус офіційного Кодексу поведінки (Code of Conduct). На прохання підписантів (Додаток Л), серед яких були найбільші технологічні платформи Facebook, Instagram, TikTok, Google Search, цей перехід набув повної юридичної сили 1 липня 2025 р. [182]. Це політичне рішення докорінно змінило правила взаємодії у цифровому середовищі, адже боротьба з дезінформацією перестала бути сферою «доброї волі» корпорацій і перетворилася на систему жорстких юридичних зобов'язань. Відтепер дотримання положень Кодексу, що охоплюють прозорість політичної реклами, демонетизацію фейкового контенту та співпрацю з фактчекерами, стало для платформ ключовим критерієм виконання їхніх обов'язків зі зменшення системних ризиків відповідно до вимог DSA. Порушення цих норм більше не обмежується репутаційними втратами, а тягне за собою реальні фінансові санкції.

Для України цей зсув відкриває унікальне стратегічне вікно можливостей. Повна інтеграція нашої держави у Єдиний цифровий ринок ЄС, яка є частиною євроінтеграційного треку, дозволить автоматично поширити дію цих захисних інструментів на український інформаційний простір. Це означатиме кінець епохи «подвійних стандартів» модерації, коли платформи виділяли значно менші ресурси на безпеку в Східній Європі порівняно із Західною. Глобальні техногіганти будуть юридично зобов'язані модерувати український сегмент

інтернету, протидіяти російським ботофермам та маркувати дезінформацію за тими ж високими стандартами безпеки та під загрозою тих же гігантських штрафів, що діють для держав-членів ЄС.

Серед держав-членів ЄС найбільш комплексний підхід до побудови національної екосистеми протидії дезінформації застосовує Франція [266, p. 37-41]. Французька модель унікальна тим, що вона, покладаючись лише на м'яку силу та медіаграмотність, вибудовує жорстку вертикаль захисту, яка включає спеціалізоване законодавство, технічні служби розвідки та потужний регуляторний орган. Ця екосистема функціонує як скоординований інструмент, в якому кожен елемент відповідає за свій рівень безпеки. Основою екосистеми став ухвалений у 2018 р. закон, який створив унікальний правовий прецедент: під час виборчих кампаній французькі суди мають право протягом 48 годин розглядати позови та зобов'язувати цифрові платформи видаляти контент, якщо він є «явно неправдивим» і поширюється «масово та штучно», тобто за допомогою ботоферм. Це вивело проблему протидії дезінформації з теоретичної дискусії в площину правової процедури захисту виборчих прав [288]. У 2021 р. Франція створила технічне ядро екосистеми – згадувану VIGINUM, яка працює виключно з відкритими даними та виявляє технічні ознаки іноземного цифрового втручання (FIMI), тобто є «сенсором» екосистеми, який сигналізує про атаки ще до того, як вони досягнуть піку [287]. У 2022 р. в результаті злиття регуляторів телерадіомовлення (CSA) та інтернету (Hadopi) було створено супер-регулятора Arcom, який отримав безпрецедентні повноваження щодо нагляду за цифровими платформами. Arcom не модерує контент вручну, але контролює, чи виконують Facebook, Twitter (X), YouTube та інші свої зобов'язання щодо прозорості алгоритмів та боротьби з маніпуляціями. Саме Arcom є національним координатором цифрових послуг у рамках виконання DSA, забезпечуючи зв'язок між національним та загальноєвропейським рівнями регулювання [85].

Ще одним референтним прикладом моделювання онлайн екосистеми в протидії дезінформації є Естонія, яка ґрунтує її на системі обміну даними X-Road на основі децентралізованої та захищеної взаємодії між державними реєстрами

[161]. Коли 99 % державних послуг доступні онлайн [302], а кожен громадянин може перевірити, хто і коли переглядав його персональні дані (принцип прозорості), це руйнує ґрунт для конспірологічних наративів про «корумповану владу» чи «таємний контроль». Високий рівень довіри до цифрової інфраструктури дозволив Естонії артикулвати ідею i-Voting (інтернет-голосування), яка, попри численні спроби дискредитації з боку російської пропаганди, користується підтримкою понад 50 % виборців [353]. Це демонструє, що прозора цифрова екосистема сама по собі є антидотом від дезінформації, спрямованої на підрив легітимності інститутів влади. Реакція естонської системи на зростання загроз після 2022 р. продемонструвала концептуально новий рівень безпеки через реалізацію концепції Data Embassies, відповідно до якої критичні бази даних держави зарезервовані на серверах у Люксембурзі, які мають дипломатичний імунітет. Це нівелює один із ключових наративів гібридної війни, що відображений в загрозі перетворення держави на державу, що не відбулася. Навіть у разі окупації території, цифрова держава продовжує функціонувати, виплачувати пенсії та верифікувати громадян, що робить дезінформацію про «крах держави» беззмістовною [275]. Естонський досвід доводить, що цифровий вимір онлайн екосистеми є стратегічним інструментом інформаційної безпеки.

Цей досвід має пряму кореляцію з українськими реаліями. У 2022 р. Україна, наслідуючи естонський досвід, змогла врятувати свої цифрові реєстри, оперативно перемістивши їх у хмарні сховища за кордон. Цей крок зберіг керованість державою та став потужним сигналом для суспільства: держава існує, дані захищені, хаос, який пророкувала російська дезінформаційна машина, не настав [161]. Формування української онлайн екосистеми, ядром якої виступає концепція «держави у смартфоні», є репрезентативним прикладом адаптації до умов повномасштабної війни: по-перше, нормативна база формується в умовах воєнного стану, коли безпека та цифрова стійкість визначені пріоритетами національного виживання; по-друге, інституційна матриця включає Міністерство цифрової трансформації [38] та Центр протидії

дезінформації при РНБО [63]; по-третє, роль громадянського суспільства в Україні підтверджується масовим використанням чат-ботів («єВорог» [37]) та діяльністю OSINT-спільнот, що фактично інтегровані у систему національної розвідки; по-четверте, застосунок «Дія» вийшов далеко за межі класичного інструменту надання адміністративних послуг, ставши каналом прямої, верифікованої та двосторонньої комунікації між державою і громадянином. В умовах інформаційного хаосу та спроб ворога посіяти паніку, «Дія» забезпечила державі монополію на достовірність у кишені кожного українця. Інтеграція спеціалізованих воєнних сервісів, таких як чат-бот «єВорог» (для безпечного повідомлення про пересування окупантів), можливість купівлі військових облігацій та участь в опитуваннях щодо дерусифікації, перетворила застосунок на інструмент залучення кожного громадянина до активної оборони держави. Фактично, «Дія» стала цифровим відображенням суспільного договору воєнного часу, за якого кожен користувач є не просто отримувачем послуг, а й учасником національного спротиву [35].

Іншим показником адаптивності української екосистеми є застосунок «Повітряна тривога» [45]. Розроблений у рекордні терміни завдяки синергії держави та IT-сектору (Ajax Systems, Stfalcon), він еволюціонував від простої системи оповіщення про небезпеку до повноцінного безпекового медіа-хабу. Застосунок став всеохопним інструментом виживання: окрім сповіщень про загрози, він інтегрував розділ «Корисне» з посиланнями на офіційні ресурси для допомоги переселенцям, координаційні чати волонтерів та мапи укриттів. Інтеграція офіційних новин та інструкцій з безпеки безпосередньо в застосунок дозволила частково витіснити сумнівні анонімні Telegram-канали з ніші оперативного інформування. Як зазначається у дослідженнях, саме наявність таких довірених цифрових інструментів, розроблених державою та присутніх у смартфонах більшості населення, знижує запит суспільства на альтернативні, часто маніпулятивні джерела інформації в кризові моменти [277, p. 183]. Українська національна модель екосистеми демонструє, як технології можуть консолідувати суспільство та забезпечувати стійкість держави перед обличчям

екзистенційної загрози. На відміну від європейської моделі, в якій ключову роль відіграють платформи-посередники, українська модель базується на прямій цифровій взаємодії держави та громадян через довірені мобільні застосунки. Концептуальна різниця полягає в тому, що європейська модель є регуляторною (держава встановлює правила для посередників), то українська є інфраструктурною (держава створює власну альтернативну екосистему).

Для української національної моделі онлайн екосистеми як інструменту протидії дезінформації актуальною є нерозв'язана проблема анонімних телеграм-каналів. За даними комплексного дослідження медіаспоживання, проведеного на замовлення USAID-Internews, частка українців, які використовують Telegram для отримання новин, стабільно зростала протягом останніх років. Станом на кінець 2024 – початок 2025 рр. цей показник сягнув 73–75 % серед дорослого населення. Для порівняння, друге за популярністю джерело (YouTube) охоплює лише близько 19–21 %, що демонструє фактичну монополію Telegram у сфері оперативного інформування, а відтак, поширення дезінформації [261]. Така концентрація аудиторії на платформі з анонімними каналами створює безпрецедентну вразливість українського суспільства до дезінформації, оскільки понад дві третини громадян України щодня споживають контент, який не проходить жодної редакційної перевірки та не підпадає під дію Закону «Про медіа» [47]. На відміну від глобальних платформ (Meta, Google, TikTok), що підпадають під дію європейського DSA та зобов'язані дотримуватися стандартів прозорості, Telegram тривалий час уникав системного співрегулювання, що перетворило його на ключовий інструмент проведення операцій іноземного інформаційного маніпулювання та втручання.

Небезпека анонімних мереж полягає у відсутності механізмів атрибуції та ідентифікації джерела, оскільки архітектура платформи дозволяє ворожим акторам маскувати зовнішні дезінформаційні кампанії, що створює умови для руйнування інфраструктурної довіри до офіційних каналів комунікації (як-от застосунок «Дія»), оскільки анонімні джерела оперують емоційно забарвленим контентом, що не проходить жодних фільтрів чи верифікації. За даними

аналітичних звітів Atlantic Council (DFRLab), саме анонімність та відсутність алгоритмічної модерації дозволяють Telegram-каналам ставати центрами поширення панічних настроїв, дискредитації державних інститутів та координації деструктивної діяльності в умовах гібридної війни [153]. Більше того, Telegram-канали часто виступають інструментом «обходу» санкційних обмежень, запроваджених ЄС проти російських державних медіа, ретранслюючи заборонені наративи через мережу анонімних проксі-ресурсів. У контексті необхідності посилення стійкості до дезінформації, небезпека таких каналів полягає у спробах ерозії національної єдності через гру на внутрішніх суперечностях, що вимагає посилення технічного моніторингу та розвитку альтернативної, державної інфраструктури сповіщення [322].

Отже, формування онлайн екосистеми як інструменту протидії дезінформації в ЄС є комплексним процесом, що поєднує цілеспрямоване інституційне конструювання з еволюцією мережевих взаємодій. Водночас жодна інфраструктурна модель на сьогодні не є універсальною, оскільки дезінформація залишається багатовимірною загрозою, яка не має єдиного технічного чи регуляторного рішення. Відтак, основним завданням європейської онлайн екосистеми є забезпечення системної координації всіх суб'єктів, які протидіють інформаційним маніпуляціям. Сформовані європейські практики дозволяють стверджувати, що результативність онлайн екосистем може оцінюватися через ефективність визначеного рівня прозорості. Згідно з вимогами DSA, платформи зобов'язані надавати незалежним дослідникам доступ до своїх внутрішніх даних (API), що дозволяє вперше в історії об'єктивно виміряти реальні масштаби дезінформаційних кампаній. Проте залишається відкритим питання «асиметрії виконання», оскільки ефективність політики ЄС часто нівелюється здатністю іноземних акторів швидко адаптувати методи маніпуляції до нових алгоритмічних обмежень, що вимагає постійного оновлення критеріїв оцінки ризиків [113, p. 235–241, 243, 250–252].

Аналіз європейської онлайн екосистеми свідчить про оновлення парадигми її формування від парадигми «саморегульованого інтернету» до

парадигми інструменту забезпечення безпекового середовища. Головним досягненням тут є впровадження моделі співрегулювання, в якій техногіганти вперше отримали правові зобов'язання в межах DSA та Кодексу практики.

Здійснений аналіз формування онлайн екосистеми дозволяє визначати їх як перспективний інструмент політики протидії дезінформації в ЄС, що остаточно не сформувався, але може бути ідентифікований через низку типових характеристик, в яких відображена логіка його інституційної еволюції та функціонального розширення. По-перше, онлайн екосистема ґрунтується на інституційному закріпленні правил взаємодії між державними органами, приватними платформами та громадянським суспільством, що забезпечує легітимність і сталість процесів модерації контенту. По-друге, її розвиток демонструє ефект поступового нарощування компетенцій, коли нові інструменти, такі як Посилений кодекс практики щодо дезінформації 2022 р. чи інтеграція його у правову структуру DSA у 2025 р., перетворюються на обов'язкові стандарти діяльності для технологічних гігантів, включно з Facebook, Instagram, TikTok та Google Search. По-третє, онлайн екосистема характеризується децентралізованою архітектурою, що спирається на мережу національних і регіональних хабів, як у випадку EDMO, створеної у 2020 р., яка об'єднує фактчекерів, дослідників, експертів з медіаграмотності та представників медіаіндустрії. По-четверте, вона функціонує як середовище транскордонної координації, що дозволяє виявляти «переміщені наративи» та організовувати обмін даними у режимі реального часу. По-п'яте, онлайн екосистема забезпечує інституційне включення громадянського суспільства, яке отримує прямий доступ до комунікації з платформами, як у випадку французького регулятора Arcom, що координує виконання DSA. По-шосте, вона створює нову модель відповідальності, в якій прозорість алгоритмів і звітність компаній стають обов'язковими елементами цифрової безпеки в організації протидії дезінформації. По-сьоме, екосистема формує механізм примусовості, коли порушення правил більше не обмежується репутаційними втратами, а тягне

за собою фінансові санкції, що було закріплено після набуття Кодексом практики юридичної сили 1 липня 2025 р.

Висновки до розділу 3

Здійснений аналіз безпекових інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни вказує на те, що стратегічні комунікації ЄС як інструмент реалізації політики протидії дезінформації зазнав трансформації від фрагментарних реактивних практик до інституційно закріпленої політики «стратегічного наративу». Їхня ефективність ґрунтується на здатності поєднувати технологічні механізми викриття неправдивих повідомлень із формуванням власних наративів, які закріплюють легітимність європейського курсу та консолідують суспільства навколо європейських демократичних цінностей. Важливим є те, що ці комунікації функціонують як частина офіційного дискурсу взаємопов'язаних інституцій, тому кожна нова ініціатива створює ефект «ланцюгової реакції», підсилюючи інші напрями політики протидії дезінформації у безпековому вимірі. Саме ця логіка взаємозалежності пояснює, чому навіть обмежені ресурси можуть бути компенсовані ефектом накопичення результату та взаємного підсилення інститутів. Водночас стратегічні комунікації ЄС виконують функцію адаптації до нових викликів, коли зовнішні загрози змушують інституції розширювати власні компетенції та створювати нові механізми координації. Це проявляється у поступовій інституціоналізації таких інструментів, як RAS та StratCom Task Forces. Кожен із цих елементів, виконуючи свою безпосередню функцію в протидії дезінформації, стає каталізатором для формування нових стандартів колективної дії, що зміцнює стійкість європейських інститутів та громадян до споживання дезінформаційних наративів. Таким чином, стратегічні комунікації ЄС є інструментом, який одночасно забезпечує захист від дезінформації та створює умови для поглиблення інтеграційних процесів, адже боротьба з маніпуляціями стає спільним інтересом, що об'єднує держави-члени та партнерів.

Дослідження особливостей формування системи цифрових безпекових механізмів протидії дезінформації в ЄС дає підстави зробити висновок, що період з 2014 по 2025 рр. став етапом *примусового дорослішання* європейської

системи цифрової безпеки як інструменту протидії дезінформації. Якщо на початку російської агресії у 2014 р. реакція ЄС мала переважно символічний та реактивний характер, то на сьогодні спостерігається поєднання політичної волі у протидії дезінформації з жорсткою нормативною базою, синергією державних інституцій та громадянського суспільства, міжнародною кооперацією між державами-членами ЄС та використанням нейромережевих технологій. Головним результатом цієї еволюції стала відмова від трактування дезінформації як «фейкових новин» і перехід до концепції FIMI, що дозволило змістити акцент із боротьби з окремими інформаційними вкидами на виявлення ворожих суб'єктів та їхніх методів. Створення спеціалізованих оперативних груп (Task Forces) та Системи швидкого сповіщення (RAS) надало ЄС необхідну гнучкість, дозволивши враховувати культурні особливості різних регіонів світу при збереженні єдиного інформаційного периметра. Виявлено, що комунікаційних зусиль недостатньо, доки цифрові платформи залишаються вразливими за своєю архітектурою. Саме тому стратегія ЄС перейшла до формування цифрових інструментів протидії дезінформації на основі DSA та Акту про штучний інтелект. Інтеграція технологій ШІ в цифрові інструменти протидії дезінформації (VERA.ai та AI4TRUST) в поєднанні з технологіями цілісності даних (KSI та «Трембіта») формують «цифрове алібі» держави, забезпечуючи незмінність логів та децентралізацію реєстрів, що робить марними спроби ворога поширювати дезінформаційні наративи про неспроможність європейських держав-членів та держав-кандидатів ЄС протидіяти інформаційним викликам.

Принципове значення для дієвої сукупності безпекових інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни має формування національних онлайн екосистем у сфері протидії дезінформації, поряд із загальноєвропейською, оскільки саме вони забезпечують інституційне закріплення локальних практик та адаптацію загальних правил до специфіки мовного, культурного та політичного контексту кожної країни. Національні екосистеми виступають як автономні інституційні вузли, що інтегрують державні органи, громадянське суспільство, академічні спільноти та

технологічні компанії у власний простір взаємодії, створюючи умови для оперативного реагування на загрози, які мають локальне походження або специфічні форми прояву. Їхня цінність полягає у тому, що вони здатні виявляти та нейтралізувати наративи, які залишаються непомітними для централізованого моніторингу. Водночас загальноєвропейська екосистема виконує функцію інтеграційного каркасу, який забезпечує єдині стандарти прозорості, відповідальності та підзвітності для всіх учасників цифрового простору та створює умови для транскордонної координації. Таким чином, національні екосистеми співвідносяться із загальноєвропейською як взаємодоповнюючі рівні: перші забезпечують глибину та деталізацію у локальному вимірі, другі гарантують узгодженість і примусовість виконання правил у наднаціональному просторі. Ця взаємодія створює ефект функціонального розширення, коли кожна нова сфера застосування технологій та інституційних практик на національному рівні інтегрується у загальноєвропейську систему, посилюючи її стійкість. Водночас інституційна логіка передбачає, що національні екосистеми не є ізольованими утвореннями, а функціонують як частини ширшої архітектури, в якій локальні знання та глобальні стандарти протидії дезінформації взаємно підсилюють одне одного. У результаті формується багаторівнева модель політики протидії дезінформації, в якій національні екосистеми забезпечують адаптацію та деталізацію, а загальноєвропейська екосистема гарантує узгодженість, легітимність і незворотність процесу.

РОЗДІЛ 4
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ІНСТРУМЕНТИ РЕАЛІЗАЦІЇ ПОЛІТИКИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

4.1. Формування системи засобів верифікації інформації

Проаналізована вище інституційна основа європейської та української системи протидії дезінформації визначає лише загальні стратегічні межі та нормативні правила її функціонування. Для реального захисту інформаційного простору від дезінформаційних атак однієї лише наявності інституцій та правових рамок недостатньо, оскільки вони потребують наповнення конкретними прикладними інструментами та методами, які здатні працювати з інформаційними атаками безпосередньо в момент їх виникнення [9, с. 38-41]. Якщо інституції є базою, то інформаційно-комунікаційні інструменти, такі як верифікація, медіаосвіта та мережева активність громадянського суспільства, є конкретними інструментами, які забезпечують фізичне виявлення та нейтралізацію загрози в режимі реального часу. Саме тому в четвертому розділі ми переходимо до детального розгляду практичного інструментарію, що забезпечує національну стійкість засобами інформаційно-комунікаційних технологій [333, p. 18].

Верифікація інформації це один з основних інструментів протидії дезінформації на етапі її появи в інформаційному просторі. Умовно, можна означити інструмент верифікації інформації, як реактивний, на відміну від інструментів медіаосвіти, які є більше превентивними. Як зазначають у своєму дослідженні К. Вардлі та Х. Дерашхан, верифікація є критичною ланкою, що дозволяє локалізувати «інформаційний розлад» (information disorder) до моменту його масового поширення [392, p. 67]. Водночас верифікація є інструментом першої черги, до якого має вдаватися громадянин при зіткненні із сумнівною новиною, що перетворює її на елемент індивідуальної цифрової гігієни. Проте на рівні системи політичних інститутів вона трансформується у складну систему,

що охоплює механізми виявлення, фільтрації та технічної атрибуції дезінформаційних наративів. У загальній моделі протидії дезінформації в державах-членах ЄС верифікація «посідає місце центрального операційного вузла. Верифікація виступає системою і ланкою в загальній архітектурі протидії дезінформації в країнах Європейського Союзу» [110, p. 52]. Унікальність цього завдання для ЄС, як підкреслює дослідниця Н. Бентзен, полягає у необхідності одночасної роботи з контентом на десятках офіційних мов, враховуючи при цьому специфічні історичні контексти та регіональні вразливості, які експлуатує агресор [99].

Верифікація, як інформаційно-комунікаційний інструмент протидії дезінформації, повинен включати декілька субінструментів для виявлення, фільтрації та протидії дезінформаційних наративів. Правове визначення поняття верифікація, зазвичай прив'язується до сфери застосування, приміром медичної чи фінансової. Наприклад у Законі України «Про верифікацію та моніторинг державних виплат» зустрічаємо таке визначення: «верифікація – комплекс заходів щодо збору та перевірки достовірності інформації, що визначена законодавством для призначення, нарахування та/або здійснення державних виплат і впливає на визначення права на отримання та розмір таких виплат, а також виявлення невідповідності даних у автоматизованих інформаційних системах, реєстрах, базах даних» [46]. А в постанові Кабінету Міністрів України від 15 квітня 2020 р. зміст верифікації означений як «комплекс заходів з порівняння, встановлення відповідності та підтвердження відомостей, що містяться в реєстрах центральної бази даних, з відомостями, що містяться в тих самих або інших реєстрах центральної бази даних або інших державних інформаційних ресурсах, а також відомостями, одержаними, зокрема шляхом електронної взаємодії, від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, які є володільцями та/або розпорядниками таких відомостей, відомостей, одержаних у результаті заходів з моніторингу виконання умов договорів та перевірки НСЗУ» [22].

В англомовних джерелах поняття «верифікація» вживається поруч з поняттям «валідація». Верифікація та валідація є незалежними процедурами, які використовуються для перевірки того, що продукт, послуга чи система відповідають певним вимогам, а також відповідають призначенню [236, p. 3]. В науковому дискурсі верифікація в контексті протидії дезінформації розглядається в нерозривному зв'язку з поняттям «валідація». За визначенням Р. Прессмана, цей дуалістичний підхід дозволяє відповісти на два ключові запитання: «чи правильно ми будуємо систему?» (верифікація) та «чи правильну систему ми будуємо?» (валідація) [342]. Для формування системи інформаційно-комунікаційних інструментів реалізації політики протидії дезінформації в умовах гібридної війни ця концепція набуває особливого значення, оскільки верифікація відповідає за технічну перевірку факту на достовірність, тоді як валідація дозволяє оцінити, чи відповідає обраний метод спростування меті протидії дезінформації – нейтралізації її деструктивного впливу на аудиторію. Як підкреслює С. Андрьоль, у сучасному інформаційному середовищі верифікація трансформується з суто процедурного акту на інструмент стратегічного управління дезінформаційними ризиками. Це дозволяє фіксувати невідповідність даних та викривати логіку поширення дезінформації, що є критично важливим для збереження стійкості демократичних інститутів [83, p. 115]. В нашому подальшому дослідженні перевірка інформації на достовірність буде позначатись словом «верифікація», тобто як перевірка, за якою, відповідно до європейських принципів протидії дезінформації, автоматично слідує викриття, висвітлення і як результат протидія, нейтралізація первинного деструктивного призначення фейку, чи маніпуляції.

Для глибшого розуміння об'єкта верифікації доцільно звернутися до класифікації, запропонованої дослідницею у сфері інформаційних процесів К. Вордл. У своїй доповіді, підготовленій для європейських політичних інституцій, вона обґрунтувала необхідність відмови від спрощеного терміну «fake news» на користь терміну дезінформація, який відповідає концепту «інформаційного розладу». К. Вордл виокремлює три типи шкідливої інформації, що є критично

важливим для побудови механізму протидії їй в умовах гібридної війни: місінформація як хибна інформація без наміру завдати шкоди; дезінформація як свідомо створена неправдива інформація з метою заподіяння шкоди; дезінформація як malinformation – правдива інформація, яка використовується зловмисно для завдання шкоди, наприклад, злив приватних даних [393]. Така градація дозволяє верифікаторам чітко розрізняти помилки журналістів та цілеспрямовані спецоперації ворога, застосовуючи до них різні інструменти реагування. Відповідно, верифікація інформації – це процес перевірки точності та достовірності будь-яких даних, фактів чи тверджень. Подекуди, науковці використовують поняття «фактчекінг», що є синонімом верифікації, адже обидва поняття вказують на перевірку достовірності, але верифікація це ширше системне поняття. Цю думку поділяє і українська дослідниця Н. Карпчук, яка наголошує, що в умовах гібридної війни ЄС переносить верифікацію з поля професійного обов'язку журналіста на поле політичної відповідальності, створюючи єдину «публічну сферу» захисту від зовнішніх маніпуляцій [25, с. 75].

Методи верифікації різноманітні та дозволяють виявити будь які дезінформаційні прояви. Неурядові та державні організації використовують ряд інструментів та прийомів: ідентифікація джерел (ви можете відстежити, звідки пішла інформація, і оцінити надійність джерела) [365]; порівняння з іншими джерелами (інструменти дозволяють порівняти інформацію з різних джерел і виявити суперечності); аналіз мови (за допомогою спеціальних алгоритмів можна виявити ознаки пропаганди, емоційної маніпуляції та інших прийомів дезінформації) [405]; аналіз відео та аудіо (програмне забезпечення, яке дозволяє перевіряти відеоконтент на правдивість за допомогою зворотного пошуку кадрів або аудіоредактори, що дозволяють аналізувати звукові файли на наявність змін або монтажу).

Існують інструменти, котрі не дають готової відповіді, але відкривають для користувача можливості перевірити достовірність інформації. Для прикладу людина, котра свідомо і уважно ставиться до споживання інформації може

використовувати складні та затратні по часу інструменти: зворотний пошук зображень, який дозволяє знайти першоджерело зображення та перевірити, чи не було воно змінено, за допомогою Google Images чи TinEye [250]. Також можна вдатися до виконання певного алгоритму дій: оцінити джерело (хто, коли і з якою метою поширив певне повідомлення), перевірити джерела (реальність події, свідків, статистичні дані), звернути увагу на наявність апеляції до емоцій, звірити з іншими джерелами інформації, проаналізувати візуальний супровід на сліди фабрикації. Слід підкреслити, що в умовах «обчислювальної пропаганди» верифікація перестає бути лише інтелектуальною дією і стає симбіозом експертних дій людини та алгоритмічної обробки даних, що дозволяє масштабувати спростування відповідно до швидкості поширення дезінформаційних хвиль. Звичайно всі вище перелічені інструменти є загальнодоступними, але використовуються в більшості випадків фахівцями, а не громадянами ЄС.

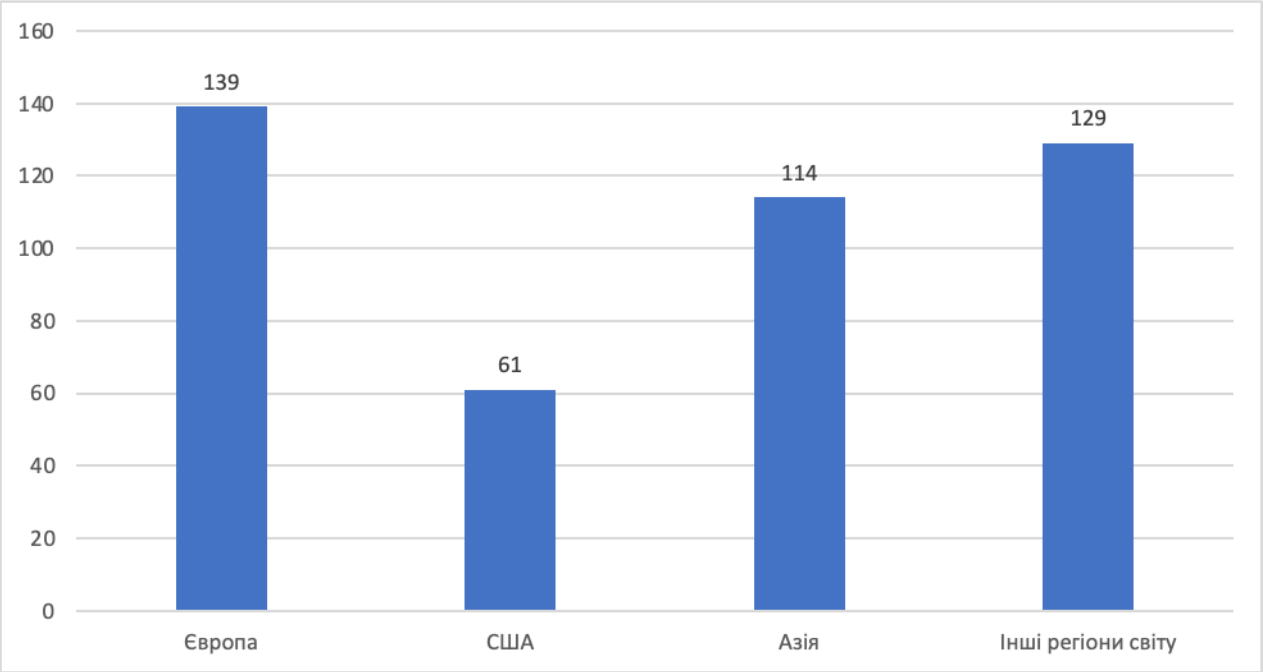
Процес верифікації інформації в процесі протидії дезінформації є структурованим алгоритмом, що базується на випробуваних та міжнародно визнаних стандартах. Зокрема, методологія більшості професійних фактчекінгових організацій, що діють в ЄС, спирається на принципи Кодексу етики Міжнародної мережі фактчекінгу [259]. Спочатку завжди здійснюється ідентифікація, коли інституція виокремлює новину чи твердження, що потребує перевірки. Потім відбувається вибір інструментарію, а він в свою чергу вже залежить від технічних можливостей та ресурсів (людських або фінансових) [198]. Далі етап збору доказів в авторитетних першоджерелах, одночасно класифікуючи їх за критеріями: правда, дезінформація, маніпуляція. Після відбувається аналіз та систематизація. І тільки після експертної редакції відбувається публікація або оприлюднення результатів із обов’язковим наданням читачеві всіх посилань на використані докази. Тобто до споживачів інформації доходить спростування за яким стоїть цілий механізм, вироблений в умовах неперервності дезінформаційних загроз [240]. Саме такий алгоритм

закладено в основу діяльності флагманського проєкту ЄС з протидії дезінформації EUvsDisinfo.

Технологічне забезпечення функціонування даного алгоритму автоматичної верифікації інформації в мережі здійснюється ЄС через власно створений інструментарій. Вдалим прикладом такої політики став проєкт InVID/WeVerify, реалізований за підтримки грантової програми Horizon 2020. Фактично, ЄС профінансував створення «цифрового помічника», який сьогодні став галузевим стандартом для європейських фактчекерів та дослідників дезінформації [379]. Цінність цього інструменту для політичного аналітика чи журналіста полягає в автоматизації складних технічних процесів. Плагін дозволяє за лічені секунди розкласти будь-яке підозріле відео з соцмереж на окремі кадри та перевірити, чи не публікувалися вони раніше в іншому контексті. Також він містить інтуїтивно зрозумілі фільтри, які підсвічують можливі сліди фотомонтажу або цифрового втручання у зображення. Завдяки такій технологічній підтримці, фахівці можуть оперативно реагувати на інформаційні вкиди, не витрачаючи години на ручну перевірку технічних параметрів контенту. Як вказано на сайті проєкту: «Мета WeVerify – вирішити актуальні проблеми перевірки контенту за допомогою партисипативного підходу до перевірки, алгоритмів з відкритим кодом, машинного навчання з низькими накладними витратами «людина в циклі» та інтуїтивно зрозумілої візуалізації. Контент соціальних мереж та веб-сайтів буде проаналізовано на предмет виявлення дезінформації; розглянуто в контексті ширшої екосистеми соціальних мереж та медіа; а оманливий та сфабрикований контент буде викритий як такий, за допомогою мікротаргетингового спростування та відкритих баз даних відомих фейків на основі блокчейну» [397].

Таким чином, платформи для перевірки фактів є основним засобом верифікації інформації, як для пересічного споживача, медіа, так і для дослідника дезінформації (Додаток М). Часто в ЄС вони постають не «згори», а «знизу». Тобто, фактчекінгові організації виникають спочатку як спільнота небайдужих громадян: журналістів, науковців, громадян, які розуміють важливість протидії

дезінформації. За даними щорічного звіту Duke Reporters' Lab, організації, що спеціалізуються на перевірці достовірності інформації, активно діють уже у 116 країнах світу. Станом на середину 2025 р. глобальна мережа налічувала 443 активні проєкти (Малюнок 4.1.1 [356]).



Малюнок 4.1.1. Регіональна структура організацій, що здійснюють верифікацію інформації

Дані малюнку 4.1.1 вказують на те, що Європа є безумовним лідером у цій сфері: тут функціонує 139 таких ініціатив, що є найвищим показником серед усіх регіонів світу. Значна їх частина зосереджена в державах-членах ЄС, однак потужні осередки верифікації діють і за його межами, зокрема в Україні. Наразі в українському медіапросторі працює 5 визнаних міжнародною спільнотою (індексованих у базі Duke) фактчекінгових організацій, три з яких мають офіційний статус підписантів Кодексу принципів IFCN: VoxCheck, StopFake та Ґвара Медіа [356].

Як приклад низової ініціативи, що масштабувалась, О. Гороховський [11] наводить чеську організацію Demagog.cz [150], яка є проєктом, що виник у 2012 р. в стінах Університету Масарика (м. Брно, Чехія) завдяки ініціативі студентів. Дана організація є важливим ресурсом для верифікації інформації та захисту від

російської дезінформації, адже на сайті організації є окремий розділ «Війна в Україні» [121]. Напис розміщений на початку розділу лаконічно роз'яснює контекст та мету висвітлення тематики російсько-української війни: «З лютого 2022 року, коли Росія вторглася в Україну, цей конфлікт став центральною темою публічних дискусій, а також вірусних постів у соцмережах. Demagog.cz постійно перевіряє правдивість окремих заяв чеських політиків, а також правдивість вибраного контенту Facebook та Instagram у рамках співпраці з Facebook» [149]. Щодо результатів верифікації, то варто звертатись до критеріїв конкретної організації. Demagog.cz пропонує критерії верифікації інформації, які можуть бути покладені в змістову основу системи інструментів верифікації інформації для протидії дезінформації (Таблиця 4.1.1.)

Таблиця 4.1.1

Критерії верифікації інформації

Правда	Інформація може бути визначена як достовірна лише тоді, коли вона узгоджується з відповідним контекстом і має можливість бути перевіреною через надійні джерела. У такому випадку вона не є просто набором фактів, а набуває статусу підтвердженого знання, що може бути використане для формування обґрунтованих висновків та прийняття рішень. Відповідність контексту гарантує коректність інтерпретації, а можливість перевірки забезпечує її об'єктивність та захищає від маніпуляцій. Саме поєднання цих двох умов (релевантності та верифікованості) дозволяє оцінювати інформацію як правдиву.
Неправда	Інформацію слід розглядати як недостовірну у випадках, коли її фактична складова не збігається з відкритими загальнодоступними даними або ж вона не має підтвердження у жодному релевантному джерелі, доступному для перевірки. За таких умов вона втрачає статус об'єктивного знання і перетворюється на потенційно маніпулятивний матеріал, що може вводити аудиторію в оману. Відсутність відповідності фактичній базі чи неможливість верифікації через авторитетні джерела є ключовими критеріями, які дозволяють кваліфікувати інформацію як неправдиву.
Оманливе твердження	Твердження втрачає свою достовірність тоді, коли використані факти, що самі по собі є правильними, але подані у

	викривленому контексті, який змінює їхнє значення або навмисно вириває їх із початкової логіки. У такому випадку інформація перестає бути нейтральним відображенням реальності й перетворюється на інструмент маніпуляції. До цієї категорії належать також порівняння, які зовні виглядають коректними, проте не мають належного зв'язку з предметом аналізу, створюючи хибні аналогії та вводячи аудиторію в оману. Саме невідповідні чи недоречні зіставлення, що ґрунтуються на формально правильних даних, але застосовані поза релевантним контекстом, становлять одну з найбільш поширених форм дезінформаційних практик.
Неможливо перевірити	Твердження класифікується як таке, що не підлягає перевірці, у випадку коли відсутня можливість знайти джерело, здатне підтвердити його фактичну достовірність. Іншими словами, якщо на основі відкритої та загальнодоступної інформації неможливо ані підтвердити, ані спростувати наведені дані, воно втрачає статус перевірюваного й переходить у категорію неперевірюваних тверджень. Така ситуація створює інформаційний вакуум, у якому неможливо встановити об'єктивність чи хибність повідомлення, що робить його потенційно небезпечним для коректного аналізу та використання у процесі прийняття рішень.

Складено за: [148].

Значення критеріїв верифікації інформації для формування інформаційно-комунікаційних інструментів протидії дезінформації полягає у тому, що вони створюють основу для інституційної довіри та посилюють функціональну ефективність європейської системи протидії дезінформації. Саме завдяки чіткому розмежуванню між правдивими, неправдивими та неперевірюваними твердженнями можливо вибудувати механізми, які дозволяють відфільтровувати інформаційні потоки та мінімізувати ризики маніпуляцій. Критерії перевірюваності гарантують, що комунікаційні інструменти спираються на дані, які відповідають контексту та можуть бути підтверджені. Визначення неправдивих тверджень через їхню невідповідність загальнодоступним джерелам дозволяє створювати алгоритмічні моделі, здатні автоматично ідентифікувати дезінформаційні матеріали та блокувати їх поширення. Категорія

неперевірюваних тверджень має особливе значення, адже вона вказує на інформаційні зони невизначеності, які потребують додаткового дослідження та аналітичної роботи, щоб уникнути хибних інтерпретацій. Таким чином, ці критерії можуть бути покладені в основу загальноєвропейських принципів верифікації інформації в процесі протидії дезінформації. Відповідно, модель діяльності Demagog.cz може бути референтною для європейського фактчекінгу, бо вона є незалежною (фінансується пожертвами читачів або грантами, переважно від ЄС), прозорою (на сайті доступні звіти організації), співпрацює з іншими організаціями, регулярно та своєчасно реагує на дезінформаційні вкиди (внутрішні та зовнішні). Варто також згадати, що організація виникла, як ініціатива студентів, котрі не ставили на меті сам заробіток або політичні амбіції, а саме верифікацію інформації та протидію дезінформації на тлі російської агресії проти України та Європи.

Усвідомлюючи, що окремі низові ініціативи, якими б ефективними вони не були, не здатні самостійно протистояти масованим дезінформаційним атакам, Єврокомісія ініціювала створення відповідної інституційної інфраструктури, до якої були включені: StratCom (з 2015 р.) [189] RAS (з 2018 р.) [166], EDMO (з 2020 р.) [381]. Найбільш відомим публічним продуктом East StratCom, який функціонує як інструмент верифікації, є флагманський проєкт EUvsDisinfo. Це не просто медіа, а відкрита база даних, що каталогізує тисячі верифікованих випадків прокремлівської дезінформації. Кожен запис у базі містить оригінальну цитату, її аналіз (верифікацію) та спростування з посиланням на фактичні дані [225]. Тому EUvsDisinfo слугує одночасно архівом для дослідників, інструментом підвищення обізнаності для громадськості та джерелом верифікованих даних для медіа та національних урядів [224].

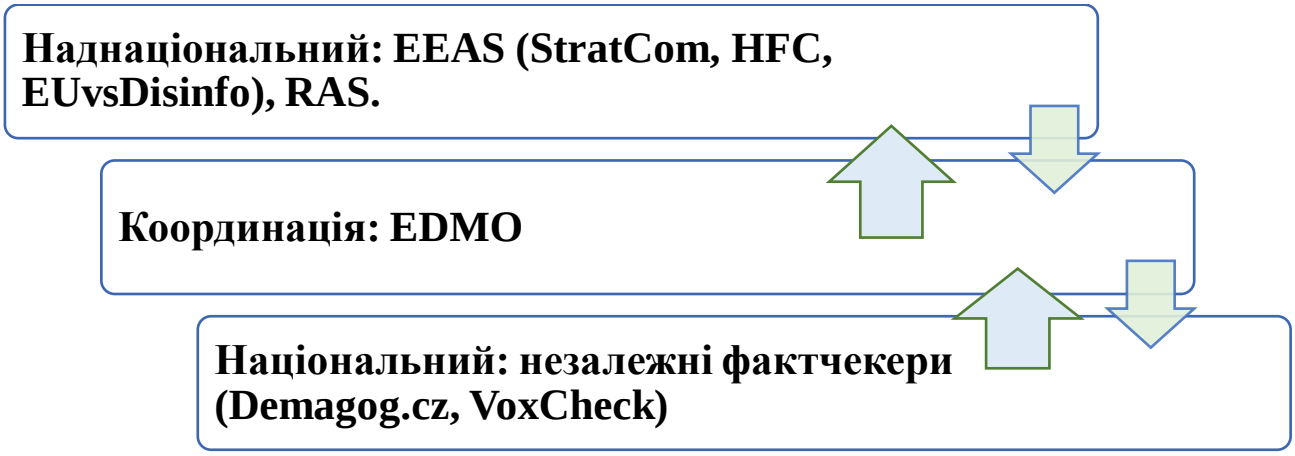
Важливим елементом системи верифікації інформації на інституційному рівні ЄС є гібридний аналітичний осередок EU Hybrid Fusion Cell (HFC), створений у структурі EEAS. На відміну від публічних платформ фактчекінгу, HFC діє як внутрішній «центр обробки даних», куди стікається інформація як з відкритих джерел, так і розвідувальні дані від держав-членів ЄС. Його створення

у 2016 р. стало відповіддю на потребу верифікувати не поодинокі фейки, а комплексні гібридні атаки, де дезінформація є лише одним із компонентів [167]. Аналітики осередку співставляють інформацію про кібератаки, економічний тиск та дезінформаційні вкиди, щоб підтвердити або спростувати наявність скоординованої ворожої кампанії з дезінформації. Такий підхід дозволяє верифікувати атрибуцію загрози, тобто, з високою долею ймовірності визначити її джерело (найчастіше, Росію або Китай). Це критично важливо для прийняття політичних рішень, адже санкції чи дипломатичні кроки вимагають верифікованої доказової бази, яка формується саме тут [254]. Осередок генерує понад 100 оцінок гібридних загроз на рік, які розповсюджуються серед держав-членів ЄС через інтегровані механізми [219]. Саме тому, HFC є хабом, що перетворює розрізнені дані на верифіковану аналітику для вищого політичного керівництва ЄС.

З інтеграцією в європейське поле протидії дезінформації засобів FIMI, що офіційно закріплена у стратегічних документах Європейської служби зовнішніх справ у 2021 р., має принципове значення для процесу верифікації [220]. Перехід до концепції FIMI означав, що в процесі верифікації інформації HFC та StratCom фокусуються не лише на перевірці фактологічної точності окремого повідомлення за дихотомічною моделлю *правда – брехня*, а на виявленні маніпулятивної поведінки, а це включає аналіз підозріло неприродної активності ботоферм, використання фейк-акаунтів, непрозоре замовлення політичної реклами. Верифікація у форматі FIMI дозволяє чітко відрізнити внутрішній європейський дискурс, від цілеспрямованих ворожих операцій зовнішніх акторів (Росія чи Китай), навіть якщо вони базуються на помилкових судженнях, що є критично важливим для збереження свободи слова в демократичному суспільстві [134]. Це позначилося і на стійкості до дезінформації, яка вимірюється за допомогою відповідного Індексу. Всі держави-члени ЄС, так само, як і Україна перебувають в зоні високих показників. Особливо за критерієм «Цифрова війна» (Digital warfare) [156]. Цей показник відображає здатність

держави та суспільства виявляти та нейтралізувати ворожі інформаційні операції на основі верифікованої інформації [89].

Таким чином, система інструментів верифікації інформації в ЄС є системою, що поєднує низові ініціативи громадянського суспільства, координовані через EDMO, з потужними наднаціональними аналітичними центрами (EEAS StratCom, HFC). Ця система підкріплена власними технологічними розробками (InVID та WeVerify) та унікальними регуляторними важелями впливу на глобальні платформи (DSA), що дозволяє ефективно протидіяти сучасним гібридним загрозам (Малюнок 4.1.1, складено автором).



Малюнок 4.1.1. Інституційна модель верифікації інформації в ЄС)

Важливість такої структури інституційної моделі верифікації інформації в ЄС визначається завданнями з протидії дезінформації. Завдяки EDMO громадські організації отримують можливість брати участь у процесі перевірки інформації, тоді як EEAS StratCom та HFC формують стратегічний рівень аналітики, що дозволяє узгоджувати дії у масштабі всього ЄС. Технологічні інструменти, такі як InVID та WeVerify, забезпечують технічну спроможність швидко ідентифікувати маніпулятивний контент, а регуляторні механізми, закріплені в DSA створюють правові рамки для примусу глобальних платформ до прозорості та відповідальності. Така інтегрована модель дозволяє ЄС ефективно реагувати на сучасні гібридні загрози, поєднуючи інституційні,

технологічні та нормативні ресурси в єдину систему, яка здатна захищати демократичний інформаційний простір ЄС від зовнішніх маніпуляцій та внутрішніх вразливостей. На сьогодні верифікація інформації в ЄС вийшла за межі функції медіа та набула ознак компоненту безпекової політики. Ключовою особливістю європейської моделі є її дворівнева архітектура. Вона вдало поєднує гнучкість незалежних громадських фактчекерів із потужним аналітичним ресурсом наднаціональних інституцій, таких як StratCom чи Hybrid Fusion Cell. Важливо, що ця система не розірвана: координаційні майданчики, насамперед EDMO, забезпечують єдині стандарти та швидкий обмін даними між усіма учасниками. Крім того, аналіз засвідчив перехід ЄС до проактивної позиції. Завдяки впровадженню концепції FIMI фокус змістився з простої перевірки контенту на виявлення маніпулятивної поведінки іноземних акторів. Показово, що для цього ЄС використовує весь арсенал засобів: від власних технологічних розробок (InVID) до жорсткого регуляторного тиску на глобальні платформи через DSA.

Попри свою технологічність, створена в ЄС модель верифікації інформації має кілька системних вад, які в умовах реальної ескалації політики дезінформації з боку Росії, Китаю чи держав ІДІЛ можуть стати критичними. По-перше, це бюрократична інерція. Поки RAS проводить політичні узгодження між 27 країнами-членами ЄС, дезінформаційні мережі, що діють без будь-яких етичних та правових обмежень, встигають «засіяти» інформаційне поле ЄС тисячами дезінформаційних повідомлень. Відтак, йдеться про конфлікт швидкостей: бюрократична машина ЄС рухається у правовому полі, тоді як держави-генератори дезінформації працюють у полі невизначеного регулювання. По-друге, зберігається критична залежність від платформ. Навіть під тиском DSA, технічні гіганти (Meta, X, TikTok) неохоче відкривають «чорну скриньку» своїх алгоритмів. Верифікатори часто бачать лише наслідки маніпуляцій, а не механіку їхнього поширення, що уповільнює процес застосування проактивних стратегій протидії дезінформації. По-третє, існує регіональний дисбаланс експертизи. Ресурси EDMO часто концентруються навколо західноєвропейських

мовних сегментів, тоді як східний європейський фланг, який першим приймає інформаційний удар, змушений покладатися на обмежені локальні ініціативи.

Таким чином, здійснений аналіз особливостей процесу формування системи засобів верифікації інформації як інструменту реалізації європейської політики протидії дезінформації в ЄС дозволив визначити низку його особливостей. По-перше, він розгортався на основі інституційного закріпленні правил, що забезпечують легітимність та сталість взаємодії між державними органами, цифровими платформами та громадянським суспільством в реалізації процедури верифікації інформації. По-друге, спостерігається поступове розширення функціональних компетенцій, коли нові інструменти перевірки інформації інтегруються у вже існуючі механізми протидії дезінформації, створюючи ефект накопичення та посилення. По-третє, система має багаторівневу структуру, в якій локальні ініціативи громадських організацій координуються через EDMO, а наднаціональні структури, такі як EEAS, StratCom та HFC, забезпечують стратегічний рівень аналітики. По-четверте, важливою рисою є транскордонна координація процесу «закритої» верифікації, яка дозволяє виявляти та нейтралізувати інформаційні атаки, що поширюються одночасно у кількох країнах. По-п’яте, в процесі формування системи засобів верифікації інформації, як інструменту реалізації європейської політики протидії дезінформації, ЄС інтегрує технологічні інновації, зокрема інструменти InVID та WeVerify, які забезпечують технічну спроможність швидкої перевірки контенту. По-шосте, логіка процесу спирається на нормативні механізми примусу, закріплені в DSA, що створюють юридичні рамки для відповідальності глобальних платформ. По-сьоме, процес формування засобів верифікації інформації характеризується взаємним підсиленням локальних знань та наднаціональних стандартів, що забезпечує узгодженість і стійкість у протидії гібридним загрозам.

Кортоткостокова перспектива перетворення системи верифікації на справді дієвий інформаційно-комунікаційний інструмент протидії дезінформації пов’язується нами з більш активним використанням засобів ШІ, тоді як

середньострокова перспектива розвитку системи верифікації інформації в ЄС може бути означена як етап консолідації та посилення, коли існуючий каркас поступово перетворюється на стійку й більш ефективну модель. У цьому часовому вимірі головним завданням стає інституційне зміцнення: узгодження локальних практик із наднаціональними стандартами, зменшення фрагментації між країнами та формування спільних критеріїв верифікації інформації.

4.2. Компетентністні інструменти формування стійкості до дезінформації

Якщо інструменти верифікації, розглянуті у попередньому підрозділі, є реактивним інструментом протидії дезінформації, спрямованим на боротьбу вже з наявними дезінформаційними повідомленнями та наративами, то медіаграмотність (media literacy) та медіаосвіта (media education) є превентивним стратегічним інструментом протидії дезінформації [204]. В умовах гібридної війни цей інструмент остаточно перейшов із суто освітньої площини у сферу безпеки ЄС [307]. Сек'юритизація медіаграмотності в ЄС означає перетворення цієї компетенції з факультативної освітньої навички на ключовий елемент інституційної стійкості, що забезпечує захист демократичних процесів від зовнішніх інформаційних маніпуляцій та втручань. У межах оновленої Стратегії кібербезпеки ЄС (2024–2025 рр.) медіаграмотність закріплена як критична вимога, яка формує когнітивний простір у статусі повноцінної оборонної зони [194]. Це свідчить про перехід від логіки реактивного «виправлення помилок» до логіки превентивного «запобігання зараженню», в якій громадянин постає носієм колективної стійкості (стійкості громад) [297].

Повномасштабне вторгнення Росії в Україну у 2022 р. стало каталізатором цього процесу, чітко продемонструвавши, що технологічні та регуляторні інструменти, зокрема ASD, не можуть бути ефективними без когнітивного «щита». Оскільки основна мета російських інформаційних операцій у державах-членах ЄС полягає у підриві суспільної єдності, ерозії довіри до демократичних інститутів та послабленні політичної волі щодо підтримки України, політика ЄС

у цій сфері спрямована на блокування ворожих наративів та довгострокове формування «колективного імунітету», тобто виховання критично мислячого громадянина, здатного самостійно ідентифікувати маніпулятивні техніки та чинити їм опір. Для України цей досвід є показовим, оскільки у сучасному ЄС медіаосвіта розглядається як фундаментальний елемент інформаційно-комунікаційного механізму протидії гібридним загрозам, тоді як українська система середньої освіти орієнтована переважно на підготовку до складання НМТ, а не на формування свідомого громадянина, готового до викликів інформаційної доби. Це підкреслює необхідність переорієнтації освітньої політики на розвиток когнітивної стійкості, що стає невід'ємною складовою національної безпеки.

Усвідомлення медіаграмотності як дієвого інформаційно-комунікаційного інструменту протидії дезінформації в ЄС має чітке інституційне закріплення і не обмежується декларативними формулюваннями, а відображене у нормативних та стратегічних документах, які створюють багаторівневу рамку зобов'язань і механізмів реалізації. На правовому рівні фундаментом виступає Директива про аудіовізуальні медіапослуги (Audiovisual Media Services Directive, AVMSD), оновлена у 2018 р. як відповідь на нові виклики цифрового середовища. Стаття 33а цієї редакції вперше юридично зобов'язала всі 27 держав-членів ЄС здійснювати заходи з розвитку медіаграмотності та регулярно звітувати про їх виконання перед Єврокомісією [172]. Таким чином, медіаосвіта була переведена зі статусу рекомендаційного інструменту у площину юридичного обов'язку, що означає інституціоналізацію цієї сфери у межах європейського правового простору. На стратегічному рівні медіаграмотність визначена як один із ключових стовпів захисту демократії у Плані дій з європейської демократії, представленому у 2020 р. [175]. У цьому документі стійкість демократичних процесів, зокрема виборів, прямо пов'язується зі здатністю громадян приймати протистояти маніпуляціям. План передбачає конкретні заходи для посилення медіаграмотності та підтримки громадянського суспільства, яке працює у цій сфері, розглядаючи їх як відповідь на зловмисне іноземне втручання. На рівні

освітніх практик реалізується План дій у галузі цифрової освіти (2021–2027), який закріплює другий стратегічний пріоритет – «Посилення цифрових навичок та компетентностей» [174]. У його межах передбачено розробку настанов для вчителів щодо виховання цифрової грамотності та боротьби з дезінформацією. Це означає інвестицію у формування когнітивного «щита» майбутніх поколінь європейців, що має забезпечити довгострокову стійкість суспільства до інформаційних маніпуляцій.

Повномасштабне вторгнення Росії в Україну у 2022 р. стало потужним каталізатором для негайної мобілізації інституційних механізмів ЄС в протидії дезінформації. EDMO, що виконує функцію координаційного центру, оперативно створила спеціальну робочу групу, спрямовану на аналіз та узгодження ініціатив у сфері медіаграмотності як прямої відповіді на дезінформацію в умовах російсько-української війни [194]. Згідно зі звітом EDMO, саме вторгнення 2022 р. спричинило масштабну хвилю низових ініціатив у державах-членах ЄС, які були спрямовані на розвиток критичного мислення та когнітивної стійкості громадян. До цього процесу активно долучилися профільні неурядові організації, університети, суспільні мовники, освітні центри та бібліотечні спільноти, що розширили коло суб’єктів протидії дезінформації. Багато з цих проєктів реалізовувалися через партнерські моделі між різними інституціями, а окремі отримували пряму фінансову підтримку від національних урядів, що вказує на розуміння загроз на всіх рівнях політичної та соціальної системи. Геоаналіз звіту зафіксував найбільшу активність у двох групах держав. Перша група – це держави, що безпосередньо межують із війною або мають історичний досвід протистояння Росії, серед яких Естонія, Литва, Чехія та Фінляндія. Друга група – це держави з глибоко усталеними традиціями медіаосвіти, такі як Бельгія, Нідерланди та Данія. Водночас автори звіту наголосили на певній асиметрії реагування, відзначивши відсутність вичерпних даних від найбільших днржав-членів ЄС, зокрема Франції, Німеччини та Польщі, які мають значні ресурси для реалізації подібних програм [197]. Таким чином, інституційні механізми ЄС були миттєво адаптовані до нових умов, а

функціональне розширення політики у сфері медіаграмотності стало відповіддю на гібридні загрози, спричинені російсько-українською війною.

Хоча Директива AVMSD та План дій з європейської демократії визначають загальні рамки та стандарти, практична імплементація цих положень у ЄС здійснюється через національні механізми, що залишає державам-членам простір для створення та реалізації власних моделей. Така логіка спрямовує на створення багаторівневої системи, в якій наднаціональні норми задають орієнтири, але конкретні інструменти формування медіаграмотності формуються у відповідності до внутрішніх політичних та соціальних контекстів. Як наслідок, у межах ЄС виникають різні національні підходи до розвитку медіаграмотності, ефективність яких значною мірою визначається історичними умовами та безпосередньою близькістю до російської загрози. У країнах Балтії, таких як Естонія та Литва, а також у Чехії чи Фінляндії, де існує досвід тривалого протистояння інформаційним операціям Росії, медіаосвітні програми набувають характеру системної оборонної практики. Водночас у державах із глибоко усталеними традиціями медіаосвіти, як-от Бельгія, Нідерланди чи Данія, акцент робиться на інтеграції критичного мислення у ширші освітні та культурні процеси. Така диференціація свідчить про функціональне розширення європейської політики, коли загальні стандарти задають напрям, але конкретні моделі імплементації стандартів медіаграмотності формуються у взаємодії між наднаціональними нормами та національними інституційними практиками, що забезпечує адаптивність системи до різних типів загроз.

Аналіз ландшафту протидії дезінформації в ЄС, здійснений EDMO та представлений у звітах за 2025 р., показує, що медіаграмотність залишається найбільш поширеним інструментом протидії дезінформації у національних стратегіях держав-членів ЄС (Додаток Н). Огляд ситуації у 27 країнах демонструє стійку тенденцію, коли більшість урядів віддають перевагу «м’яким» освітнім заходам перед жорстким законодавчим регулюванням контенту, проте у 2025–2026 рр. ці заходи дедалі частіше базуються на методиках пребанкінгу, тобто випереджального спростування маніпулятивних наративів [154]. Водночас

простежується чітка кореляція між найвищим рівнем медіаграмотності в державах-членах ЄС та формуванням розвинених екосистеми протидії FIMI, що підтверджує нерозривний зв'язок між освітнім виміром протидії дезінформації та інституційною верифікацією інформації. Найбільш показовим прикладом є Фінляндія, яка у 2025 р. знову посіла перше місце в Європі за Індексом медіаграмотності [308]. Для цієї країни медіаосвіта є ключовим безпековим компонентом концепції «тотальної оборони». Ще з часів Холодної війни, а особливо після 2022 р., Фінляндія інтегрувала навички критичного мислення та превентивної протидії дезінформації не в один окремий предмет, а в усі шкільні дисципліни. На уроках математики учні навчаються аналізувати маніпулятивну статистику та алгоритми ШІ, на уроках історії розпізнавати пропагандистські метанаративи, на уроках мистецтва виявляти складні візуальні фейки та діпфейки. Цей загальнонаціональний підхід координується Національним аудіовізуальним інститутом (KAVI) і охоплює всю освітню вертикаль від дитячих садків до підготовки державних службовців у сфері стратегічних комунікацій [317]. Така інституційна інтеграція створює одне з найбільш стійких до маніпуляцій суспільств у світі, демонструючи, що медіаграмотність у середньостроковій перспективі має стати системним елементом політики безпеки, який забезпечує когнітивну стійкість та довготривалу здатність протидіяти дезінформаційним загрозам.

В Німеччині формується інша, більш інституційно закріплена модель медіаграмотності як інструменту протидії дезінформації, що спирається на потужну державну інфраструктуру та враховує як внутрішні загрози екстремізму, так і зовнішні впливи, зокрема російські спроби маніпулювати великою російськомовною громадою. Центральну роль у цій архітектурі виконує Федеральне агентство громадянської освіти (Bundeszentrale für politische Bildung, BPB), що є унікальною державною, але політично нейтральною, інституцією, завдання якої полягає у зміцненні демократичної культури [117]. Саме BPB системно розробляє та безкоштовно поширює високоякісні освітні матеріали (книги, веб-ресурси, відео), які пояснюють механізми функціонування

дезінформації та формують когнітивну стійкість громадян. Якщо приклад Фінляндії демонструє інтеграцію медіаграмотності у шкільну систему, то Німеччина через ВРВ показує, як держава може фінансувати громадянську освіту, водночас залишаючи її політично нейтральною, що забезпечує довіру суспільства до цього інструменту. Паралельно на рівні федеральних земель діють власні медіа-агентства (Landesmedienanstalten), які реалізують практичні тренінги для різних цільових груп, від школярів до пенсіонерів [281]. Вони відповідають за освітні програми та нагляд за приватним телебаченням, радіо та онлайн-медіа, дотриманням вимог щодо захисту неповнолітніх і розвитку медіаграмотності у межах компетенцій федеральних земель.

Доповнюючи аналіз національних моделей, варто звернути увагу на досвід Швеції, ґрунтовно проаналізований професоркою Н. Карпчук. Дослідниця акцентує, що шведська модель інформаційної підтримки та медіаосвіти інтегрована в державну стратегію «психологічного захисту» населення. Цей підхід є особливо цінним для України, оскільки вказує на те, як держава може ефективно комунікувати з громадянами про загрози та формувати стійкість без запровадження цензури чи порушення демократичних свобод [24, с. 18]. Ми підтримуємо наукову позицію Н. Карпчук, що Швеція розглядає поінформованість громадян про європейські справи не просто як демократичну норму, а як елемент національної безпеки [24, с. 21-24]. Логіка шведського уряду така: чим краще громадянин розуміє механізми прийняття рішень у Брюсселі та Стокгольмі, тим важче ворожим акторам (зокрема РФ) маніпулювати його думкою через наративи про «втрату суверенітету» чи «диктат ЄС». Унікальною інституційною особливістю Швеції є створення у 2022 р. спеціалізованого Агентства психологічного захисту (Myndigheten för psykologiskt försvar) [56], яке перебрало на себе функції координатора в протидії дезінформації, покладаючись на методи просвіти та підтримки медіа. Відтак, можна стверджувати, що шведська стратегія базується на «принципі прозорості» (offentlighetsprincipen), який конкретизується в діях держави: Швеція протидіє дезінформації через надання швидкого та відкритого доступу до об’єктивної інформації, що повною

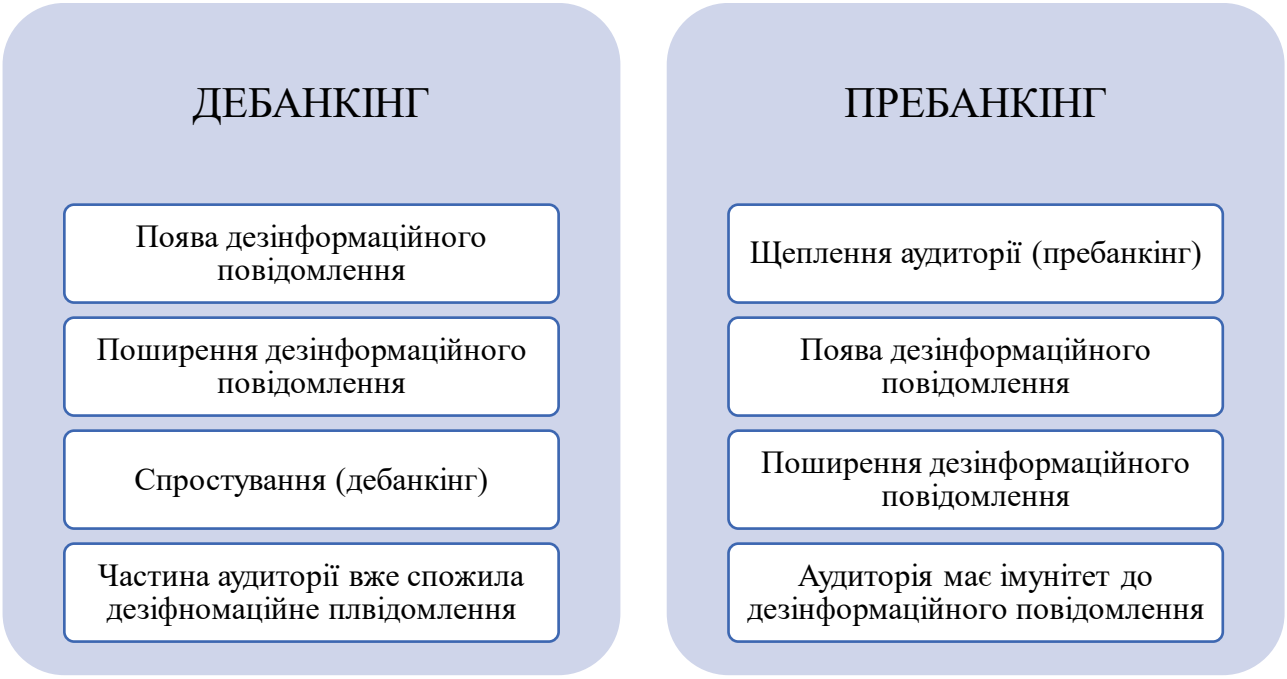
мірою відповідає європейським принципам публічної політики. Цей досвід є критично важливим для України, оскільки демонструє, як можна будувати потужну систему інформаційного спротиву, спираючись на довіру між державою та суспільством, а не на заборони.

Професорка Н. Піпченко суттєво поглибила аналіз шведського підходу, акцентуючи увагу на тому, що система медіаграмотності Швеції адаптується до протидії конкретним скоординованим загрозам не лише з боку Росії, а й Китаю та Ірану [339, p. 19]. Науковиця деталізує практичний інструментарій Агентства психологічного захисту, виокремлюючи освітню кампанію «Не дай себе обдурити» (Don’t Be Fooled) [374]. Ця ініціатива не просто закликає до критичного мислення, а надає громадянам чіткі алгоритми верифікації джерел перед поширенням контенту. Окрім того, Н. Піпченко звертає увагу на нормативне закріплення медіаосвіти через «Закон про бібліотеки» та «Закон про освіту», що дозволяє імплементувати навички критики джерел на всіх рівнях освіти від дошкільного виховання, де діти вчаться розрізняти вигадку і реальність, до співпраці держави з медіаінституціями, такими як Fojo Media Institute [229].

Проаналізовані національні моделі демонструють фундаментальний, довгостроковий підхід до побудови стійкості до дезінформації на індивідуальному та національному рівнях та на рівні громад. Найуспішніші моделі медіаграмотності в ЄС розглядають її не як факультатив, а як довгострокову стратегічну інвестицію в національну стійкість. Однак, окрім цих широких інституційних стратегій, сучасна інформаційна війна вимагає розробки і більш гнучких, технологічних інструментів, здатних діяти на випередження безпосередньо в цифровому середовищі, де дезінформація поширюється найшвидше.

Одним із найбільш інноваційних та технологічно орієнтованих інструментів медіаосвіти, що набув широкого поширення після 2022 р., виступає метод «пребанкінгу» (pre-bunking), або так звана «когнітивна інокуляція». Його сутність полягає у випереджальному формуванні стійкості до маніпулятивних

технік, коли аудиторія отримує своєрідну «вакцину» проти дезінформаційних стратегій ще до того, як вони будуть застосовані (Малюнок 4.2.1, складено автором).



Малюнок 4.2.1. Порівняння дебанкінгу та пребанкінгу як інструментів медіаосвіти

Дані Малюнку 4.2.1 вказують на те, що на відміну від дебанкінгу, який є реактивним процесом спростування вже існуючого фейку, пребанкінг працює превентивно, створюючи інституційно закріплений механізм когнітивного захисту. Пребанкінг стає частиною освітніх програм, комунікаційних кампаній та цифрових інструментів, що інтегруються у багаторівневу модель протидії дезінформації в ЄС засобами медіаграмотності. Академічною основою дебанкінгу є теорія психологічної інокуляції (psychological inoculation), яка, за аналогією з медичною вакциною, передбачає два ключові кроки. По-перше, це попередження про загрозу (threat): людину спершу інформують про те, що її сприйняття реальності може стати об’єктом маніпулятивної атаки. Це саме по собі активізує когнітивні захисні механізми. По-друге, це попереджувальне спростування: людині надають «ослаблену» дозу самої маніпуляції (наприклад, «Вами спробують маніпулювати, використовуючи емоційну мову та нападки на

інших»), одразу пояснюючи, чому цей аргумент є хибним або яка техніка за ним стоїть [355]. У результаті, коли людина згодом стикається з повноцінною дезінформаційною атакою, вона вже має сформовані «когнітивні антитіла» для її розпізнання та нейтралізації.

Такий підхід кардинально змістив фокус медіаосвіти в ЄС: замість нескінченної гонитви за спростуванням окремих фейків, він навчає розпізнавати універсальні маніпулятивні тактики (пошук «цапа-відбувайла», створення фальшивої дилеми, гра на страхах). Найбільш масштабним застосуванням цього інструменту в контексті гібридної війни стала кампанія, реалізована Google Jigsaw у 2022-2023 рр. у країнах Центральної та Східної Європи. Усвідомлюючи ризики російських інформаційних операцій, спрямованих на розкол єдності між місцевим населенням та українськими біженцями, Google запустив серію коротких пребанкінг-відео у Польщі, Чехії та Словаччині. Ці відео, що демонстрували рекламу на платформах YouTube та Facebook, у простій формі пояснювали глядачам, як розпізнати техніки емоційного маніпулювання, що використовуються для розпалювання ненависті до біженців [358]. Згодом, у партнерстві з інституами протидії дезінформації України та громадськими організаціями (VoxCheck), аналогічні кампанії пребанкінгу були запущені і в українському інформаційному просторі [62]. Пребанкінг є вдалим прикладом того, як академічні розробки з когнітивної психології, помножені на технологічні можливості великих платформ та політичну волю інституцій ЄС, перетворилися на ефективний інструмент превентивної інформаційної безпеки в реалізації політики протидії дезінформації.

Український досвід у сфері медіаграмотності є унікальним, оскільки він розвивався не стільки як планова освітня ініціатива, скільки як життєво необхідна навичка виживання в умовах перманентної інформаційної агресії з 2014 р. Повномасштабне вторгнення лише прискорило інституціоналізацію цих процесів, в яких держава взяла на себе чітку координаційну роль. Ключовим суб’єктом у сфері неформальної освіти виступило Міністерство культури та інформаційної політики, яке у 2021 р. запустило національний проєкт з

медіаграмотності «Фільтр». Цей проєкт діяв як хаб, що об'єднав зусилля держави, громадських організацій та міжнародних донорів, створюючи єдину комунікаційну рамку для поширення навичок критичного мислення серед дорослого населення України [31]. Паралельно Міністерство цифрової трансформації через свою платформу «Дія. Освіта» масово поширює освітні серіали, присвячені навичкам цифрової безпеки, аналізу інформації та протидії фейкам [36].

Водночас, за найбільш системний, формальний та довгостроковий трек відповідає Міністерство освіти і науки України (МОН). Стратегія МОН полягає в інтеграції медіаграмотності безпосередньо у державні освітні стандарти. Центральним механізмом для цього стала реформа «Нова українська школа» (НУШ). У концепції НУШ медіаграмотність та навички критичного мислення визначені як наскрізна ключова компетентність, що має розвиватися впродовж усього навчання [34]. Це означає, що навички не викладаються лише як окремий предмет, а інтегруються у гуманітарні дисципліни: на уроках історії учні навчаються аналізувати пропаганду в історичних джерелах, на уроках громадянської освіти вчаться розпізнавати політичні маніпуляції. Для реалізації цього підходу МОН зосередилось на масштабній підготовці вчителів. У партнерстві з ключовими міжнародними організаціями, як-от IREX (з його проєктом «Learn to Discern»), та за підтримки Посольства США, були проведені програми підвищення кваліфікації для десятків тисяч українських освітян [33]. Більше того, ці програми інтегровані у навчальні плани підготовки педагогічних працівників, що забезпечує підготовку вже нового покоління вчителів, які володіють необхідними компетенціями.

Звісно, ця державна вертикаль була б неможливою без підтримки потужного громадського сектору, який часто виступає виконавцем та новатором у цій сфері. Завдяки грантовій підтримці від програм ЄС (Creative Europe), урядів держав-членів ЄС та міжнародних фондів, в Україні сформована гнучкість в реалізації вузькоспеціалізованих проєктів. Зокрема, «Детектор медіа» (з ресурсом «MediaSapiens») та «Вокс Україна» (VoxCheck), проводять власні

тренінги та виступають основними розробниками методологічних матеріалів, які держава згодом залучає до формування політики протидії дезінформації. Водночас, вимірювання за Disinformation Resilience Index 2024 вказують на те, що попри потужні кампанії з медіаграмотності, Україна все ще стикається з викликами у сфері «суспільної вразливості» (Societal vulnerability). Це підкреслює необхідність переходу від загальних національних кампаній до точкової роботи з найбільш вразливими групами населення, що корелює з європейським підходом формування стійких моделей медіаграмотності та медіаосвіти.

Нестандартним кроком формування медіаграмотності в ЄС є використання ігрових технологій (gamification) для масового навчання користувачів алгоритмам розпізнавання дезінформації. Цей підхід базується на вже згадуваній теорії інокуляції, але реалізується через інтерактивні цифрові платформи, що дозволяє охопити мільйонні аудиторії. Референтним прикладом такого інструменту є онлайн-гра «Bad News», розроблена нідерландською кампанією DROG у співпраці з Кембриджським університетом. На відміну від традиційних освітніх курсів, цей цифровий симулятор ставить користувача на місце творця дезінформації. Гравець вчиться використовувати шість ключових тактик маніпуляції: дискредитацію опонентів, гру на емоціях, поляризацію, конспірологію, тролінг та використання ботів. Дослідження, проведене на вибірці з 15 тис. користувачів, показало, що після 15 хвилин гри здатність гравців розпізнавати маніпулятивні заголовки зростає в середньому на 21 % [376].

Успіх цього інструменту спонукав до створення спеціалізованих цифрових рішень для конкретних загроз. У відповідь на пандемію COVID-19 та російську дезінформацію про вакцини, за підтримки уряду Великої Британії та ВООЗ було запущено гру «Go Viral!». Цей інструмент фокусується на механізмах поширення медичних фейків у соціальних мережах, навчаючи користувачів ідентифікувати емоційно забарвлений контент та псевдоекспертність. За даними розробників, гра отримала понад 200 млн переглядів у різних мовних версіях, ставши глобальним інструментом цифрової гігієни [401].

Ще одним важливим кейсом є гра «Harmony Square» («Площа Гармонії»), розроблена за підтримки Держдепартаменту США та Google Jigsaw. Цей симулятор відтворює механіку політичної дестабілізації: гравець має завдання розколоти мирне суспільство, використовуючи дезінформаційні наративи, тролінг та штучну поляризацію. Цінність цього цифрового освітнього інструменту полягає в тому, що він наочно демонструє, як зовнішні актори (на кшталт російських спецслужб) використовують соціальні мережі для провокування реальних вуличних протестів та насильства. Інтеграція цих інструментів у стратегії цифрової безпеки держав-членів ЄС, зокрема Фінляндії, Естонії та Чехії, засвідчує формування нового підходу у формуванні медіаграмотності як інструменту протидії дезінформації – цифрових ігор. Вони дозволяють державі взаємодіяти з молоддю на зрозумілій їй мові технологій, формуючи стійкість до дезінформації в ігровому форматі. Для України, яка стикається з масованою пропагандою у TikTok та Telegram, адаптація та масштабування таких рішень (як це робить проєкт «NotaEnota») є критично важливою складовою цифрової оборони [248].

Підсумовуючи аналіз ролі медіаграмотності та медіаосвіти як компетентністних інформаційно-комунікаційних інструментів протидії дезінформації, можна стверджувати, що вони остаточно вийшли за рамки допоміжних освітніх ініціатив. Якщо технічна верифікація виконує роль «реактивного щита», то медіаграмотність є формою «когнітивного імунітету», що забезпечує довгострокову стійкість суспільства до іноземних інформаційних маніпуляцій та втручання (FIMI). Позитивними сторонами європейської моделі є її глибока інституціоналізація та перехід від логіки «гасіння пожеж» (дебанкінгу) до стратегії «інформаційної вакцинації» (пребанкінгу). Досвід Фінляндії, яка інтегрувала критичне мислення в межах концепції «тотальної оборони», доводить, що найефективнішим захистом є не цензура, а здатність громадянина ідентифікувати маніпулятивну поведінку на підсвідомому рівні. Німецька модель демонструє успішний приклад того, як держава може фінансувати громадянську освіту, зберігаючи її повну редакційну незалежність,

а шведський підхід через Агентство психологічного захисту підкреслює пріоритет радикальної прозорості над заборонами. Водночас, головною проблемою залишається «конфлікт швидкостей» між поширенням дезінформації та результатами впровадження медіаграмотності в державах-членах ЄС. Для України критичним залишається внутрішній розрив: попри успішні національні проєкти на кшталт «Фільтра» чи «Дія. Освіта», формальна шкільна освіта все ще перебуває в пастці підготовки «виконавців тестів», де медіаграмотність часто сприймається педагогами як додаткове паперове навантаження, а не як життєво необхідна навичка виживання. З огляду на сучасні виклики, пропозиції щодо вдосконалення медіаосвіти як інструменту протидії дезінформації мають розглядатися крізь призму внутрішніх потреб ЄС, держав-членів та держав-кандидатів. З огляду на це, основними пропозиціями щодо вдосконалення медіаосвіти як інструменту протидії дезінформації є такі.

Технологізація освітнього процесу передбачає перехід від ручного аналізу контенту до використання інструментів штучного інтелекту, які дозволяють учням та студентам у реальному часі виявляти мережеву координацію ботів та ідентифікувати діпфейки. Це підвищить ефективність навчання та формує когнітивну стійкість молодого покоління, перетворюючи освітні практики на елемент ефективного інструменту протидії дезінформації. Убезпечення через прозорість, як показує досвід Швеції, базується на відкритті державних архівів та забезпеченні швидкого доступу до першоджерел, що знімає ґрунт для конспірологічних наративів і водночас зміцнює довіру громадян до демократичних інститутів.

Мережева синергія передбачає максимальну інтеграцію громадських OSINT-спільнот у державні освітні стандарти, що дозволяє наповнити навчальні плани актуальними кейсами замість застарілих підручників. Це створює ефект взаємного підсилення, коли волонтерські ініціативи та державні ресурси працюють у єдиній системі, забезпечуючи адаптивність до нових викликів. Для України особливо корисним є досвід європейської інституціоналізації статусу верифікаторів та вчителів як агентів безпеки. Українська модель, сформована в

умовах повномасштабної війни після 2022 р., вже зараз є більш динамічною за європейську, проте їй бракує сталості фінансування та правових гарантій, які забезпечують AVMSD та DSA.

Для України медіаграмотність має стати не факультативним елементом освітньої системи, а фундаментом формування громадянської ідентичності, що поєднує освітні практики з державними безпековими структурами, такими як РНБО чи StratCom. Це дозволить інтегрувати гнучкість волонтерських ініціатив зі стратегічними ресурсами держави, посилюючи створену багаторівневу модель протидії дезінформації, в якій медіаосвіта набуде статусу інструменту протидії дезінформації, подібно до практик держав-членів ЄС.

4.3. Роль інститутів громадянського суспільства у реалізації європейської політики протидії дезінформації

Логічним продовженням аналізу технологічних та освітніх запобіжників дезінформації є перехід від дослідження самого інструментарію до питання суб’єктності тих, хто безпосередньо втілює ці стратегії в реальних умовах інформаційного протистояння. Якщо верифікація та медіаграмотність формують «технологічний щит» та «когнітивний імунітет» суспільства, то саме громадянське суспільство виступає суб’єктом, який перетворює теоретичні моделі безпеки на щоденну захисну практику в умовах гібридної війни [36, p. 124–147]. Нагадаємо, що початок збройного протистояння на території автономної республіки Крим, Луганської та Донецької областей України мав підготовчий етап у вигляді інформаційної підготовки [9, с. 215-218]. РФ формувала громадські організації для підтримки вторгнення та формування лояльності у місцевого населення до загарбників, поширюючи дезінформацію та дискредитаційні наративи про євроінтеграціїю пропагуючи ненависть до жителів областей Західного регіону України, створюючи проросійські політичні партії та громадські організації, підтримуючи воєнізовані молодіжні табори [8, с. 63-64]. Таким чином, точний рік саме гібридної війни є достеменно невідомим, адже

питання в тому, коли саме Росія почала вести цю війну прихованими методами або діяти методами «soft power» [252, p. 19].

Особливо виразною роль громадянського суспільства у протидії російській дезінформації стала після 24 лютого 2022 р. Провідна роль неурядового сектору є характерною не лише для України, а й для загальноєвропейського простору. Як зазначається у дослідженні EDMO, у багатьох державах-членах ЄС саме громадські організації та спільноти фактчекерів заповнюють прогалини у державній політиці, беручи на себе функції моніторингу загроз та підвищення обізнаності громадян. Це підтверджує, що в умовах гібридної війни громадянське суспільство перестає бути тільки споживачем безпеки [196]. Для підтвердження цієї тези та визначення ролі громадських організацій в реалізації європейської політики протидії дезінформації, звернемося до порівняння досвіду країни п’ятого розширення ЄС: Латвії, Литви, Естонії. Таке обмеження сукупності об’єктів порівняння дозволить побачити специфіку формування інституційних практик протидії дезінформації у регіоні, який має безпосереднє сусідство з Росією, кількісно значні російські етнічні меншини (крім Литви), спільний з Україною досвід перебування в Радянському Союзі, прагнення інтеграції у структури ЄС та НАТО, в яких країни вже є повноправними учасниками [378]. Важливим чинником є спільна військово-інформаційна загроза, яка визначає логіку політики протидії дезінформації.

Протидія дезінформаційним атакам від самого моменту відновлення незалежності була одним із ключових пріоритетів держав Балтії. Події лютого 2022 р., коли Росія здійснила повномасштабне вторгнення в Україну, стали каталізатором глибоких трансформацій у сфері політики дезінформації цих держав та зумовили суттєве коригування стратегій безпеки [256]. Литва вибудувала двовекторну систему протидії дезінформації: з одного боку, вона послідовно розвиває власні національні інституційні та технологічні спроможності, а з іншого – активно інтегрується у багатонаціональні механізми ЄС, що передбачають співпрацю та взаємну підтримку. Попри те, що Литва вже здобула репутацію одного з провідних міжнародних центрів у сфері

кіберзахисту, найбільш небезпечними чинниками для її інформаційної та цифрової безпеки залишаються дії російських і китайських спецслужб [256]. Усвідомлення необхідності комплексного підходу до оборони, включно з цифровим виміром, закріплене на інституційному рівні, а зростання рівня поінформованості серед органів влади, бізнесових структур та громадянського суспільства створює підґрунтя для позитивної оцінки литовської моделі інформаційної безпеки.

У межах реалізації політики проти російської дезінформації в Литві сформувався союз між громадянським суспільством та провідними медіа. Спільний проєкт, започаткований військовими у партнерстві з громадськими організаціями, спрямований на системний моніторинг та оперативне викриття дезінформаційних матеріалів ще до їхнього поширення. Ініціатори наголошують, що їхня діяльність охоплює близько 90 % населення Литви, яке регулярно споживає новинний контент [343]. Платформа Demaskuok.lt («розвінчування») використовує автоматизовані алгоритми для аналізу до 10 тис. публікацій у литовських та російських засобах масової комунікації, маркуючи їх за ключовими ознаками та виявляючи потенційні дезінформаційні вкиди [312]. Після первинної автоматичної обробки волонтери здійснюють додаткове відсіювання матеріалів і визначають рівень загрози. Відібрані повідомлення передаються журналістам, які спеціалізуються на тематиках, що активно експлуатуються російською пропагандою, забезпечуючи таким чином превентивне блокування поширення маніпулятивного контенту [123].

Латвія у 2021 р. посіла 25-ту позицію у світовому рейтингу Міжнародного індексу кібербезпеки (NCSI) [135]. Попри цей показник, загальні ризики для суспільства залишаються актуальними. У латвійській стратегії кіберзахисту на 2019–2022 рр. була чітко визначена необхідність приділяти особливу увагу медіаосвіті як ключовому елементу формування стійкості до інформаційних загроз [384]. Естонія, своєю чергою, змогла утвердитися як один із провідних промоутерів цифровізації та кіберзахисту, демонструючи приклад комплексного підходу до інформаційної безпеки. Саме Естонія за підтримки НАТО у 2008 р.

заснувала в Таллінні Cooperative Cyber Defense Center of Excellence, що стало важливим міжнародним майданчиком для розробки та координації стратегій кібероборони [319]. У 2014 р. Рига перетворилася на базу для іншої структури НАТО, яка спеціалізується на протидії російському впливу, – Центру передових стратегічних комунікацій (Strategic Communications Center of Excellence), що стало важливим кроком у зміцненні регіональної та міжнародної системи інформаційної безпеки [4, с. 67].

Таким чином, тільки Литва сформувала модель протидії дезінформації серед країн Балтії, в якій передбачена активна участь громадянського суспільства. На відміну від Латвії та Естонії, де превалює акцент на державних структурах та регуляторних інструментах, литовська модель вирізняється високим рівнем залучення волонтерів та медіа, що створює ефективний симбіоз між офіційними інституціями та суспільними ініціативами. Латвія більшою мірою орієнтується на правові механізми та обмеження доступу до дезінформаційних ресурсів, тоді як Естонія робить ставку на цифрові інновації та кіберзахист, інтегруючи їх у загальну систему національної безпеки. Литва ж демонструє комплексний підхід, в якому технологічні рішення (як-от Demaskuok.lt) поєднуються з широкою мобілізацією суспільства. Саме ця багатовимірність дозволяє Литві розвивати стійку культуру критичного мислення серед населення.

Важливою частиною діяльності інститутів громадянського суспільства в державах Балтії є «рух ельфів» [321], який виник з метою протидії російським інтернет-«тролям» [61] у країнах Балтії в 2016 р. Його учасниками є активісти, які прагнуть боротися з поширенням дезінформації у цифровому середовищі. «Ельфи» не мають формалізованої організаційної структури, більшість з них діє анонімно. До складу руху входять представники різних професій (учителі, лікарі, члени литовського парламенту). Балтійські «ельфи» стали показовим прикладом самоорганізації громадянського суспільства у відповідь на сучасні виклики та водночас слугують зразком для країн Західної Європи, демонструючи, як слід усвідомлювати масштаби російської загрози та мобілізувати всі можливі ресурси

для протидії. Первинна низова ініціатива групи з 10–20 осіб перетворилася на рух, що поширився на всі країни Балтії та охопив значну частину Європи. Такий рівень самоорганізації став можливим завдяки багаторічному розвитку в умовах цифровізації, інтеграції до євроатлантичних структур та специфічному історичному контексту Латвії, Литви та Естонії [257].

Вище ми згадували, що у 2018 р. подібна ініціатива почала активно розвиватися й у Чехії, що також є державою-членом ЄС [271]. Ще у 2015 р. два чеські аналітичні центри започаткували програми, спрямовані на дослідження та протидію російському інформаційному впливу [123]. Зокрема, програма Kremlin Watch Monitor, яка реалізується неурядовою організацією European Values Think-Tank, мала на меті виявлення та нейтралізацію інструментів російської дезінформації [123]. Паралельно Prague Security Studies Institute започаткував власну Ініціативу з протидії російському впливу. Починаючи з кінця 2015 р. три найбільші аналітичні центри Центральної Європи – GLOBSEC Policy Institute, Political Capital Institute та European Values Think-Tank – регулярно публікують щотижневий огляд Infowar Monitor.

Феномен «балтійських ельфів» після початку повномасштабного вторгнення Росії в Україну отримав своє глобальне продовження у вигляді руху NAFO (North Atlantic Fella Organization). Ця децентралізована інтернет-спільнота, що використовує інструменти гумору, сатири, мемів та координації у соціальних мережах, продемонструвала виняткову результативність у нейтралізації російської пропаганди, спрямованої на західну аудиторію. Діяльність NAFO підтвердила, що низові громадянські ініціативи здатні масштабуватися до глобального рівня, перетворюючись на вагомий чинник міжнародної інформаційної безпеки та формуючи нову модель суспільного спротиву дезінформаційним кампаніям.

Інститути громадянського суспільства успішно формують спільний досвід блокування телевізійних каналів, що поширюють російський контент і порушують національне законодавство. Під тиском громадських організацій Сейм Латвії ухвалив рішення про заборону мовлення російською мовою у

громадських засобах масової інформації, проте ця норма набула чинності лише з 2026 р. [55]. Такий підхід демонструє характерну для Балтійських країн комбіновану стратегію, в якій розвиток медіаграмотності та активна участь громадянського суспільства у протидії дезінформації поєднуються із законодавчими обмеженнями щодо діяльності російських ЗМІ та навіть із поступовим відходом від використання російської мови як інструменту впливу. У цьому контексті громадянське суспільство виступає ключовим чинником, адже саме воно формує запит на захист інформаційного простору, підтримує ініціативи з медіаосвіти та забезпечує суспільну легітимність рішень влади. Російська мова, яка традиційно використовувалася для комунікації з національною меншиною, дедалі більше розглядається як канал поширення м'якої сили РФ у державах Балтії, що створює ризики дезінтеграції суспільства. Саме тому поєднання громадянських ініціатив із державними заборонними заходами стає прикладом того, як суспільство і влада спільно реагують на виклики дезінформаційної політики, формуючи стійку модель протидії інформаційним загрозам.

Беручи до уваги інформацію про те, що медіа-регулятори Латвії, Литви, Польщі, Румунії та України у Варшаві підписали декларацію про співпрацю та взаємну підтримку у сфері боротьби з дезінформацією, можна говорити про формування довготривалого процесу інтеграції систем протидії та обміну практичним досвідом [60]. У документі закріплено положення про взаємну підтримку у здійсненні заходів, спрямованих на аналіз та стримування багатовекторної дезінформації, насамперед російської, на національному, регіональному та міжнародному рівнях. Країни-підписанти задекларували намір започаткувати програми спільного навчання громадян, які мають на меті формування навичок виявлення, реагування та запобігання поширенню дезінформаційних матеріалів, а також розбудову співпраці між європейськими та національними платформами фактчекінгу. Важливим елементом декларації є прагнення до створення єдиних механізмів регулювання медіа у державах-учасницях, що дозволить забезпечити узгодженість у підготовці та реалізації

спільних оцінок і позицій щодо протидії дезінформації. У цьому процесі громадянське суспільство маркується як основний партнер державних інституцій, адже саме воно забезпечує легітимність таких рішень, формує суспільний запит на захист інформаційного простору та активно долучається до практичної реалізації освітніх і фактчекінгових ініціатив.

Прикладом співпраці громадських організацій України та країн Балтії є естонсько-українська програма «Стійка Україна», яка спрямована на впровадження стандартів оцінки суспільної стійкості та постійне оновлення цієї системи. Дана інституція здійснює кількісні та якісні дослідження у сфері безпеки, визначає слабкі місця у стійкості суспільства та актуалізує їх як на місцевому, так і на національному рівні. Програма організовує публічні заходи та навчальні візити до Естонії, що сприяє поширенню знань і практик серед інститутів громадянського суспільства. «Стійка Україна» реалізується Міжнародним Центром Оборони та Безпеки (ICDS) з 2016 р. за підтримки Міністерства закордонних справ Естонії, що підкреслює важливість міжнародної співпраці у формуванні стійких суспільних моделей [48]. Ключова роль громадського сектору отримала кількісне підтвердження у міжнародних дослідженнях. Автори Disinformation Resilience Index наголошують, що високий рівень стійкості України забезпечується насамперед якістю громадянського суспільства, відповідно горизонтальні зв’язки та волонтерські ініціативи можуть компенсувати інституційні слабкості та обмежені ресурси держави в умовах війни [89].

В Україні в авангарді боротьби з російською дезінформацією та викриття фейкових інформаційних повідомлень стояла громадська організація «Телекритика», яка з 2016 р. змінила назву на ГО «Детектор медіа» [15]. Саме навколо цієї структури відбулася консолідація інших організацій, що створили основу громадського сектору протидії дезінформаційному впливу Росії. «Телекритика» представляла українські медіа у глобальному контексті та брала участь у процесах формування незалежних українських ЗМІ. Організація розробляла онлайн-курси для журналістів та широкої аудиторії, серед яких

«Журналістське розслідування: основи», «Новинна грамотність» та «Медіадрайвер». У 2016 та 2018 рр. «Детектор медіа» здійснив два масштабні дослідження якості журналістської освіти у вищих навчальних закладах та запропонував рекомендації для вдосконалення навчального процесу. Організація підтримує медіаосвітню ініціативу «MediaSapiens» [309], проєкт контролю за виборчим процесом «Вибори та ЗМІ», а також спеціалізовані програми з перевірки інформації та моніторингу маніпуляцій – «Медіачек» та «Детектор маніпуляцій» [13]. Представники ГО «Детектор медіа» беруть участь у роботі експертних груп та дорадчих органів, що займаються протидією дезінформації, опираючись на європейські принципи в цій сфері. Аналізуючи український досвід протидії дезінформації, аналітики організації підготували низку ґрунтовних звітів, серед яких «Інформаційне споживання, потреби та погляди мешканців сходу України» [21], «Як російська пропаганда впливає на суспільну думку в Україні» [73]. Ці матеріали насичені соціологічними даними, що дозволяють оцінити рівень впливу Росії на українські медіа та інші ключові аспекти інформаційної безпеки. З 2020 р. ГО «Детектор медіа» почала застосовувати штучний інтелект для боротьби з дезінформаційними кампаніями, що стало прикладом інноваційного використання технологій громадянським суспільством у сфері інформаційної безпеки.

Прикладом діяльності неурядової організації, яка покликана підтримувати медіа та зміцнювати інформаційну стійкість суспільства, є Український кризовий медіа-центр (УКМЦ). Цей центр започаткував новий напрям роботи – забезпечення цілодобової допомоги засобам масової комунікації, що висвітлюють події в Україні. Матеріали, які готуються організацією, дублюються французькою, німецькою та англійською мовами, що дозволяє громадянському суспільству через медіа доносити українську позицію до міжнародної аудиторії. УКМЦ проводив щоденні брифінги, здійснював моніторинг українських медіа, підтримував комунікацію з Міністерством оборони України та іншими державними інституціями, створював і поширював інфографіку щодо ситуації в зоні антитерористичної операції. Важливим

нововведенням стало впровадження принципу «One Voice» при коментуванні подій на Сході України, що забезпечувало узгодженість інформаційних повідомлень та підвищувало довіру суспільства до офіційних джерел [10].

В аналогічний часовий період виникла ініціатива студентів, викладачів та випускників Могилянської школи журналістики у співпраці з редакторами Digital Future of Journalism, яка отримала назву StopFake.org [372]. Цей проєкт був створений як інструмент захисту інформаційного простору від поширення фейкових повідомлень і діє на основі системного фактчекінгу. Вже у перші дні після запуску відвідуваність сайту досягала 50–70 тис. переглядів на добу, що засвідчило швидку та активну реакцію громадянського суспільства на виклики дезінформаційної політики [7]. Згодом StopFake розширив свою діяльність, почав проводити дослідження російської пропаганди як в Україні, так і на міжнародному рівні, а також організовувати відкриті тренінги з медіаграмотності та практики протидії дезінформації. Таким чином, проєкт став прикладом того, як громадянське суспільство здатне мобілізувати власні ресурси для створення ефективних механізмів захисту від інформаційних атак, поєднуючи освітню діяльність із практичним аналізом дезінформаційних наративів.

Як відповідь на виклики російсько-української війни та необхідність диверсифікації інформаційного простору виникла харківська незалежна медіа-платформа Ґвара Медіа, яка спеціалізується на конвергентній журналістиці [5]. Цей проєкт продовжив висвітлювати події після початку російського вторгнення у 2022 р., зосередившись на документуванні військових злочинів російських сил в Україні, зокрема у Харківській області. Вже 28 лютого 2022 р., у перші дні повномасштабної агресії, команда Ґвара Медіа створила фактчек-бот «ПЕРЕВІРКА», який став інструментом для верифікації новин та відсівання дезінформаційних матеріалів і фейків. Автори проєкту подбали про міжнародну проекцію результатів своєї діяльності, забезпечивши переклад контенту англійською мовою, зокрема, це стосувалося розслідувань, короткометражних документальних фільмів, репортажів та новин. Особливого значення набув чат-

бот «ПЕРЕВІРКА», адже він вирізняється простотою використання та ефективним алгоритмом із трьох кроків: відкриття чату у популярних месенджерах Viber або Telegram, надсилання новини (чи фото, відео, тексту або посилання) та отримання аргументованої відповіді від фактчекерів. Станом на березень 2026 р. чат-бот мав 54778 користувачів та здійснив 113818 перевірок запитів, викривши 16 994 фейків [6]. Його діяльність отримала офіційне визнання, свідченням чого є те, що посилання на бот було розміщене Міністерством цифрової трансформації України у дописі на Facebook, де перелічувалися сервіси для інформаційної боротьби з агресором-Росією. Ґвара Медіа дотримується принципів Кодексу International Fact-Checking Network (IFCN), що підтверджує її відповідність міжнародним стандартам фактчекінгу [243]. Цей приклад демонструє, як громадянське суспільство здатне швидко перепрофілюватися у кризових умовах війни та створювати дієві інструменти для боротьби з дезінформацією, поєднуючи локальну активність із глобальними стандартами інформаційної безпеки.

Важливим індикатором інкорпорації громадських організацій в українській моделі протидії дезінформації є високий рівень інституціоналізації взаємодії між громадянським сектором та безпековими структурами. Якщо у 2014 р. така співпраця мала переважно ситуативний характер, то після початку повномасштабного вторгнення вона перетворилася на системну та часто формалізовану практику. Провідні громадські організації не діють окремо від держави, а інтегруються як рівноправні партнери ключових державних інституцій. Так, Центр протидії дезінформації, який виконує функцію головного безпекового верифікатора, уклав офіційний Меморандум про співпрацю з незалежною аналітичною платформою VoxCheck [391]. Це партнерство спрямоване на прямий обмін аналітичними даними та методологіями виявлення інформаційних операцій, що здійснюються противником [69]. Водночас Центр стратегічних комунікацій та інформаційної безпеки (StratCom Ukraine), який займається розробкою державних наративів, працює у тісній синергії з громадянським сектором [62]. Показовим прикладом є запуск спільних проєктів,

серед яких ініціатива Google та Jigsaw з пребанкінгу дезінформації. У межах цієї ініціативи уповноважені Українською державою інститути працюють спільно із такими громадськими організаціями як «Детектор медіа», StopFake та Vox Ukraine [65]. Такий формат державно-громадського партнерства дозволяє координувати інформаційні кампанії у режимі реального часу, формуючи широке поле політики протидії дезінформації та залучаючи громадянське суспільство до формування сталих практик національної інформаційної безпеки.

Головною перевагою інститутів громадянського суспільства в протидії дезінформації є їх здатність компенсувати повільність державних інститутів через механізми самоорганізації. Досвід балтійських «ельфів» та чеських активістів продемонстрував, як низові ініціативи можуть стати зразком для всієї Європи. Рух NAFO став логічним продовженням цього феномену, довівши, що децентралізована інтернет-спільнота може ефективно нейтралізувати поширення дезінформаційних наративів на глобальному рівні.

Українська модель протидії дезінформації демонструє високий рівень інституціоналізації співпраці між органами влади та громадянським суспільством, коли такі організації, як StopFake, VoxCheck та «Детектор медіа», діють не відокремлено, а у синергії з РНБО та МКІП. Це свідчить про формування суспільно-центричної моделі, яка є більш гнучкою, порівняно з класичними європейськими моделями. Важливим напрямом розвитку є запозичення європейського правового статусу для верифікаторів та освітян як агентів безпеки, що дозволить незалежним організаціям подолати грантову залежність і отримати чіткі правові гарантії діяльності. Саме поєднання європейської інституційної сталісті з українською швидкістю реагування створює передумови для тривалого когнітивного суверенітету демократичного простору. Громадянське суспільство у цій моделі виконує багатофункціональну роль: по-перше, проводить освітні кампанії для формування навичок розпізнавання дезінформації; по-друге, здійснює фактчекінг та надає висновки щодо достовірності інформації; по-третє, розвиває медіаграмотність, навчаючи критичному мисленню та вмінню ідентифікувати ознаки маніпуляцій; по-

четверте, забезпечує захист журналістів, які викривають дезінформацію, надаючи їм юридичну та фінансову підтримку, а також допомагаючи протистояти політичному чи економічному тиску. Таким чином, український досвід доводить, що громадянське суспільство є одним з основних суб'єктів реалізації політики протидії дезінформації в умовах гібридної війни.

Висновки до розділу 4

Аналіз інформаційно-комунікаційних інструментів протидії дезінофрмації дозволяє стверджувати, що в умовах сучасної гібридної війни їх ефективність від рівня інституційного закріплення та перспектив функціонального розширення. Верифікація на сьогодні позиціонується в ЄС як важливий операційний вузол організації протидії дезінформації, оскільки вона є засобом управління ризиками, що забезпечує стійкість демократичних інституцій у багатомовному та багатокультурному середовищі ЄС. Європейська практика довела, що верифікація інформації є частиною багаторівневої системи, в якій технологічні інновації (InVID/WeVerify, Horizon 2020), професійні стандарти (IFCN, EUvsDisinfo) та низові ініціативи (Demagog.cz, VoxCheck, StopFake, Ґвара Медіа) взаємодіють, забезпечуючи ефективність європейського та національних механізмів протидії дезінформації. Такий підхід відображає потенціал ефекту взаємного підсилення в протидії дезінформації, коли інституційні рамки задають правила, а громадянське суспільство та технологічні платформи наповнюють їх конкретним змістом. Верифікація у такій моделі виконує функцію «фільтра» і «атрибутора» дезінформаційних наративів, дозволяючи виявляти неправдиві повідомлення, розуміти логіку їхнього поширення та визначати цільову спрямованість. Унікальність європейського підходу полягає у тому, що функції верифікації інформації переміщуються з площини технічної процедури до площини політичної відповідальності, що уможливлює посилення європейської моделі протидії дезінформації за критеріями інституційної стійкості та функціональної адаптивності, коли система здатна реагувати на нові виклики гібридної війни, враховуючи історичні контексти та регіональні вразливості.

Медіаграмотність та медіаосвіта в сучасних умовах гібридної війни є ключовим елемент формування стійкості спільнот до дезінформації. Якщо технічна верифікація виконує роль реактивного щита, то медіаграмотність формує когнітивний імунітет, що забезпечує довготривалу захищеність суспільства від іноземних інформаційних маніпуляцій. Європейські практики демонструють перехід від логіки дебанкінгу до стратегії пребанкінгу, яка опирається на необхідність превентивного навчання як «інформаційної вакцинації». Попри сформовану варіативність національних моделей медіаграмотності та медіаосвіти в державах-членах ЄС, головною проблемою залишається конфлікт швидкостей між поширенням дезінформації та впровадженням освітніх програм. Для України критичною є потреба подолати розрив між успішними національними проєктами («Фільтра» чи «Дія. Освіта») та формальною шкільною системою, в якій медіаграмотність часто сприймається як додаткове навантаження вчителя. Технологізація освітнього процесу через використання штучного інтелекту може стати дієвим інструментом для виявлення бот-мереж та діпфейків у реальному часі, а інтеграція громадських OSINT-спільнот у навчальні стандарти створюватиме ефект взаємного підсилення державними ресурсів у протидії дезінформації та волонтерськими ініціативами.

Дослідження ролі інститутів громадянського суспільства у протидії дезінформаційним викликам у Латвії, Литві та Естонії показує, що саме ці структури стають основними агентами у формуванні когнітивної стійкості суспільства. Їхня діяльність доводить важливість не лише державної координації, але й відсутності перешкоджання з боку держави, коли паралельні їй інституції виконують суспільно значиму функцію. У цьому контексті громадянське суспільство постає як автономний, але водночас інтегрований елемент загальної архітектури протидії дезінформації, що забезпечує адаптивність системи до нових викликів. Досвід Латвії, Литви та Естонії показує, що ефективність протидії дезінформації залежить від здатності держави інтегрувати громадські ініціативи у власну політику безпеки, створюючи

багаторівневу систему, в якій інституційні рамки ЄС наповнюються конкретними практиками. Для України цей досвід є особливо важливим, адже він наближає її до європейських принципів протидії дезінформації, які засвідчують, що стійкість до гібридних загроз формується, зокрема, і шляхом внормованої діяльності інститутів громадянського суспільства, які набувають статусу суб'єкта інструменту когнітивної оборони ЄС.

ВИСНОВКИ

У даному дисертаційному дослідженні було аналізовано сукупність та функціональні можливості механізмів тй інструментів реалізації політики протидії дезінформаційним впливам в ЄС в контексті гібридної війни. Вивчення еволюції європейського підходу до політики протидії дезінформації в контексті російської агресії проти України дозволяє зробити загальний висновок про те, що вироблення європейської політики протидії дезінформації можна характеризувати, як поступовий, подекуди надміру бюрократизований, але результативний процес. Предметний аналіз механізмів та інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни дозволяє зробити такі висновки.

Дослідження теоретико-методологічних засад вивчення політики протидії дезінформації в умовах гібридної війни дозволило визначити, що найбільш релевантним інструментарієм для аналізу протидії дезінформації є синергія неоінституціонального та неофункціонального підходів. Встановлено, що методологічний потенціал неоінституціоналізму полягає у здатності пояснити вплив політичних інститутів на формування когнітивних рамок та нормативних очікувань суспільства, що безпосередньо визначає рівень сприйняття інформаційних загроз. Застосування цього підходу дозволило диференціювати причини різного рівня стійкості держав до дезінформаційних атак, виходячи з аналізу взаємозв'язку між інституційною довірою, легітимністю політичних рішень та здатністю соціуму до мобілізації ресурсів. Визначено, що механізм протидії дезінформації в неоінституціональному вимірі постає як багаторівневий комплекс правил і структур, що інтегрує три ключові вектори: історичний (трансформація інститутів), раціонально-вибірковий та соціологічний (нормативні структури та суспільна довіра). Паралельно, неофункціоналізм дозволяє розглядати політику протидії дезінформації як процес функціонального розширення, в якому боротьба з маніпуляціями вимагає інтеграції безпекової, інформаційної та комунікаційної політик, зміцнюючи загальну інституційну

архітектуру ЄС. Важливим теоретичним компонентом дослідження визначено концепт стійкості, який у сучасному політологічному дискурсі виступає універсальною рамкою для балансування між захистом демократичних інститутів та збереженням фундаментальних свобод. Стійкість трактується не як статичний стан, а як динамічна здатність системи до адаптації та відновлення легітимності в умовах перманентних гібридних викликів.

Вивчення основних принципів політики протидії дезінформації в ЄС та державах-членах як основи формування європейського механізму реагування на інформаційні загрози в умовах гібридної війни довело, що ці принципи є основою для узгоджених дій інституцій ЄС, держав-членів та приватних суб'єктів у сфері інформаційної безпеки: перший принцип полягає у визнанні дезінформації як явища, що не завжди має ознаки незаконності, але здатне завдавати шкоди суспільству, демократичним процесам та інституціям, що потребує спеціальних політичних і регуляторних заходів; другий принцип стосується забезпечення прозорості, зокрема у сфері політичної реклами та діяльності цифрових платформ, що має запобігати прихованому поширенню неправдивих повідомлень та маніпуляцій; третій принцип передбачає обмеження монетизації дезінформації, тобто створення умов, за яких економічна вигода від поширення неправдивого контенту стає неможливою, що має зменшити стимули для його продукування; четвертий принцип полягає у розвитку співпраці між платформами, державними інституціями та незалежними фактчекінговими організаціями, що забезпечує багаторівневу перевірку достовірності інформації та підвищує її якість; п'ятий принцип спрямований на розширення можливостей громадян, зокрема через підвищення рівня медіаграмотності та розвиток критичного мислення, що дозволяє суспільству самостійно розпізнавати неправдивий контент; шостий принцип стосується створення механізмів підзвітності та регулярного звітування цифрових платформ про виконання взятих зобов'язань, що забезпечує контроль з боку Єврокомісії та громадськості; сьомий принцип полягає у посиленні координації між державами-членами ЄС та міжнародними партнерами, що має забезпечити узгодженість дій у глобальному

інформаційному просторі та підвищити ефективність протидії транснаціональним кампаніям дезінформації. Разом з тим, питання координації цих принципів з принципами політики протидії дезінформації, що реалізується в державах-членах ЄС, європейська політика не узгоджує достатньою мірою.

Здійснене дослідження безпекових інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни довело важливість перетворення стратегічних комунікацій на інституційно закріплену політику «стратегічного наративу». Ефективність цього інструментарію базується на синергії технологічного викриття дезінформації та активного просування демократичних цінностей, що створює ефект «ланцюгової реакції» у посиленні інституційної стійкості. Інституціоналізація таких інструментів, як StratCom Task Forces та RAS, надала системі необхідну гнучкість та здатність до функціональної адаптивності. Важливим аспектом є інтеграція технологій штучного інтелекту у поєднанні з технологіями цілісності даних, що формують «цифрове алібі» держави та забезпечують незмінність державних реєстрів перед зовнішніми втручаннями.

Принципове значення для дієвої сукупності безпекових інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни має формування національних онлайн екосистем у сфері протидії дезінформації, поряд із загальноєвропейською, оскільки саме вони забезпечують інституційне закріплення локальних практик та адаптацію загальних правил до специфіки мовного, культурного та політичного контексту кожної країни. Національні екосистеми виступають як автономні інституційні вузли, що інтегрують державні органи, громадянське суспільство, академічні спільноти та технологічні компанії у власний простір взаємодії, створюючи умови для оперативного реагування на загрози, які мають локальне походження або специфічні форми прояву. Їхня цінність полягає у тому, що вони здатні виявляти та нейтралізувати наративи, які залишаються непомітними для централізованого моніторингу. Водночас загальноєвропейська екосистема виконує функцію інтеграційного каркасу, який забезпечує єдині стандарти прозорості,

відповідальності та підзвітності для всіх учасників цифрового простору та створює умови для транскордонної координації. Національні екосистеми співвідносяться із загальноєвропейською як взаємодоповнюючі рівні: перші забезпечують глибину та деталізацію у локальному вимірі, другі гарантують узгодженість і примусовість виконання правил у наднаціональному просторі. Ця взаємодія створює ефект функціонального розширення, коли кожна нова сфера застосування технологій та інституційних практик на національному рівні інтегрується у загальноєвропейську систему, посилюючи її стійкість. Водночас інституційна логіка передбачає, що національні екосистеми не є ізольованими утвореннями, а функціонують як частини ширшої архітектури, де локальні знання та глобальні стандарти протидії дезінформації взаємно підсилюють одне одного. У результаті формується багаторівнева модель політики протидії дезінформації, в якій національні екосистеми забезпечують адаптацію та деталізацію, а загальноєвропейська екосистема гарантує узгодженість, легітимність і незворотність процесу.

Вивчення інформаційно-комунікаційних інструментів реалізації європейської політики протидії дезінформації в умовах гібридної війни дозволило констатувати трансформацію логіки захисту інформаційного простору ЄС. Верифікація на сьогодні позиціонується в ЄС як важливий інструмент організації протидії дезінформації, оскільки вона є засобом управління ризиками, що забезпечує стійкість демократичних інституцій у багатомовному та багатокультурному середовищі ЄС. Унікальність європейського підходу полягає у тому, що верифікація інформації трансформувалася з технічної процедури на політичну відповідальність, що уможливлює забезпечення переходу європейської моделі протидії дезінформації від інституційної стійкості до функціональної адаптивності, коли система здатна реагувати на нові виклики гібридної війни, враховуючи історичні контексти та регіональні вразливості. Медіаграмотність та медіаосвіта в сучасних умовах гібридної війни є ключовим елемент формування стійкості спільнот до дезінформації. Європейські практики демонструють перехід від логіки

дебанкінгу до стратегії пребанкінгу, яка опирається на необхідність превентивного навчання як «інформаційної вакцинації». Попри сформовану варіативність національних моделей медіаграмотності та медіаосвіти в державах-членах ЄС, головною проблемою залишається конфлікт швидкостей між поширенням дезінформації та впровадженням освітніх програм. Дослідження ролі інститутів громадянського суспільства у протидії дезінформаційним викликам у Латвії, Литві та Естонії показує, що саме ці структури стають основними агентами у формуванні когнітивної стійкості суспільства. Їхня діяльність доводить важливість не лише державної координації, але й відсутності перешкоджання з боку держави, коли паралельні їй інституції виконують суспільно значиму функцію. У цьому контексті громадянське суспільство постає як автономний, але водночас невід'ємний елемент європейської моделі протидії дезінформації, що забезпечує адаптивність системи до нових викликів.

При визначенні ролі та місця України у зміцненні європейської стійкості доведено, що український практичний досвід безпосередньої протидії гібридній агресії є стратегічним активом для ЄС, оскільки збагачує його інструментарій верифікованими даними про новітні тактики маніпуляцій. Україна де факто є елементом загальноєвропейського безпекового периметра. Попри успішну нормативну конвергенцію із правовим полем ЄС, виявлено певний дефіцит інституційної зрілості. Для остаточного завершення інтеграції та зміцнення стійкості Україні необхідно: відмовитися від практики позасудового блокування ресурсів на користь правової визначеності; забезпечити реальну фінансову та політичну незалежність регулятора медіа та Суспільного мовника; імплементувати анти-SLAPP директиви для захисту розслідувальної журналістики; змістити акцент із каральних методів на розвиток когнітивної резистентності та цифрового суверенітету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Т. Механізми Anti-SLAPP: як захистити свободу слова від юридичного тиску. *Лабораторія цифрової безпеки*. 2024. URL: https://dslua.org/publications/anti-slapp-mechanisms/.

2. Бурдяк В. Політико-психологічний компонент медіаграмотності vs маніпулювання ЗМІ суспільною свідомістю. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2022. Вип. 10. С. 43-63.

3. Бурдяк В., Федорчак Т. Взаємодія політичних інститутів України та Вишеградської четвірки в роки повномасштабної війни. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2025. Вип. 17. С. 227-246.

4. Гарькавий Є. М. Організація стратегічних комунікацій відповідно до стандартів НАТО. *Вісник Донецького національного університету імені Василя Стуса.* Серія політичні науки. 2023. № 8. С. 60–66.

5. Ґвара Медіа: офіційний сайт. URL: https://gwaramedia.com/.

6. Ґвара Медіа. Перевірка: разом зможемо. 2025. URL: https://gwaramedia.com/perevirka-razom-smozhemo/.

7. Гладка К. Stop fake: як припинити вигадки про Україну? Тиждень.ua. 2014. 11 трав. URL: https://tyzhden.ua/Columns/50/109290.

8. Горбулін В. П. П’ятий вимір гібридної війни. *Вісник Національної академії наук України.* 2015. № 8. С. 60–65.

9. Горбулін В. П. Світова гібридна війна: український фронт: монографія / В. П. Горбулін. Київ: НІСД, 2017. 496 с.

10. Горбулін В. П., Власюк О. С. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2015 році». Київ: НІСД, 2015. URL: https://niss.gov.ua/sites/default/files/2015-12/POSLANNYA-2015_giper_new-4af35.pdf

11. Гороховський О. Фактчек як тренд розслідувань: можливості та перспективи. Київ: Представництво «Фонду Фрідріха Науманна за Свободу» в Україні, 2021. 94 с. URL:https://www.amo.cz/wp-

content/uploads/2017/06/AMO_Factchecking-jako-trend-v-investigativni-zurnalistice-moznosti-a-perspektivy.pdf.

12. Детектор медіа. Президентка Молдови підписала закон про заборону російського інформаційного мовлення. 2022. URL: https://detector.media/infospace/article/200282/2022-06-19-prezydentka-moldovy-pidpysala-zakon-pro-zaboronu-rosiyskogo-informatsiynogo-movlennya/

13. Детектор медіа: хто ми. URL: https://go.detector.media/about/#what.

14. Детектор медіа. Євросоюз заборонив мовлення RT та Sputnik. 2022. URL: https://detector.media/infospace/article/197112/2022-03-02-ievrosoyuz-zaboronyv-movlennya-rt-ta-sputnik/

15. Детектор медіа. Історія ГО. 2023. URL: https://go.detector.media/istoriya-go/.

16. Європейська правда. Макрон назвав Russia Today та Sputnik органами пропаганди. 2017. URL: https://www.eurointegration.com.ua/news/2017/05/29/7066400/

17. Європейська правда. Боррель: санкції проти Росії працюють, хоча самі по собі не зупинять війну. 2023. URL: https://www.eurointegration.com.ua/news/2022/12/27/7153183/.

18. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи. *Історико-політичні проблеми сучасного світу*. 2021. Вип. 43. С. 30–39.

19. Звоздецька О. Інституційні механізми протидії дезінформації в ЄС: проблеми та здобутки. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2022. Вип. 10. С. 107–122.

20. Звоздецька О. Протидія дезінформації в Європейському Союзі: правовий аспект. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2021. Вип. 9. С. 245–262.

21. Інформаційне споживання, потреби та погляди мешканців сходу України: дослідження. MediaSapiens. 14 листопада 2017. URL: https://ms.detector.media/mediadoslidzhennya/post/19925/2017-11-14-

informatsiyne-spozhyvannya-potreby-ta-poglyady-meshkantsiv-skhodu-ukrainy-doslidzhennya/.

22. Кабінет Міністрів України. Про внесення змін до деяких постанов Кабінету Міністрів України щодо питань електронної системи охорони здоров'я: Постанова від 15 квітня 2020 р. № 348. URL: https://zakon.rada.gov.ua/laws/show/348-2020-%D0%BF#Text.

23. Кабінет Міністрів України. Трембіта здійснила понад 1,6 млрд транзакцій між держреєстрами: новина. 2023. URL: https://www.kmu.gov.ua/news/trembita-zdijsnila-ponad-16-mlrd-tranzakcij-mizh-derzhreyestrami.

24. Карпчук Н. П. Інформаційна підтримка європейської інтеграції: досвід Швеції. *Міжнародні відносини: теоретико-практичні аспекти*. 2023. Вип. 11. С. 17–30.

25. Карпчук Н. П. Публічна сфера Європейського Союзу як основа його ефективної комунікаційної політики. *Науковий вісник СНУ ім. Лесі Українки*. 2013. № 9. С. 73–77.

26. Карпчук Н. П. Стратегічна комунікація ЄС як засіб у боротьбі з дезінформацією. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2019. № 1 (5). С. 33–42.

27. Лабораторія цифрової безпеки. Координатор цифрових послуг: чому він важливий та яким має бути? 2023. URL: https://dslua.org/wp-content/uploads/2023/09/Koordynator-tsyfrovykh-posluh.pdf

28. Макух-Федоркова І. Вплив цифрової дезінформації на перебіг російсько-української війни. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2025. Вип. 16. С. 129–138.

29. Макух-Федоркова І. Масова комунікація в соціальних мережах крізь призму класичних теорій. *Історико-політичні проблеми сучасного світу.* 2025. Вип. 52. С. 99–110.

30. Макух-Федоркова І., Федорчук О. Формування концепцій масової комунікації у 40-60-х рр. XX ст. на основі досліджень громадської думки. *Історико-політичні проблеми сучасного світу*. 2023. Вип. 47. С. 228–238.

31. Міністерство культури та інформаційної політики України. Національний проєкт з медіаграмотності «Фільтр». URL: https://filter.mkip.gov.ua/

32. Міністерство культури та стратегічних комунікацій України. Дорожня карта відновлення медіапростору та забезпечення плюралізму в післявоєнний період. Київ, 2024. https://zakon.rada.gov.ua/rada/show/v0451921-24#Text

33. Міністерство освіти і науки України. Впровадження медіаграмотності в освітній процес: МОН та IREX підписали меморандум. 2023. 18 травня. URL: https://mon.gov.ua/news/vprovadzhennya-mediagramotnosti-v-osvitnii-protses-mon-ta-irex-pidpisali-memorandum.

34. Міністерство освіти і науки України. Нова українська школа: концептуальні засади реформування середньої школи. 2016. URL: https://mon.gov.ua/storage/files/new-school-book-FINAL-5-5-2016.pdf.

35. Міністерство цифрової трансформації України. Дія – Державний веб-портал електронних послуг: офіційний сайт. URL: https://diia.gov.ua/

36. Міністерство цифрової трансформації України. Дія.Освіта. URL: https://osvita.diia.gov.ua/.

37. Міністерство цифрової трансформації України. єВорог: офіційний сайт. 2022. URL: https://evorog.gov.ua/.

38. Міністерство цифрової трансформації України. Про Міністерство. URL: https://thedigital.gov.ua/ministry.

39. Міністерство цифрової трансформації України. Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта». URL: https://trembita.gov.ua/.

40. Міністерство цифрової трансформації України. Трембіта: статистика системи. 2025. URL: https://trembita.gov.ua/ua/statistics

41. Нестеряк Ю. В. Міжнародні критері інформаціно безпеки держави: теоретико-методологічни аналіз. *Вісник НАДУ*. 2013. № 3. С. 40−45.

42. Нечаєва-Юрійчук Н. Грузія як тестовий майданчик для путінської політики «повернення земель»: від окупації територій до антиєвропейського курсу «Грузинської мрії». *Медіафорум: аналітика, прогнози, інформаційний менеджмент.* 2024. Т. 15. С. 123–145.

43. Офіс Президента України. Спільні безпекові зобов'язання між Україною та Європейським Союзом. Брюссель, 27 червня 2024 року. URL: https://www.president.gov.ua/news/ukrayina-ta-yes-pidpisali-spilni-bezpekovi-zobovyazannya-91813

44. Пацек Б., Пєвцов Г. В. Військова доктрина Російської Федерації: історична еволюція та застосування в контексті війни в Україні. *Військова стратегія і технології.* 2025. № 2 (2). С. 114–128.URL: https://journals.uran.ua/milstratech/article/view/342404

45. Повітряна Тривога. URL: https://www.ukrainealarm.com/.

46. Про верифікацію та моніторинг державних виплат: Закон України від 17.10.2019 № 324-IX. URL: https://zakon.rada.gov.ua/laws/show/324-20.

47. Про медіа: Закон України від 13 груд. 2022 р. № 2849-IX. Відомості Верховної Ради України. 2023. № 47-49. Ст. 119. URL: https://zakon.rada.gov.ua/laws/show/2849-20.

48. Програма «Стійка Україна»: офіційний сайт. URL: https://resilient-ukraine.org/about/us

49. Рада національної безпеки і оборони України. Рішення про створення Центру протидії дезінформації: Указ Президента України від 19 березня 2021 р. № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21#Text

50. Розкладай І. Правове регулювання дезінформації: від «Про медіа» до DSA. Центр демократії та верховенства права (CEDEM). 2024. URL: https://cedem.org.ua/analytics/desinformatsiya-dsa/

51. Ротар Н. Особливості концептуалізації ідеї цифрового суверенітету в сучасній політичній науці. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2023. Вип. 3(17). С. 229–244.

52. Ротар Н. Теоретико-методологічні підходи в політичних дослідженнях. *Політична наука в Україні. 1991-2016: у 2 Т.* Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ: Парламентське видавництво, 2016. Т. 1. Політична наука: західні тренди розвитку й українська специфіка. С. 92–140.

53. Ротар Н. Формування політики захисту електоральної моделі політичної участі від дезінформаційних впливів (на прикладі політики Європейського Союзу). *Історико-політичні проблеми сучасного світу*. 2021. Том. 43. С. 179–193.

54. Ротар Н. Ю. Політичні ідентичності в сучасній Україні: міська громада Чернівців. К.: ІПіЕНД ім. І.Ф. Кураса НАН України, 2016. 344 с.

55. Сейм Латвії підтримав заборону мовлення російською мовою громадським ЗМІ. Інформаційне агентство «Українські Національні Новини». 28 вересня 2023. URL: https://www.unn.com.ua/uk/news/2048478-seym-latviyi-pidtrimav-zaboronu-movlennya-rosiyskoyu-movoyu-gromadskim-zmi.

56. Стельмах Д. А. Протидія російським дезінформаційним кампаніям: досвід ЄС. *Інформація і право.* 2025. № 2(53). С. 155–163.

57. Стьопкін А. Інституціоналізація політики протидії дезінформації в Європейському Союзі. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2022. Том 10. С. 196–208.

58. Стьопкін А. Особливості концептуалізації поняття дезінформація в сучасній політичній науці. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2024. Том 15. С. 320–336.

59. Стьопкін А. Особливості національних моделей політики протидії дезінформації в державах-членах ЄС. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2025. Вип. 4(24). С. 115–137.

60. Україна домовилася з чотирма країнами ЄС разом боротися з дезінформацією. *Європейська правда.* 2023. 5 жовтня. URL: https://www.eurointegration.com.ua/news/2023/10/5/7170826/.

61. УНІАН. Трамп звернувся з попередженням до України перед переговорами в Женеві. 2026. URL: https://www.unian.ua/world/mirni-peregovori-tramp-zrobiv-poperedzhennya-ukrajini-13288422.html

62. УНІАН. Трамп розкрив деталі свого «мирного плану» для України: Зеленському доведеться його схвалити. 24 листопада 2025. URL: https://www.unian.ua/politics/mirniy-plan-ssha-tramp-zayaviv-shcho-zelenskomu-dovedetsya-yogo-shvaliti-13204005.html

63. Центр протидії дезінформації при РНБО України. Google та Jigsaw у партнерстві з ЦПД запускають ініціативу з медіаграмотності в Україні. URL: https://cpd.gov.ua/announcement/google-ta-jigsaw-u-partnerstvi-z-czpd-zapuskayut-inicziatyvu-z-mediagramotnosti-v-ukrayini/.

64. Центр протидії дезінформації. Аналіз мережі проросійських Telegram-каналів в українському інформаційному сегменті: звіт. РНБО України. Київ, 2024. URL: https://cpd.gov.ua/reports/analiz-merezhi-prorosijskyh-telegram-kanaliv/.

65. Центр протидії дезінформації. Меморандум про співпрацю між ЦПД та VoxCheck. URL: https://cpd.gov.ua/.

66. Центр протидії дезінформації. Новий фейк про продаж Україною західної зброї на чорному ринку. 2023. URL: https://cpd.gov.ua/international-direction/yevropa/novyj-fejk-pro-prodazh-ukrayinoyu-zahidnoyi-zbroyi-na-chornomu-rynku/.

67. Центр протидії дезінформації. Операція «Матрьошка»: як росія використовує західні медіа для поширення фейків. 2024. URL: https://cpd.gov.ua/main/operacziya-matryoshka-yak-rosiya-vykorystovuye-zaxidni-media-dlya-poshyrennya-fejkiv/.

68. Центр протидії дезінформації. Україна та ЄС посилюють співпрацю в боротьбі з дезінформацією. 2024. URL: https://cpd.gov.ua/main/ukrayina-ta-yes-posylyuyut-spivpraczyu-v-borotbi-z-dezinformacziyeyu/.

69. ЦПД і «Вокс Україна» підписали Меморандум про співпрацю. Центр протидії дезінформації. 16 жовтня 2024. URL: https://cpd.gov.ua/events/czpd-i-voks-ukrayina-pidpysaly-memorandum-pro-spivpraczyu/.

70. Шуляк А. М., Шуляк Н. О. Стратегічні комунікації та інформаційна гігієна: національна безпека в умовах глобальних викликів: монографія / Волинський національний університет імені Лесі Українки. Луцьк: Вежа-Друк, 2025. 250 с.

71. Шуляк А. Публічна дипломатія та зв'язки з громадськістю як компоненти стратегічних комунікацій ЄС. *Стратегічні комунікації ЄС: протидія деструктивним впливам: кол. моногр.* / Н. П. Карпчук, Б. М. Юськів, А. М. Шуляк, С. В. Федонюк, Н. О. Шуляк; за заг. ред. Н. Карпчук. Луцьк: Вежа-Друк, 2023. С. 128–144.

72. Шуляк Н. О., Шуляк А. М. Інформаційна гігієна в еру цифрових загроз: від пропаганди до гібридних атак. *Вісник Маріупольського державного університету. Серія: Історія. Політологія.* 2024. Вип. 40. С. 185–195. DOI: 10.34079/2226-2830-2024-15-40-185-195.

73. Як російська пропаганда впливає на суспільну думку в Україні: дослідження. MediaSapiens. 13 лютого 2017. URL: https://ms.detector.media/mediadoslidzhennya/post/18384/2017-02-13-yak-rosiyska-propaganda-vplyvaie-na-suspilnu-dumku-v-ukraini-doslidzhennya/.

74. AFP FACTUEL: À propos. URL: https://factuel.afp.com/a-propos.

75. AFP Factuel. 2025. URL: https://factuel.afp.com/

76. AI4TRUST pilot platform. 2023. URL: https://pilot.platform.ai4trust.eu/.

77. AI4TRUST: AI-based-toolbox for trusted information. European Commission, CORDIS. 2024. URL: https://cordis.europa.eu/project/id/101070190

78. Alemanno A. How to Counter Fake News? A Taxonomy of Anti-fake News Approaches. *European Journal of Risk Regulation.* 2018 Vol. 9(1). P. 1–5.

79. Almond G. The return to the state. *American Political Science Rewiew*. 1988. Vol. 82. P. 853–874.

80. Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It. By Ben Nimmo. URL: https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/

81. Andersen J., Søe, S. O. Communicative actions we live by: The problem with fact-checking, tagging or flagging fake news – the case of Facebook. *European Journal of Communication*. 2020. Vol. 35(2). P. 126–139.

82. Anderson C. W. Propaganda, misinformation, and histories of media techniques. *Harvard Kennedy School Misinformation Review*. 2021. Vol. 2. C. 1–7.

83. Andriole S. J. Verification and Validation of Information and Decision Systems. Amsterdam: Elsevier, 2024. 240 p.

84. ARCOM: Autorité de régulation de la communication audiovisuelle et numérique: site officiel. URL: https://www.arcom.fr/.

85. ARCOM: Autorité de régulation de la communication audiovisuelle et numérique. Missions. URL: https://www.arcom.fr/nos-missions.

86. Atlantic Council's DFRLab. Narrative and Network: Russian Information Operations in Ukraine: special report. 2023. URL: https://www.atlanticcouncil.org/reports/narrative-and-network/.

87. Atlantic Council's DFRLab. The Elves: Lithuania's Digital Resistance and the Fight Against Disinformation. 2021. URL: https://www.atlanticcouncil.org/blogs/turkeysource/lithuanias-digital-elves-fight-russian-disinformation/.

88. Autorité de régulation de la communication audiovisuelle et numérique. 2025. URL: https://www.arcom.fr/

89. Avramenko A., Shelep A. Disinformation Resilience Index 2024. EAST Center. 2024. URL: https://east-center.org/wp-content/uploads/2024/12/DRI_2024_edition.pdf.

90. Baade B. Fake News and International Law. *European Journal of International Law.* 2018. Vol. 29(4). P. 1357–1376.

91. Bakir V. Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting. *Frontiers in Communication.* 2020. Vol. 5. Art. 67.

92. Baldwin J. A., Alvarado A., Jarratt-Snider K., Hunter A., Keene C., Castagno A. E., Ali-Joseph A., Roddy J., Begay M. A. Jr., Joseph D. H., Goldtooth C., Camplain C., Smith M., McCue K., Begay A. B., Teufel-Shone N. I. Understanding Resilience and Mental Well-Being in Southwest Indigenous Nations and the Impact of COVID-19: Protocol for a Multimethods Study. *JMIR Research Protocols.* 2023. Vol. 12.

93. Barnes P., Thomas C. H. Sustainable development and governance in Europe. London, New York: Routledge, 2013. 264 p.

94. Bayer J., Bitiukova N., Bard P., Szakács J., Alemanno A., Usai E. Disinformation and propaganda – impact on the functioning of the rule of law in the European Union and its Member States: study. Brussels: European Parliament, 2021. 170 p. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.

95. Bayer J., Bitiukova N., Bard P., Szakács J., Alemanno A., Uszkiewicz E. Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States. *SSRN Electronic Journal*. 2019.

96. Ben-Dor G., Pedahzur A., Canetti D., Zaidise E. The role of public opinion in Israel's national security. *American Jewish Congress: Congress Monthly.* 2002. Vol. 5 (69). P. 13–15.

97. BENEDMO: About the project. URL: https://benedmo.eu/english/.

98. Benkler Y., Faris R., Roberts H. Network propaganda: Manipulation, disinformation, and radicalization in American politics. Oxford University Press, 2018. URL: https://www.researchgate.net/publication/369944867_Network_Propaganda_Manipulation_Disinformation_and_Radicalization_in_American_Politics

99. Bentzen N. Countering disinformation: An analytical framework for European Union action. Brussels: European Parliamentary Research Service (EPRS), 2024. 32 p.

100. Bentzen N. EU strategic communications with its neighbourhood: briefing. European Parliamentary Research Service. 2016. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/583823/EPRS_BRI(2016)583823_EN.pdf.

101. Bentzen N. Russia's influence in the Western Balkans: briefing. European Parliamentary Research Service. 2017. URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/603960/EPRS_ATA(2017)603960_EN.pdf

102. Berry J. M., Sobieraj S. The outrage industry: Political opinion media and the new incivility. Oxford University Press, 2013. URL: https://archive.org/details/outrageindustryp0000berr

103. Betzel M., Nyakas L., Papp T., Kelemen L., Monori Z., Varga Á., Marrazzo F., Matějka S., Ó Fathaigh R., Helberger N. Notions of Disinformation and Related Concepts (ERGA Report) [Report]. European Regulators Group for Audiovisual Media Services. 2020. URL:

104. Bezpečnostní Informační Služba. Kontrašpionáž. 2025. URL: https://www.bis.cz/kontraspionaz/

105. Bezpečnostní informační služba. Tisíce euro za ruskou propagandu. BIS odhalila vlivového agenta. 2023. URL: https://www.bis.cz/aktuality/tisice-euro-za-ruskou-propagandu-bis-odhalila-vlivoveho-agenta-2675c9f4.html?page=2

106. Bezpečnostní informační služba. Výroční zpráva 2023. Annual Report 2023. URL: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2023-vz-cj.pdf

107. BfJ. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG). Bundesgesetzblatt I, 2017. S. 3352. URL: https://www.gesetze-im-internet.de/netzdg/

108. Blockchain – e-Estonia: official website. 2024. URL: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/.

109. Bonini E. Farmers' protests exploited to spread fake news about EU climate policy, study nails European far-right. Eunews. 2024. URL: https://www.eunews.it/en/2024/06/03/farmers-protests-exploited-to-spread-fake-news-about-eu-climate-policy-study-nails-european-far-right/

110. Bontcheva K., Nakov P. Artificial Intelligence for Fact-Checking: Theory and Practice. Synthesis Lectures on Human Language Technologies. Cham: Springer Nature, 2023. 165 p.

111. Borba L. Debunking the myth: sanctions against Russia aren't working. Medium. 2022. URL: https://leviborba.medium.com/debunking-the-myth-sanctions-against-russia-arent-working-49442a814

112. Born K., Edgington N. Analysis of philanthropic opportunities to mitigate the disinformation/propaganda problem. William and Flora Hewlett Foundation, URL: https://www.hewlett.org/wp-content/uploads/2017/11/Hewlett-Disinformation-Propaganda-Report.pdf

113. Bouza García L., Oleart A. From self to co-regulation in the EU's approach to disinformation: The framing power of Big Tech business lobbies in the lead to the Digital Services Act. *International Review of Public Policy*. 2024. Vol. 6 (1). P. 149–168.

114. Bradshaw S., Bailey H., Howard P. N. Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Oxford: Oxford Internet Institute, 2021. 30 p. URL: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf

115. Brennen J. S. Formulating deformation: The flows of formless information. *International Journal of Communication.* 2020. Vol. 14. C. 4578–4598.

116. Brennen J. S., Simon F. M., Howard P. N., Nielsen R. K. Types, sources, and claims of COVID-19 misinformation. *Reuters Institute for the Study of Journalism*. 2020. URL: https://www.oxfordmartin.ox.ac.uk/publications/types-sources-and-claims-of-covid-19-misinformation/

117. Bundeszentrale für politische Bildung (bpb). URL: https://www.bpb.de/.

118. Burdiak V. Legal Framework for Youth Policy in the European Union. *Історико-політичні проблеми сучасного світу.* 2025. Вип. 52. С. 91–98.

119. Burkhardt J. M. Combating fake news in the digital age. *Library Technology Reports*. 2017. Vol. 53(8). URL: https://journals.ala.org/index.php/ltr/issue/view/662

120. Canetti D., Waismel-Manor I., Cohen N., Rapaport C. What does national resilience mean in a democracy? Evidence from the United States and Israel. *Armed Forces and Society*. 2014. Vol. (40). P. 504–520.

121. CEDMO (Central European Digital Media Observatory). Fact-checking landscape in the Czech Republic: Strengthening regional resilience. Prague: Charles University, 2024. 48 p. URL: https://cedmo.eu/

122. Center for Countering Digital Hate. The disinformation dozen: Why platforms must act on twelve leading online anti-vaxxers. 2021. URL:

123. Center for European Policy Analysis (CEPA). The «Elves» vs. the Trolls: Civil Society's Role in Baltic Information Defense, 2020. https://cepa.org/comprehensive-reports/democratic-offense-against-disinformation/

124. Chadwick A., Stanyer J. Deception as a bridging concept in the study of disinformation, misinformation, and misperceptions: Toward a holistic framework. *Communication Theory*. 2022. Vol. 32(1). P. 1–24.

125. Chan M.-P. S., Jones C. R., Jamieson K. H., Albarracín D. Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation. *Psychological Science.* 2017. Vol. 28, No. 11. P. 1531–1546.

126. Chandler D., Coaffee J. The Routledge Handbook of International Resilience, Routledge, 2017. 402 p.

127. CheckFirst. Loophole: A stress test of the EU's ad transparency rules : Special report. Paris, 2024. 54 p. URL: https://www.checkfirst.network/reports/loophole-ad-transparency-stress-test.

128. Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*. 2019. Vol. 107(6). P.

1753–1820. URL: https://californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security/.

129. Coimisiún na Meán: official website. 2024. URL: https://www.cnam.ie/.

130. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling online disinformation: a European Approach. Brussels, 26.4.2018 COM(2018). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018DC0236

131. Convention for the Protection of Human Rights and Fundamental Freedoms, Pub. L. No. 213 U.N.T.S 221. 1950. URL: https://www.echr.coe.int/Documents/Archives_1950_Convention_ENG.pdf

132. Council of Europe Commissioner for Human Rights. Press freedom must not be undermined by measures to counter disinformation about COVID-19. Commissioner for Human Rights. 2020, March 4. URL: https://www.coe.int/en/web/commissioner/view/-/asset_publisher/ugj3i6qSEkhZ/content/press-freedom-must-not-be-undermined-by-measures-to-counter-disinformation-about-covid-19

133. Council of Europe. CDMSI. Resisting disinformation: 10 building blocks to strengthen information integrity. 2025. December. URL: https://rm.coe.int/resisting-disinformation-10-building-blocks/.

134. Council of the European Union. Council conclusions on Foreign Information Manipulation and Interference (FIMI): (11583/22). 2022. URL: https://data.consilium.europa.eu/doc/document/ST-11583-2022-INIT/en/pdf.

135. Council of the European Union. Council Decision (CFSP) on an Assistance Measure under the European Peace Facility to support the Ukrainian Armed Forces. *Official Journal of the EU*. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401471

136. Council of the European Union. Council Regulation (EU) 2024/2642 of 8 October 2024 establishing a framework for restrictive measures in view of Russia’s

destabilising actions abroad. *Official Journal of the EU*. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/2642/oj/eng

137. Council of the European Union. Joint Security Commitments between the European Union and Ukraine. Brussels, 27 June 2024. 12 p. URL: https://www.consilium.europa.eu/media/oredhmis/eu-ukraine-security-commitments-en.pdf

138. Criminal Code (as amended by the Media and Defamation Act, 2018) Malta. (n.d.). URL:

139. Criminal Code, Austria. URL: https://www.jusline.at/gesetz/stgb

140. Criminal Code, Czech Republic, 2009(2011). URL:

141. Criminal Code, Greece, 2019. URL:

142. Criminal Code, Hungary, 2020. URL:

143. Criminal Code, Slovak Republic, 2005 URL:

144. D'Adamo I., Massimo G., Nallapaneni M. K. Europe moves toward pragmatic sustainability: A more human and fraternal approach. *Sustainability*. 2024. Vol. 16(14). P. 6161. https://www.mdpi.com/2071-1050/16/14/6161

145. Daukšas V. Using AI to spot and stop disinformation in real time: case study of Debunk.org. Medium. 2023. URL: https://medium.com/jigsaw/using-ai-to-spot-and-stop-disinformation-in-real-time-7b3b4a2e6e3c.

146. DEBUNK.ORG: Countering disinformation through analysis and tools. URL: https://www.debunk.org/.

147. DELFI (2025). URL: https://rus.delfi.lv/

148. Demagog.cz. O nás. URL: https://demagog.cz/o-nas

149. Demagog.cz. Ukrajina. URL: https://demagog.cz/tag/ukrajina

150. Demagog.cz. URL: https://demagog.cz/.

151. Deutsche Welle. Polish farmers march to protest Ukrainian imports, EU policy. 2024. URL: https://www.dw.com/en/polish-farmers-march-to-protest-ukrainian-imports-eu-policy/a-68390804

152. Digital Forensic Research Lab (DFRLab). Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Oxford: Oxford

Internet Institute, 2021. URL: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf

153. Digital Forensic Research Lab (DFRLab). Telegram as a weapon: Russian disinformation and information operations in Ukraine: official report. Atlantic Council. 2023. 32 p. URL: https://www.atlanticcouncil.org/wp-content/uploads/2023/05/Telegram-as-a-weapon-Russian-disinformation.pdf.

154. Digital Resilience in the EU: 2025 Country Profiles Update. European Digital Media Observatory (EDMO). Florence: European University Institute, 2025. 112 p. URL: https://edmo.eu/wp-content/uploads/2025/02/Digital-Resilience-EU-Update.pdf.

155. Disinformation Resilience Index 2024: 10 Countries in Focus. ed. by A. Yeliseyeu. EAST Center, Foreign Policy Council «Ukrainian Prism». Warsaw: EAST Center, 2024. 124 p. URL: https://east-center.org/wp-content/uploads/2024/12/DRI_2024_edition.pdf.

156. Disinformation Resilience Index 2024: Central and Eastern Europe / ed. by R. Szostak; East European Council for Strategic Affairs. Prague: EECSA Publishing, 2024. 118 p. URL: https://eecsa.org/dri-2024/.

157. Dobber, T., Ó Fathaigh, R., Zuiderveen Borgesius, F. J. 2019. The regulation of online political micro-targeting in Europe. *Internet Policy Review*, Vol. 8(4). URL: https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe

158. Dov Bachmann S.-D., Putter D., Duczynski G. Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy Journal*, 2023. Vol. 14(5). P. 858–869.

159. Dworkin G. Paternalism. *The Monist*. 1972. Vol. 56(1). P. 64–84.

160. E-ESTONIA. Ukrainian digital infrastructure prevails!. 2022. URL: https://e-estonia.com/ukrainian-digital-infrastructure-prevails/.

161. E-ESTONIA. X-Road: The backbone of e-Estonia. URL: https://e-estonia.com/solutions/interoperability-services/x-road/.

162. ELTA. Lietuvos teritorijoje stabdomas «Gazprom-Media» kontroliuojamų 32 televizijos programų retransliavimas. 2022. URL: https://www.lrt.lt/naujienos/lietuvoje/2/1677312/lietuvos-teritorijoje-stabdomas-gazprom-media-kontroliuojamu-32-televizijos-programu-retransliavimas

163. ENISA. Working Arrangement between the European Union Agency for Cybersecurity (ENISA) and Ukrainian Authorities. 2023. URL: https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity.

164. Eshel Y., Kimhi S. A new perspective on national resilience: Components and demographic predictors. *Journal of Community Psychology*. 2016. Vol. 44 (7). P. 833–844.

165. EU neighbours east. EU4Independent Media: Promoting independent media and high-quality journalism in the Eastern Partnership. 2025. URL: https://euneighbourseast.eu/projects/eu-project-page/?id=1736

166. European Commission, High Representative of the Union for Foreign Affairs and Security Policy. Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation (JOIN/2018/36 final). 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018JC0036.

167. European Commission, High Representative of the Union for Foreign Affairs and Security Policy. Joint Framework on countering hybrid threats: a European Union response (JOIN/2016/018 final). 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

168. European Commission. 2018 Code of practice on disinformation. URL: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

169. European Commission. 2022 Code of practice on disinformation: Transparency Centre. 2022. URL: https://disinfocode.eu/.

170. European Commission. A strengthened EU Code of Practice on Disinformation. 2022. URL: https://commission.europa.eu/topics/countering-information-manipulation/strengthened-eu-code-practice-disinformation_en.

171. European Commission. Action Plan against Disinformation: Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions (JOIN(2018) 36 final). Brussels, 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0036

172. European Commission. Audiovisual Media Services Directive (AVMSD). Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/audiovisual-and-media-services.

173. European Commission. Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors: press release. 2024. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123.

174. European Commission. Communication from the Commission: Digital Education Action Plan (2021-2027) (COM(2020) 624 final) / EUR-Lex. 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624.

175. European Commission. Communication from the Commission: On the European Democracy Action Plan (COM/2020/790 final) / EUR-Lex. 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0790.

176. European Commission. Communication on Tackling COVID-19 disinformation—Getting the facts right JOIN/2020/8 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008

177. European Commission. Digital Services Act package: Deepening the Internal Market and clarifying responsibilities for digital services (2020)2877686. 2020. URL:

178. European Commission. Digital Services Act: List of designated Digital Services Coordinators. 2024. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

179. European Commission. Directorate-General for Communications Networks, Content and Technology. High Level Expert Group on fake news and online disinformation. 2018. URL: https://op.europa.eu/s/tRk9

180. European Commission. European Democracy Action Plan: communication from the Commission (COM(2020) 790 final). Brussels, 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790.

181. European Commission. Horizon Europe. 2021. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

182. European Commission. Integration of the Strengthened Code of Practice on Disinformation into the Digital Services Act framework: Guidance and Decision of the European Board for Digital Services. Brussels, 2025. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

183. European Commission. Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Action Plan against Disinformation**.** Brussels, 5.12.2018. JOIN(2018) 36 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0036

184. European Commission. Questions and Answers – The EU steps up action against disinformation: memo. Brussels, 2018. 5 Dec. URL: https://europa.eu/rapid/press-release_MEMO-18-6648_en.htm.

185. European Commission. Tackling Online Disinformation: A European Approach COM/2018/236 final. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

186. European Commission. Ukraine 2024 Report: Commission Staff Working Document. Brussels, 2024. URL: https://neighbourhood-enlargement.ec.europa.eu/ukraine-report-2024_en.

187. European Commission. Ukraine 2025 Report: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Commission. Brussels,

2025. 142 p. URL: https://enlargement.ec.europa.eu/document/download/17115494-8122-4d10-8a06-2cf275eecde7_en?filename=ukraine-report-2025.pdf

188. European Council. Conclusions on External Relations (March 2015). Official Documents of the European Council. 2015. 12 p. URL: https://www.consilium.europa.eu/en/press/press-releases/2015/03/19/conclusions-russia-ukraine-european-council-march-2015/pdf/

189. European Council. European Council conclusions (19 and 20 March 2015). Brussels: European Council, 2015. 15 p. URL: https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

190. European Council. Sanctions against Russia explained. 2024. URL: https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/.

191. European Court of Auditors. Disinformation affecting the EU: tackled but not tamed: Special Report 09/2021. Luxembourg: Publications Office of the European Union, 2021. 64 p. URL: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf

192. European Democracy Action Plan: making EU democracies stronger. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

193. European Digital Media Observatory (EDMO). About us. URL: https://edmo.eu/about-us/.

194. European Digital Media Observatory (EDMO). Building Digital Resilience: Report on Media Literacy Initiatives in the EU and response to the war in Ukraine. Florence: European University Institute, 2024. 64 p. URL: https://edmo.eu/wp-content/uploads/2024/05/EDMO-Report-Media-Literacy-War-Ukraine.pdf.

195. European Digital Media Observatory (EDMO). Final Report of the EDMO Task Force on the 2024 European Parliament Elections. 2024. URL: https://edmo.eu/publications/final-report-2024-elections/.

196. European Digital Media Observatory (EDMO). How is disinformation addressed in the member states of the European Union? – 27 country cases. Florence: European University Institute, 2024. URL: https://cadmus.eui.eu/handle/1814/76382.

197. European Digital Media Observatory (EDMO). Mapping European media literacy initiatives in response to the war in Ukraine. 2022. 21 June. URL: https://edmo.eu/edmo-news/mapping-european-media-literacy-initiatives-in-response-to-the-war-in-ukraine/.

198. European Digital Media Observatory (EDMO). Standard Operating Procedures for Fact-checking during Crisis Situations. Brussels: EDMO Publications, 2025. 54 p. URL: https://edmo.eu/publications/.

199. European External Action Service. 1st EEAS Report on Foreign Information Manipulation and Interference Threats. Brussels, 2023. URL: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

200. European External Action Service. 1st FIMI Threat Report. 2023. URL: https://euvsdisinfo.eu/eeas-1st-fimi-threat-report-february-2023/.

201. European External Action Service. 2022 Report on EEAS Activities to Counter FIMI. 2023. URL: https://www.eeas.europa.eu/eeas/2022-report-eeas-activities-counter-fimi_en.

202. European External Action Service. 2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI). 2024. URL: https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi_en.

203. European External Action Service. 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. Brussels, 2024. URL: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

204. European External Action Service. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. 2025. URL:

https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en.

205. European External Action Service. Action Plan on Strategic Communication. Brussels, 2015. 22 June. URL: https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf

206. European External Action Service. EU Strategic Communications to counteract anti-EU propaganda: factsheet. Brussels, 2017. 21 Dec. URL: https://www.eeas.europa.eu/node/33130_en.

207. European External Action Service. Rapid Alert System. European Union External Action Service. 2022. URL: https://www.eeas.europa.eu/eeas/rapid-alert-system_en.

208. European External Action Service. Report on Foreign Information Manipulation and Interference Threats. Brussels, 2023. 32 p. URL: https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf.

209. European External Action Service. Stratcom's responses to foreign information manipulation and interference (FIMI) in 2023: official report. Brussels, 2024. URL: https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS%20Stratcom%20Annual%20Report%202023.pdf.

210. European Parliament, Council of the European Union. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

211. European Parliament. 2023 Report on Budgetary and Financial Management. Brussels: European Parliament, 2024. URL: https://www.europarl.europa.eu/cmsdata/286361/2023%20REPORT%20ON%20BUDGETARY%20AND%20FINANCIAL%20MANAGEMENT_v1.pdf.

212. European Parliament. Directive (EU) 2024/1069 on protecting persons who engage in public participation from abusive court proceedings (Strategic lawsuits

against public participation). Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/eli/dir/2024/1069/oj/eng

213. European Parliament. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)). 2016. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html.

214. European Parliament. Foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)). URL: https://www.europarl.europa.eu/doceo/document/A-9-2022-0022_EN.html.

215. European Parliament. Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (ING2): report 2023. URL: https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html.

216. European Union External Action Service EEAS. East StratCom Task Force: 10 Years of Countering Disinformation (Retrospective Report 2015–2025). European Union External Action Service. Brussels, 2025. 42 p.

217. European Union External Action Service EEAS. EU-Ukraine Cybersecurity Dialogue: 3rd meeting in Brussels. Official Press Release. July 2024. URL: https://www.eeas.europa.eu/eeas/eu-ukraine-cybersecurity-dialogue-3rd-meeting-brussels_en.

218. European Union External Action Service. 3rd Annual Report on Foreign Information Manipulation and Interference (FIMI) Threats: Networked Defence in Action. European Union External Action Service. March 2025. 54 p. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

219. European Union External Action Service. Countering Hybrid Threats. 2023. URL: https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en.

220. European Union External Action Service. Tackling Disinformation, Foreign Information Manipulation & Interference. 2021. URL:

https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

221. European Union. Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from abusive court proceedings (Strategic lawsuits against public participation). Official Journal of the EU. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401069&qid=1717387998140

222. European Union. Joint Statement following the 22nd EU-Ukraine Summit (Brussels, 6 October 2020). Council of the European Union. 2020. URL: https://www.president.gov.ua/en/news/spilna-zayava-za-pidsumkami-22-go-samitu-ukrayina-yes-64321

223. European Union. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). Official Journal of the European Union. 2022. URL: https://www.europeansources.info/record/proposal-for-a-regulation-on-a-single-market-for-digital-services-digital-services-act-and-amending-directive-2000-31-ec/

224. EUvsDisinfo. About. European Union External Action Service. URL: https://euvsdisinfo.eu/about/.

225. EUvsDisinfo. Disinfo Database. 2026. URL: https://euvsdisinfo.eu/disinformation-cases/.

226. Ferrara E., Varol O., Davis C., Menczer F., Flammini A. The rise of social bots. *Communications of the ACM.* 2016. Vol. 59, No. 7. P. 96–104. DOI:

227. Flora C. B., Lyson T. A., Spears J. D. Rural communities: legacy and change Contemporary Sociology A Journal of Reviews. 1993. Vol. 22(5). DOI:10.2307/2074627.

228. Floridi L. The philosophy of information. New York: Oxford University Press, 2011. 405 p.

229. Fojo Media Institute. Strengthening journalism for a democratic and sustainable world. Kalmar: Linnaeus University. URL: https://fojo.se/en/.

230. Foucault M. Power/knowledge: Selected interviews and other writings, 1972–1977. Knopf Doubleday Publishing Group, 1980. URL: https://books.google.com.ua/books/about/Power_Knowledge.html?id=RGeNEAAAQBAJ&redir_esc=y

231. Fox C. J. Information and Misinformation: An Investigation of the Notions of Information, Misinformation, Informing, and Misinforming. Greenwood Publishing Group, 1983. https://philpapers.org/rec/FOXIAM

232. Galeotti M. Putin's Wars: From Chechnya to Ukraine / M. Galeotti. Oxford: Osprey Publishing, 2023. 384 p.

233. Gavriněv V. Šéf boje s dezinformacemi popisuje utajovaný vládní plán. Seznam Zprávy. 2023. URL: https://www.seznamzpravy.cz/clanek/domaci-politika-sef-boje-s-dezinformacemi-popisuje-utajovany-plan-penize-dostanou-i-media-225117

234. Gherman M., Melnychuk L., Shuliak A. Anti-western narratives in Ukraine and Romania (comparative analysis). *Ideology and Politics Journal. Special issue "Anti-Americanism and anti-Western sentiments in Europe and post-Soviet states"*. 2024. Issue № 2(26). P. 150-174.

235. Giusti S. La disinformazione e la politica estera. *Vita e Pensiero.* 2023. Vol. 1. URL: https://www.researchgate.net/publication/370426507_La_disinformazione_e_la_politica_estera

236. Global Harmonization Task Force. Quality Management Systems-Process Validation Guidance (GHTF/SG3/N99-10:2004 (Edition 2). 2004. URL: https://ahwp.info/sites/default/files/6_APEC__SG3_Process_Validation_Training_KL_2008__Gunter_Frey.pdf

237. Gomez-Herrera E., Martens B. Digital Platforms and Ecosystems: a Review of Relevant Economic and Policy Issues. Joint Research Centre (JRC). *Digital Economy Working Paper* 2021-05. Seville: European Commission, 2021. 38 p. URL: https://joint-research-centre.ec.europa.eu/publications/digital-platforms-and-ecosystems-review-relevant-economic-and-policy-issues_en.

238. Goodin R. E. (ed). The Theory of Institutional Design. New York: Cambridge University Press, 1996. 288 p.

239. Gotev G. Hahn: We have some ideas how to deal with Russian propaganda. EURACTIV. 2014. URL: https://www.euractiv.com/news/hahn-we-have-some-ideas-how-to-deal-with-russian-propaganda/

240. Graves L. Deciding What's True: The Rise of Political Fact-Checking in American Journalism / Lucas Graves. New York: Columbia University Press, 2016. 320 p.

241. Grigas A. Legacies, coercion and soft power: Russian influence in the Baltic states. *The Means and Ends of Russian Influence Abroad Series*. 2012. URL: https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0812bp_grigas.pdf

242. Guess A., Lyons B. Misinformation, Disinformation, and Online Propaganda. *Social Media and Democracy*. 2020. September. P.10–33.

243. Gwara Media. Organization details. 2023. URL: https://ifcncodeofprinciples.poynter.org/profile/gwara-media

244. Haas E. B. The uniting of Europe: political, social, and economic forces, 1950–1957 (3rd ed.), Notre Dame, Indiana: University of Notre Dame Press, 2004 1958. 552 p. https://www.europarl.europa.eu/100books/file/EN-H-BW-0038-The-uniting-of-Europe.pdf

245. Hall P. A., Taylor R. C. R. Political Science and the Three New Institutionalisms. *Political Studies.* 1995. Vol. 55(1). P. 936 – 957.

246. Hameleers M. Populist Disinformation: Exploring Intersections between Online Populism and Disinformation in the US and the Netherlands. *Politics and Governance.* 2020. Vol. 8(1). P. 146–157.

247. Hameleers M., Powell T., Van der Meer T., Bos L. A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media". *Political Communication*. 2020. Vol. 37. P. 1–21.

248. Harjani T., Roozenbeek J., Van Der Linden S. A Practical Guide to Prebunking Misinformation. Cambridge: University of Cambridge; London: BBC Media Action; New York: Jigsaw, 2022. 38 p. URL: https://socialdecisionmaking.com/prebunking-guide.

249. Harrington L. M. B. Sustainability Theory and Conceptual Considerations: A Review of Key Ideas for Sustainability, and the Rural Context. *Papers in Applied Geography*. 2016. Vol. *2*(4). P. 365–382.

250. Higgins E. We Are Bellingcat: An Intelligence Agency for the People / Eliot Higgins. London: Bloomsbury Publishing, 2023. 272 p.

251. Hobfoll S. E., Hall B. J., Canetti-Nisim D., Galea S., Johnson R. J., Palmieri P. A. Refining our understanding of traumatic growth in the face of terrorism: Moving from meaning cognitions to doing what is meaningful. *Applied Psychology*. 2007. Vol. 56 (3). P. 345–366.

252. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies, 2007. 72 p.

253. Human Rights Committee. Concluding Observations of the Human Rights Committee: Cameroon. 1999. URL: https://www.refworld.org/docid/3ae6b01014.html

254. Immenkamp B. Understanding EU counter-terrorism policy (Briefing) / European Parliamentary Research Service (EPRS). 2021. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/659446/EPRS_BRI(2021)659446_EN.pdf.

255. Immergut E. The Theoretical Core of the New institutionalism. *Politics and Society*. 1998. Vol. 1. P. 5-34.

256. International Centre for Defence and Security (ICDS). (2022). The Information Front: Baltic Responses to Russia's 2022 Invasion. Tallinn, Estonia. URL: https://icds.ee/en/

257. International Centre for Defence and Security (ICDS). Digitalization and Resilience: The Baltic Experience in Hybrid Warfare. Tallinn, 2021. URL: https://www.researchgate.net/publication/397436457_Understanding_the_Resilience_to_Hybrid_Threats_in_the_Baltics

258. International Covenant on Civil and Political Rights, Pub. L. No. 99 U.N.T.S. 171 (1966). URL: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

259. International Fact-Checking Network (IFCN). Code of principles / Poynter Institute. 2016. URL: https://www.poynter.org/ifcn-fact-checkers-code-of-principles/.

260. International Fact-Checking Network. 2025. URL: https://www.poynter.org/ifcn/

261. Internews. Медіаспоживання українців: результати загальнонаціонального опитування 2025: аналітичний звіт. Київ: Медійна програма в Україні (USAID), 2025. URL: https://internews.ua/opportunity/media_trust_consumption_2025_release.

262. Jačauskas I., Beniušis V. Radijo ir televizijos komisija uždraudė Lietuvoje retransliuoti RT programas. 2020. URL: https://www.lrt.lt/naujienos/lietuvoje/2/1195699/radijo-ir-televizijos-komisija-uzdraude-lietuvoje-retransliuoti-rt-programas

263. Jack C. Lexicon of lies: Terms for problematic information. Data & Society Research Institute. 2017. URL: https://apo.org.au/sites/default/files/resource-files/2017-08/apo-nid183786.pdf

264. Janda J., Víchová V. The Kremlin's Platform in the Czech Republic. European Values Center for Security Policy, 2016. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/655290/IPOL_STU(2020)655290_EN.pdf

265. Jeangène V. J.-B. Information Manipulation: A Challenge for Our Democracies. Paris: CAPS (Ministry for Europe and Foreign Affairs) / IRSEM (Ministry of the Armed Forces), 2018. 210 p. URL: https://www.defense.gouv.fr/irsem/publications/rapport-caps-irsem-manipulations-linformation.

266. Jeangène Vilmer J.-B., Escorcia A., Guillaume M., Janovsky J. Les Manipulations de l'information: un défi pour nos démocraties: rapport. Paris: CAPS; IRSEM, 2021. 215 p. URL: https://www.diplomatie.gouv.fr/IMG/pdf/7_carnets_26_dossier_manip_info_ae_jbjv_cle811215.pdf

267. Jensen C. S. Neo-functionalism. *European Union Politics.* M. Cini, & N. P.-S. Borragán (Eds.), 6 ed. Oxford University Press, 2019. P. 55-68.

268. Joint Communication Action Plan against Disinformation. Brussels, 5.12.2018 JOIN(2018). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0036

269. Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions. Action Plan against Disinformation. Brussels, 5.12.2018 JOIN(2018). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0036

270. Justice for Journalists Foundation. Written statement by Justice for Journalists Foundation. 2023, October 5. URL: https://jfj.fund/written-statement-by-justice-for-journalists-foundation-2/

271. Kartous B. Czech Elves: Fighting Disinformation in the Heart of Europe. Prague Security Studies Institute Report, 2019. URL: https://www.freiheit.org/central-europe-and-baltic-states/how-czech-elves-are-fighting-russian-disinformation

272. Kaya R. Post Functionalism, Notes and Comments and Crises. URL: https://www.academia.edu/35712223/Post_Functionalism_Notes_and_Comments_and_Crises

273. Kimhi S., Eshel Y. Measuring national resilience: A new short version of the scale (NR-13). *Journal of Community Psychology.* 2018. Vol. 47(1). P. 517–528.

274. Kimhi S., Eshel Y., Zysberg L., Hantman S., Enosh G. Sense of coherence and socio-demographic characteristics predicting posttraumatic stress symptoms and recovery in the aftermath of the second lebanon war. *Anxiety, Stress and Coping.* 2010. Vol. 23(2). P. 139–152.

275. Kitt A., Magi M. Data Embassies: A new concept for digital continuity. Estonian Information System Authority. 2018. URL: https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/.

276. Knight J. Institutions and Social Conflict. New York: Cambridge University Press, 1992. 234 p.

277. Kosheliuk O., Blahovirna N. News in Mobile Air Raid Alert Apps and Media Literacy in Ukraine During the War Time. *Media Literacy and Academic Research.* 2025. Vol. 8(1). P. 178–193.

278. Kruglashov A. A Long Way From Ghost of the Failed State to Resistance and Resilience: The Case of Ukraine. In: Rouet, G., Pascariu, G.C. (eds) Resilience and the EU's Eastern Neighbourhood Countries. Palgrave Macmillan, Cham, 2025. P. 523–547.

279. KSI Blockchain: technology overview. Guardtime. 2024. URL: https://guardtime.com/technology/ksi-blockchain.

280. Kuklinski, J. H., Quirk, P. J., Schwieder, D. W., Rich, R. F. Just the facts, ma'am': Political facts and public opinion. *The Annals of the American Academy of Political and Social Science*. 1998. Vol. 560(1). P. 143–154.

281. Landesmedienanstalten / die medienanstalten. URL: https://www.die-medienanstalten.de/ueber-uns/landesmedienanstalten/.

282. Lash S. Critique of information. SAGE Publications Ltd, 2002. 234 p.

283. Latvijas kiberdrošības stratēģija 2019–2022. gadam: informatīvais ziņojums. Latvijas Republikas Aizsardzības ministrija ; Artis Pabriks. Rīga, 2019. URL:
https://www.mod.gov.lv/sites/mod/files/document/Latvijas_kiberdrosibas_strategija_2019-2022.pdf /

284. Law 2018-1202 of 22 December 2018 on the fight against the manipulation of information, France. URL:

285. Lazer D. M. J. The science of fake news. *Science*. 2018. Vol. 359(6380). P. 1094-1096.

286. Lee J. E. C., Sudom K. A., Zamorski M. A. Longitudinal analysis of psychological resilience and mental health in Canadian military personnel returning from overseas deployment. *Journal of occupational health psychology*. 2013. Vol. 18 (3). P. 327–337.

287. Légifrance 2021. Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé «service de vigilance et de protection contre les ingérences numériques étrangères». https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361

288. Légifrance. 2018. Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. URL: https://www.legifrance.gouv.fr/download/pdf?id=6-nJtAIQpD8-Ugn4wumM7q3PzXyh2U2x_naRfEud_Wg=

289. Légifrance. Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information». URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020828212

290. Levi L. Real fake news and fake fake news. *First Amendment Law Review*. 2018. Vol. 16. P. 223-327.

291. Lietuvos radijo ir televizijos komisija. Blokuojami 53 IP adresai, kuriais pasiekiami Rusijos propagandiniai kanalai. 2023. URL: https://www.rtk.lt/lt/naujienos/blokuojami-53-ip-adresai-kuriais-pasiekiami-rusijos-propagandiniai-kanalai

292. Longstaff P. H., Koslowski T. G., Geoghegan W. Translating Resilience: A Framework to Enhance Communication and Implementation. *Environmental Science*. 2013. URL: https://www.semanticscholar.org/paper/Translating-Resilience%3A-A-Framework-to-Enhance-and-Longstaff-Koslowski/8b6aaba82c7ca6cb550c75a97c00347b767d0e44.

293. LSM+.2. Учим латышский. 2025. URL: https://rus.lsm.lv/tema/ucim-latysskii/

294. LSM+ RUS.LSM. 2025. URL: https://rus.lsm.lv/

295. LSM+. Медиаграмотность. 2025. URL: https://rus.lsm.lv/novosti/mediagramotnost/

296. Lucas E., Pomerantsev P. Winning the information war: Techniques and counter-strategies to Russian propaganda in Central and Eastern Europe. *The Information Warfare Project.* The Centre for European Policy Analysis. 2016. URL: https://cepa.ecms.pl/files/?id_plik=2706

297. Lutsevych O. Resilient Society: Ukraine's lessons for Europe / O. Lutsevych. London: Chatham House, 2023. 52 p.

298. Lyberytė, A. Pratęstas draudimas retransliuoti Rusijos ir Baltarusijos kanalų programas. 2024. URL: https://www.lrt.lt/naujienos/lietuvoje/2/2296254/pratestas-draudimas-retransliuoti-rusijos-ir-baltarusijos-kanalu-programas

299. MacCarthy M. Machines learn that Brussels writes the rules: The EU's new AI regulation. Brookings. 2021. URL: https://www.brookings.edu/articles/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

300. Madiega T. Digital Services Act: EU Legislation in Progress. European Parliamentary Research Service. 2022. 12 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf.

301. Mahl D., Zeng J., Schäfer M. S. Conceptualizing platformed conspiracism: Analytical framework and empirical case study of BitChute and Gab. *New Media & Society*. 2024. Vol. 26(12). P. 6938–6957.

302. Majandusja Kommunikatsiooniministeerium. Digiühiskonna arengukava 2030: strateegiline dokument. Tallinn, 2021. 68 p. URL: https://www.mkm.ee/strateegia-ja-valdkonnad/infotehnoloogia/digiuhiskonna-arengukava.

303. March J. G., Olsen J. P. Elaborating the «new institutionalism». Centre for European Studies University of Oslo. *Working Paper*. March. Vol. 11. http://www.unesco.amu.edu.pl/pdf/olsen2.pdf

304. March J. G., Olsen J. P. The New Institutionalism: Organizational Factors in Political Life. *American Political Science Review.* 1984. Vol. 78(37). P. 734–749.

305. Marres N. Why we can't have our facts back. *Engaging Science, Technology, and Society*. 2018. Vol. 4. P. 423–443.

306. McKinsey & Company. Winning in digital ecosystems: digital insights report. New York: McKinsey Digital, 2018. 22 p. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/winning-in-digital-ecosystems.

307. Media literacy. Shaping Europe's digital future – European Union. 2025. November 11. URL: https://digital-strategy.ec.europa.eu/en/policies/media-literacy.

308. Media Literacy Index 2025: Resilience to Post-Truth in Europe / Open Society Institute – Sofia. Sofia: OSI, 2025. 34 p. URL: https://osis.bg/wp-content/uploads/2025/10/Media-Literacy-Index-2025.pdf.

309. MediaSapiens: офіційний сайт. URL: https://ms.detector.media/

310. MediaSapiens. Єврокомісія запускає Rapid Alert System для боротьби з дезінформацією на території Євросоюзу. 2019, 15 березня. URL: https://ms.detector.media/media-i-vlada/post/22610/2019-03-15-ievrokomisiya-zapuskaie-rapid-alert-system-dlya-borotby-z-dezinformatsiieyu-na-terytorii-ievrosoyuzu/

311. Merkel W., Croissant A. Formale und informale Institutionen in defekten Demokratien. *PVS. 2000.* Vol. 41. S. 3–30. URL: https://link.springer.com/article/10.1007/s11615-000-0002-9?utm_source=copilot.com

312. Methodology and Impact Report: AI-Driven Analysis of Information Flows in the Baltic States. 2023. URL: https://www.debunk.org/methodology

313. Morgan S. Fake news, disinformation, manipulation and online tacticsto undermine democracy. *Journal of Cyber Policy.* 2018. Vol. 3, no.1, p. 39–43.

314. National Counter Disinformation Strategy Working Group: Final Report and Recommendations. Independent Chair: Martina Chapman. Dublin, 2025. URL: https://www.gov.ie/en/department-of-culture-communications-and-sport/publications/.

315. National Cyber Security Index – Latvia. E-Governance Academy. Tallinn, 2022. URL: https://ncsi.ega.ee/country/lv/.

316. National Cyber Security Strategy and Information Defense Guidelines / Ministry of National Defence of the Republic of Lithuania. Vilnius, 2023. URL: https://www.nksc.lt/en/

317. National Media Education Policy 2025 / KAVI – Kansallinen audiovisuaalinen instituutti. Helsinki, 2025. URL: https://kavi.fi/en/media-education/.

318. NATO and Guardtime to collaborate on cyber defence: news. NATO. 2021. URL: https://www.nato.int/cps/en/natohq/news_182142.htm.

319. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn: NATO CCDCOE. URL: https://ccdcoe.org/.

320. NATO Strategic Communications Centre of Excellence. Robotrolling: Analysis of Bot Activity in Social Media: strategic report. Riga: NATO StratCom COE, 2023. 42 p. URL: https://stratcomcoe.org/publications/robotrolling-2023/.

321. NATO Strategic Communications Centre of Excellence. The "Elves" of Lithuania: Voluntary Digital Resilience. Riga. 2018. URL: https://www.nksc.lt/en/

322. NATO Strategic Communications Centre of Excellence. The Role of Telegram in Contemporary Conflict: analysis. Riga: NATO StratCom COE, 2024. 48 p. URL: https://stratcomcoe.org/publications/download/Telegram-in-Conflict-Analysis.pdf.

323. Nazarov M. National Resilience and Post-war Reconstruction of Ukraine. *Ukraine's Journey to Recovery, Reform and Post-War Reconstruction. Contributions to Security and Defence Studies.* Nate S. (eds) Springer, Cham, 2025. P. 63–73.

324. Next level partnership: Bolstering EU-NATO cooperation to counter hybrid threats in the Western Balkans. European Union Institute for Security Studies

(EUISS). 2023. URL: https://www.iss.europa.eu/publications/briefs/next-level-partnership-bolstering-eu-nato-cooperation-counter-hybrid-threats

325. Niemann A. Neofunctionalism. *The Palgrave Handbook of EU Crises.* Riddervold, M., Trondal, J., Newsome, A. (eds) Palgrave Studies in European Union Politics. Palgrave Macmillan, Cham, 2021. https://link.springer.com/chapter/10.1007/978-3-030-51791-5_6#citeas

326. Niklewicz K. Weeding out Fake News: An Approach to Social Media Regulation, Brussels, Wilfried Martens Centre for European Studies, 2017.

327. North D. C. Institutions, Institutional Change and Economic Performance. New York: Cambridge University Press; 1990. 152 p.

328. Office of the Government of the Czech Republic, Government Commissioner for Media and Disinformation. Akční plán pro čelení dezinformacím [Action Plan for Countering Disinformation]. 2023. URL: https://www.irozhlas.cz/sites/default/files/uploader_unmanaged/ap_dezinfo_230116-183115_cib.pdf

329. Online Safety and Media Regulation Act 2022: Act of the Oireachtas. No. 41 of 2022. URL: https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/html.

330. Osmundsen M., Bor A., Vahlstrup P. B., Bechmann A., Petersen M. B. Partisan polarization is the primary psychological motivation behind political fake news sharing on Twitter. *American Political Science Review.* 2021. Vol. 115(3). P. 999–1015.

331. Pamment J. The EU Hybrid Toolbox and the evolution of strategic communications. *Journal of Cyber Policy.* 2025. Vol. 9, No. 1. P. 12–29.

332. Pamment J. The EU vs Disinfo: A Strategic Assessment of Early Responses to Information Warfare. *Journal of Strategic Communication.* 2024. Vol. 12(2). P. 45–62.

333. Pamment J. The EU's Role in Fighting Disinformation: Taking Stock of the Action Plan. Washington, D.C.: Carnegie Endowment for International Peace, 2020. 44 p. URL: https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-stock-of-action-plan-pub-82286.

334. Pamment J., Nothhaft H., Agardh-Twetman S., Fjällhed A. Resisting Information Influence Activities: a guide for government and public sector organizations. Riga: NATO StratCom COE, 2018. 82 p. URL: https://stratcomcoe.org/publications/resisting-information-influence-activities-a-guide-for-government-and-public-sector-organisations/168.

335. 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(7). P. 770–780.

336. PESCO. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT): project overview. 2024. URL: https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

337. Peters G. Institutional Theory in Political Science: The New Institutionalism. 4th ed. Edward Elgar Publishing, 2019. 304 p.

338. Phillips W., Milner R. M. You are here: A field guide for navigating polarized speech, conspiracy theories, and our polluted media landscape. MIT Press, 2021.

339. Pipchenko N. O., Yurii A. Media literacy and psychological resilience: the Swedish approach to countering disinformation. *Actual Problems of International Relations*. 2025. Вип. 162(1). С. 16–23.

340. Pipchenko N. Transformation of Foreign-Policy Communication of the EU, Germany, and Ukraine. *International relations, public communications and regional studies*. 2022. Вип. 2 (13). С. 92-101.

341. President of Romania. Decree signed by the President of Romania, Mr. Klaus Iohannis, regarding the establishment of the state of emergency on the Romanian territory. 2020. URL: https://www.presidency.ro/ro/media/decrete-si-acte-oficiale/decret-semnat-de-presedintele-romaniei-domnul-klaus-iohannis-privind-instituirea-starii-de-urgenta-pe-teritoriul-romaniei

342. Pressman R. S. Software Engineering: A Practitioner's Approach. 9th ed. New York: McGraw-Hill Education, 2023. 968 p.

343. Public Report on Counter-Disinformation Efforts and StratCom Mechanisms / Lithuanian Armed Forces Strategic Communications Department. 2022. URL: https://www.eeas.europa.eu/eeas/2022-report-eeas-activities-counter-fimi_en

344. Radu R. Fighting the 'Infodemic': Legal Responses to COVID-19 Disinformation. *Social Media + Society*. 2020. Vol. 6(3). URL: https://journals.sagepub.com/doi/full/10.1177/2056305120948190

345. Rapport technique: Identification d'un réseau structuré et coordonné de diffusion de propagande pro-russe «Portal Komba». VIGINUM. Paris, 2024. 12 février. 22 p. URL: https://www.sgdsn.gouv.fr/publications/rapport-technique-portal-kombat.

346. Razumkov Centre. Ukraine 2019-2020: Wide Opportunities, Ambiguous Results. 2020. URL: https://razumkov.org.ua/uploads/other/2020-PIDSUMKI-ENG.pdf

347. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. L 2024/1689. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

348. Report on implementation of the Association Agreement between Ukraine and the European Union for 2023. URL: https://eu-ua.kmu.gov.ua/wp-content/uploads/Report-on-implementation-of-the-Association-Agreement-between-Ukraine-and-the-European-Union-for-2023.pdf

349. Report on implementation of the Association Agreement between Ukraine and the European Union for 2024. URL: https://eu-ua.kmu.gov.ua/wp-content/uploads/Zvit-Ugoda-pro-asotsiatsiyu-EN.pdf

350. Reporters Without Borders. The Propaganda Machine: How Russia's state media is funded. Paris: RSF, 2022. URL: https://rsf.org/en/russia-s-state-media-budget-surges-40-amid-war-ukraine.

351. Reuters. Deepfake footage purports to show Ukrainian president capitulating. 2022. URL: https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/ .

352. Reuters. Why are farmers protesting across Europe? 2024. URL: https://www.reuters.com/world/europe/why-are-farmers-protesting-across-europe-2024-01-30/

353. Riigi Valimisteenistus. Hääletamisest osavõtt: Riigikogu valimised 2023: statistiline aruanne. Tallinn, 2023. URL: https://rk2023.valimised.ee/et/participation/overall.

354. Roggeveen B. Mapping the fault lines: The conceptual fault lines in the EU debate on Russia. *Foundation for European Progressive Studies*. 2022. P. 1-27 URL: https://feps-europe.eu/wp-content/uploads/downloads/publications/220210%20policy%20brief%20final_eu-russia%20-barbara%20roggeveen.pdf

355. Roozenbeek J., van der Linden S., Nygren T. Prebunking interventions based on «inoculation» theory can reduce susceptibility to misinformation across cultures. *Harvard Kennedy School (HKS) Misinformation Review.* 2020. Vol. 1, Iss. 2. URL: https://misinforeview.hks.harvard.edu/article/prebunking-interventions-based-on-inoculation-theory-can-reduce-susceptibility-to-misinformation-across-cultures/.

356. Ryan E. 2025 census: Fact-checkers persevere as politicians, platforms turn up heat. *Reporters' Lab (Duke University).* 2025. June 19. URL: https://reporterslab.org/2025/06/19/fact-checkers-persevere-as-politicians-platforms-turn-up-heat/.

357. Social Media Survey 2025: Flash Eurobarometer FL014EP : report / Ipsos European Public Affairs; European Parliament. Brussels , 2025. 138 p. URL: https://europa.eu/eurobarometer/surveys/detail/3592

358. Scaling Prebunking: A Practical Guide to Prebunking Misinformation. URL: https://prebunking.withgoogle.com/docs/A_Practical_Guide_to_Prebunking_Misinformation.pdf

359. Schmitter P. Ernst B. Haas and the legacy of neofunctionalism. *Journal of European Public Policy*. 2005. Vol. 12(2). P. 255–272. URL: https://www.tandfonline.com/doi/abs/10.1080/13501760500043951

360. Schulz W., Potthast K., & Helberger N. Wissenschaftskommunikation und Social Media zwischen Rechtsschutz und Regulierungsbedarf. Berlin-Brandenburgische Akademie der Wissenschaften, 2021.

361. Scott W. R. Institutions and Organizations: Foundations for Organizational Science. Thousand Oaks, 1995. 200 p.

362. Secrétariat Général De La Défense Et De La Sécurité Nationale (SGDSN). «Portal Kombat»: un réseau structuré et coordonné de propagande prorusse. 2024. URL: https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse.

363. Senyo P. K., Liu K., Effah J. Digital business ecosystem: Literature review and a framework for future research. *International Journal of Information Management.* 2019. Vol. 47. P. 52–64. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.01.002

364. Shannon C. E. A mathematical theory of communication. *Bell System Technical Journal*. 1948. Vol. 27(3). P. 379–423. URL: https://onlinelibrary.wiley.com/doi/10.1002/j.1538-7305.1948.tb01338.x

365. Silverman C. Verification Handbook: A definitive guide to verifying digital content for emergency coverage. Maastricht: European Journalism Centre, 2020. 120 p.

366. Skocpol T. States and Social Revolutions: A Comparative Analysis of France, Russia and China. Cambridge, 1979. 419 p. URL: http://drmalik.atw.hu/RM/skocpol.pdf

367. Skowronek S. Orren K. Beyond the Iconography of Order: Notes for a «New Institutionalism». *The Dynamics of American Politics: Approaches and Interpretations.* Boulder, 1994. 312 p.

368. Solopova VFrom Trust to Truth: Actionable policies for the use of AI in fact-checking in Germany and Ukraine. *Technische Universität Berlin*. 2024. URL: https://arxiv.org/pdf/2503.18724

369. Southwell B. G., Brennen J. S. B., Paquin R., Boudewyns V., Zeng J. Defining and measuring scientific misinformation. *The Annals of the American Academy of Political and Social Science*. 2022. Vol. 700(1). P. 98–111.

370. Southwell B. G., Thorson E. A., Sheble L. The persistence and peril of misinformation. *American Scientist*. 2017. Vol. 105(6). P. 372–375.

371. Special Report Disinformation affecting the EU: tackled but not tamed. URL: https://www.eca.europa.eu/lists/ecadocuments/sr21_09/sr_disinformation_en.pdf

372. STOPFAKE: офіційний сайт. Центр медіареформ. URL: https://www.stopfake.org/uk/golovna/.

373. Sutton R. M., Douglas K. M. Conspiracy theories and the conspiracy mindset: Implications for political ideology. *Current Opinion in Behavioral Sciences*. 2020. Vol. 34. P. 118–122.

374. Swedish Psychological Defence Agency (MPF). Don't be fooled. URL: https://bliintelurad.se/en

375. Tandoc E. C., Lim Z. W., & Ling R. Defining "Fake News": A typology of scholarly definitions. *Digital Journalism*. 2018. Vol. 6(2). P. 137–153.

376. Tandoc E. C., Lim Z. W., Ling R. The 'fake news' label: it's not about truth. *Palgrave Communications.* 2019. Vol. 5, art. 71. DOI: https://doi.org/10.1057/s41599-019-0279-9.

377. Tang L., Fujimoto K., Amith M. T., Cunningham R., Costantini R. A., York F., Xiong G., Boom J. A., Tao C. 'Down the rabbit hole' of vaccine misinformation on YouTube: Network exposure study. *Journal of Medical Internet Research*. 2021. Vol. 23(1). URL: https://www.jmir.org/2021/1/e23262/

378. Teperik D., Denisa-Liepniece S., Bankauskaitė D., Kullamaa K. Resilience Against Disinformation: A New Baltic Way to Follow? Tallinn: International Centre for Defence and Security (ICDS), 2022. 64 p. URL:

https://www.researchgate.net/publication/364474732_Resilience_Against_Disinformation_A_New_Baltic_Way_to_Follow.

379. Teyssou D. WeVerify: Wider and deeper verification for all / InVID Project. 2020. 17 June. URL: https://www.invid-project.eu/weverify-wider-and-deeper-verification-for-all/

380. The 2007 Cyber Attacks on Estonia, Ten Years On: report. Tiit Tammes (ed.). Tallinn, 2017. 44 p. URL: https://ccdcoe.org/library/publications/the-2007-cyber-attacks-on-estonia-ten-years-on/.

381. The European Digital Media Observatory project kicks off. European Commission: Shaping Europe's digital future. 2020. June 2. URL: https://digital-strategy.ec.europa.eu/en/news/european-digital-media-observatory-project-kicks.

382. The Strengthened Code of Practice on Disinformation 2022. URL: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

383. Thorson E. A., Sheble L., Southwell, B. G. Conclusion: An agenda for misinformation research. In: *Misinformation and mass audiences.* Eds. B. G. Southwell, E. A. Thorson, L. Sheble. University of Texas Press, 2018. URL: https://www.researchgate.net/publication/355300647_Conclusion_An_Agenda_for_Misinformation_Research

384. Tiesību aktu projektu publiskais portāls. (2023). Informatīvais ziņojums «Nacionālās drošības koncepcija 2023». URL: https://tapportals.mk.gov.lv/legal_acts/16851249-a50a-4e69-a05b-fc4b23bf0162#

385. TikTok. TikTok's Fifth Transparency Report: Our Progress Under the EU Disinformation Code. 2024. URL: https://newsroom.tiktok.com/en-eu/tiktoks-fifth-transparency-report-our-progress-under-the-eu-disinformation-code.

386. Treaty on the Functioning of the European Union (Consolidated Version) 2012/C 326/01. *Offical Journal of the European Union.* 2012. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:FULL:EN:PDF

387. Van Hoboken J., Ó Fathaigh, R. Regulating Disinformation in Europe: Implications for Speech and Privacy. *UC Irvine Journal of International, Transnational, and Comparative Law, 6,* 9–36.

388. VERA.ai: Verification Assisted by Artificial Intelligence: official project website. 2024. URL: https://www.veraai.eu/.

389. VERA.ai: Verification assisted by artificial intelligence. 2022. URL: https://www.veraai.eu/home.

390. VIGINUM: missions et fonctionnement. Secrétariat général de la défense et de la sécurité nationale (SGDSN). 2024. URL: https://www.sgdsn.gouv.fr/missions/proteger-la-nation-face-aux-menaces/viginum.

391. VoxCheck. Аналітична платформа «Вокс Україна»: партнерство з державними безпековими структурами. URL: https://voxukraine.org/

392. Vraga E. K., Bode L. Defining misinformation and understanding its bounded nature: Using expertise and evidence for describing misinformation. *Political Communication*. 2020. Vol. 37(1). P. 136–144.

393. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making. *Council of Europe report.* 2017. Vol. 27. URL: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

394. Warleigh A. Understanding European Union Institutions. London, N.Y.: Routledge, 2002. 202 p.

395. Wasinton C. Fake news and information manipulation: Investigation on the features and objectives of the Russian disinformation campaigns in the European Union: Master's thesis. Bologna: University of Bologna, 2019. 115 p. URL: https://amslaurea.unibo.it/18606/.

396. Weingast B. R. Political Institutions: Rational Choice Perspectives. *A New Handbook of Political Science.* Robert E. Goodin, and Hans-Dieter Klingemann (eds), Oxford, 1998. URL: https://www.researchgate.net/publication/259934175_Political_Institutions_Rational_Choice_Perspectives

397. WeVerify. About WeVerify. URL: https://weverify.eu/about/.

398. Wigell M., Mikkola H., Juntunen T. Best Practices in the whole-of-society approach in countering hybrid threats. European Parliament, Directorate General for External Policies. 2021. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf

399. Winnerstig M. Tools of Destabilization: Russian soft power and non-military influence in the Baltic states. 2014. URL: http://appc.lv/wp-content/uploads/2014/12/FOI_Non_military.pdf

400. Woolley S. C., Howard P. N. (Eds). Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford: Oxford University Press, 2018. 288 p.

401. World Health Organization. What is Go Viral? 2021. URL: https://www.who.int/news/item/23-09-2021-what-is-go-viral

402. Yatid M. M. Truth Tampering Through Social Media: Malaysia's Approach in Fighting Disinformation & Misinformation. *IKAT: The Indonesian Journal of Southeast Asian Studies.* 2019. Vol. 2(2). P. 203—230. doi: 22146/ikat.v2i2.40482.

403. Yoffie D. B., Baldwin C. Y. Apple Inc. in 2020. Harvard Business School Case 720-422. Boston: Harvard Business School Publishing, 2020. 34 p. URL: https://hbsp.harvard.edu/product/720422-PDF-ENG.

404. Ziegler R., Ott K. The quality of sustainability science: a philosophical perspective. *Sustainability: Science, Practice and Policy*. 2011. Vol. 7(1). P. 31–44.

405. Zubiaga A. Detection and Resolution of Rumours in Social Media: A Survey / Arkaitz Zubiaga, Elena Kochkina, Maria Liakata. *ACM Computing Surveys*. 2018. Vol. 51(2). P. 1–36.

ДОДАТКИ

Додаток А
ПРОБЛЕМИ ВИЗНАЧЕННЯ ЗМІСТУ ПОНЯТТЯ ДЕЗІНФОРМАЦІЯ В СУЧАСНІЙ ПОЛІТИЧНІЙ НАУЦІ

Таблиця А.1.

Методологічні проблеми визначення змісту поняття дезінформація

Критерій порівняння	Мізінформація (Misinformation)	Дезінформація (Disinformation)	FIMI (Foreign Information Manipulation and Interference)
Визначення	Неправдива інформація, що поширюється без злого наміру.	Неправдива інформація, створена та поширена навмисно для завдання шкоди.	Системні маніпулятивні дії іноземного актора, спрямовані на втручання в демократичні процеси.
Намір	Відсутній. Людина помиляється або вірить у фейк.	Шкідливий. Мета — дезорієнтувати, залякати або спровокувати конфлікт.	Стратегічний. Вплив на політичні рішення, вибори або безпеку іншої держави.
Правдивість	Завжди неправдива або викривлена.	Завжди неправдива або навмисно маніпулятивна.	Може використовувати правдиві факти, але подані в маніпулятивному контексті.
Хто поширює?	Звичайні користувачі (ваша тітка у Viber, блогер, що помилився).	Спецслужби, «фабрики тролів», ангажовані медіа.	Державні або афілійовані з державою іноземні структури (наприклад, РФ або КНР).
Інструментарій	Репости, особисті розмови.	Фейкові новини, дипфейки, боти.	Кібератаки, фінансування агентів впливу, координація тисяч бот-мереж, ШІ.
Приклад	Поширення застарілого прогнозу погоди як актуального.	Вигадка про «секретні біолабораторії» для виправдання агресії.	Координована кампанія під час виборів для підтримки конкретного кандидата через зламані пошти та ботів.

Джерело: складено автором на основі аналізу стратегічних документів EEAS та звітів Європейської Комісії.

Додаток Б

ПРОБЛЕМИ НОРМАТИВНО-ПРАВОВОГО ВИЗНАЧЕННЯ ДЕЗІНФОРМАЦІЇ В ЄС

Таблиця Б.1

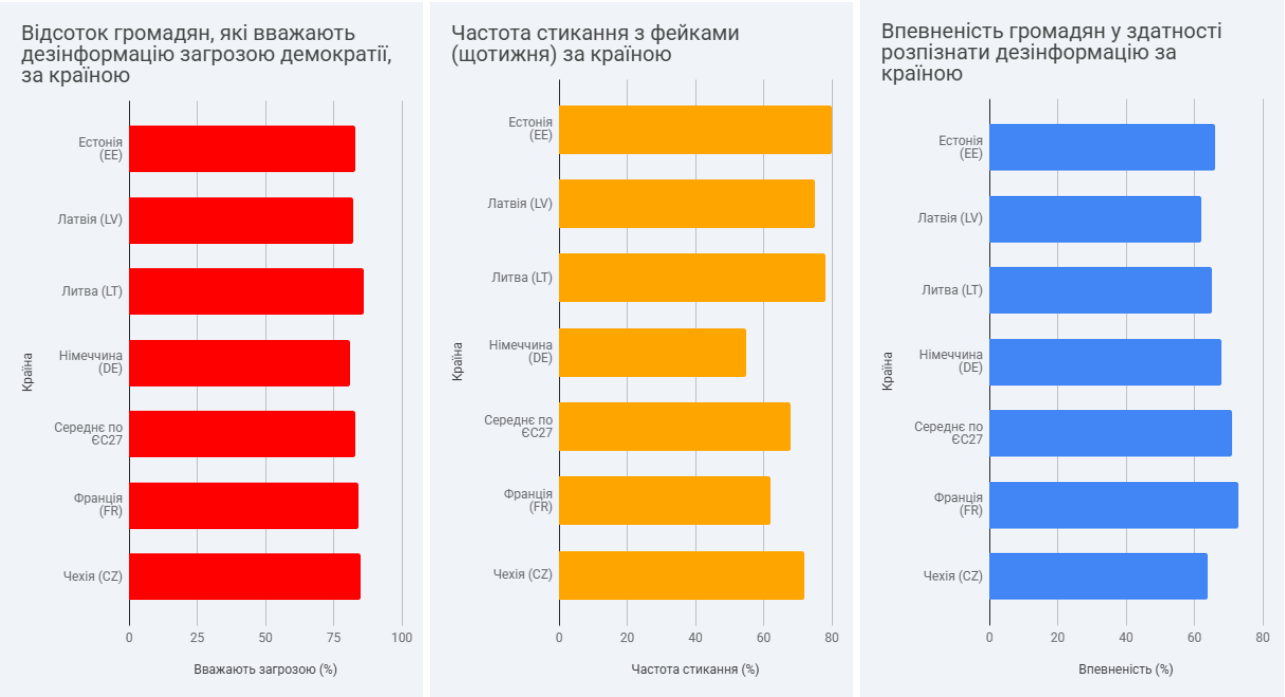
Порівняння європейських Кодексів практики протидії дезінформації 2018 р. та 2022 р.

Критерій	Кодекс 2018 р.	Посилений Кодекс, 2022 р.
Кількість підписантів	8 великих платформ та галузевих асоціацій (Google, Meta, Twitter та ін.)	Понад 40 підписантів (платформи, рекламні компанії, фактчекери, ГО, як-от Reporters Without Borders)
Кількість зобов'язань (Commitments)	5 загальних принципів	44 конкретні зобов'язання
Кількість заходів (Measures)	Близько 15 неформалізованих кроків	128 деталізованих заходів із чіткими KPI
Механізм примусу	Суто добровільний (Self-regulation)	Спільне регулювання (Co-regulation) через зв'язок із DSA
Санкції за порушення	Відсутні (репутаційні ризики)	Штрафи до 6% від глобального обороту для VLOPs)
Доступ до даних	Обмежений, на розсуд платформ	Обов'язковий доступ для перевірених дослідників (Vetted researchers)
Демонетизація	Загальні обіцянки обмежити рекламу	Конкретні заходи проти «рекламних ферм» та маніпулятивного контенту

Джерело: Складено автором за: European Commission. 2018 Code of practice on disinformation. URL: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation; European Commission. 2022 Code of practice on disinformation: Transparency Centre. 2022. URL: https://disinfocode.eu/.

Додаток В

СТІЙКІСТЬ ДО ДЕЗІНФОРМАЦІЙНИХ ВПЛИВІВ У ДЕРЖАВАХ-ЧЛЕНАХ ЄС, 2023

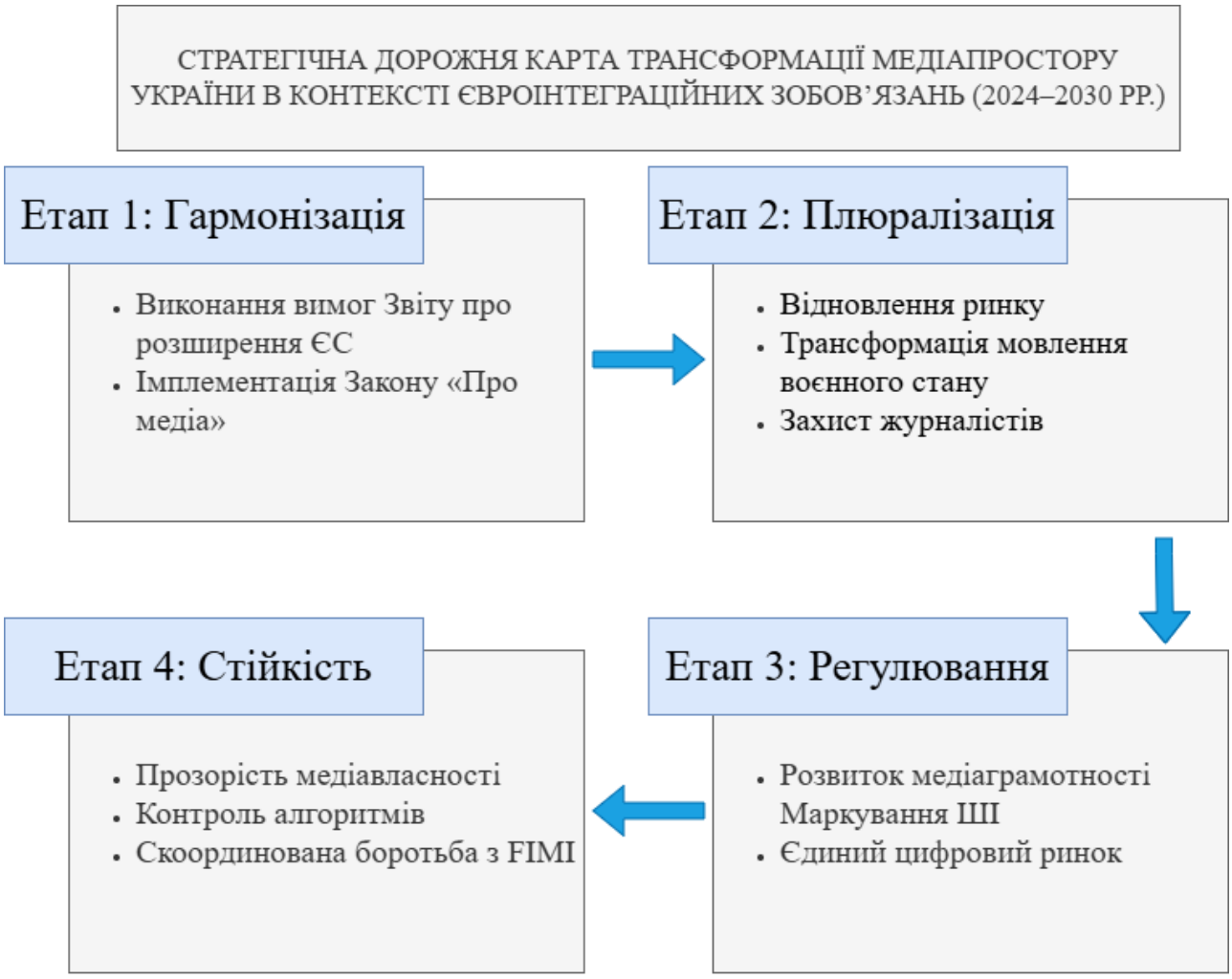


Малюнок В.1. Порівняльна характеристика показників суспільної стійкості до дезінформаційних впливів у державах-членах ЄС, 2023

Джерело: Eurobarometer Flash 522. URL: https://www.ipsos.com/sites/default/files/ct/news/documents/2023-12/Democracy_fl_522_report_en.pdf

Додаток Д

ЕТАПИ ТРАНСФОРМАЦІЇ МЕДІАПРОСТОРУ УКРАЇНИ



Малюнок Д.1. Дорожня карта трансформації медіапростору України

Джерело: Міністерство культури та стратегічних комунікацій України. Дорожня карта відновлення медіапростору та забезпечення плюралізму в післявоєнний період. Київ, 2024. https://zakon.rada.gov.ua/rada/show/v0451921-24#Text

Додаток Ж

ФУНКЦІОНУВАННЯ СИСТЕМИ ШВИДКОГО СПОВІЩЕННЯ (RAS)

Малюнок Ж.1. Алгоритм функціонування системи швидкого сповіщення (RAS) та координації з партнерами ЄС

Джерело: Rapid Alert System: strengthening coordinated and joint responses to disinformation. European External Action Service (EEAS). March 2019. URL: https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf

Додаток З

ЗМІСТ РОСІЙСЬКИХ ДЕЗІНФОРМАЦІЙНИХ КАМПАНІЙ

Таблиця 3.1

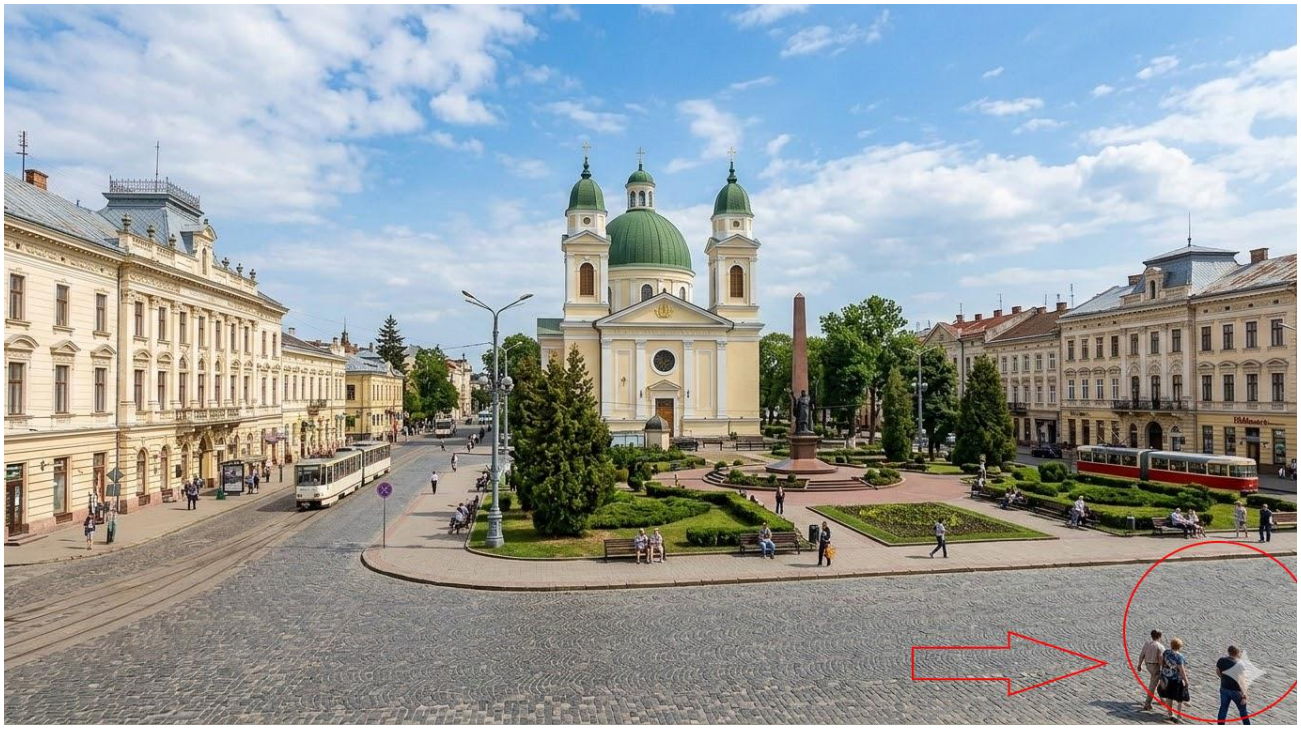
Тематична спрямованість російських дезінформаційних кампаній

Наратив	Частка в базі (%)	Цільова аудиторія	Стратегічна мета
«Нацизм в Україні»	~28%	Громадяни РФ, Україна	Дегуманізація та виправдання агресії
«Занепад Заходу»	~22%	Консервативні кола ЄС	Підрив соціальної згуртованості в ЄС
«Втрачений суверенітет»	~18%	Україна, країни Балтії, Польща	Дискредитація державності та суб'єктності
«Еліти проти народу»	~15%	Населення ЄС	Провокування протестів та політичної нестабільності
«Біолабораторії / Секретна зброя»	~10%	Глобальний Південь	Формування екзистенційного страху перед НАТО
Інші (ЛГБТ, мігранти, русофобія)	~7%	Різні сегменти	Створення «інформаційного шуму»

Джерело: EUvsDisinfo (East StratCom Task Force / EEAS). URL: https://euvsdisinfo.eu/disinformation-cases/

Додаток К

ПОЗНАЧЕННЯ ЗГЕНЕРОВАНОГО КОНТЕНТУ



Малюнок К.1. Приклад позначення ШІ контенту
(Чат Gemini, промт: «Згенеруй зображення Соборної площі в Чернівцях»

Додаток Л

ПІДПИСАНТИ ПОСИЛЕНОГО КОДЕКСУ ПРАКТИКИ ЩОДО ДЕЗІНФОРМАЦІЇ

Таблиця Л.1

Реєстр підписантів Посиленого Кодексу практики щодо дезінформації (станом на 2026 р.)

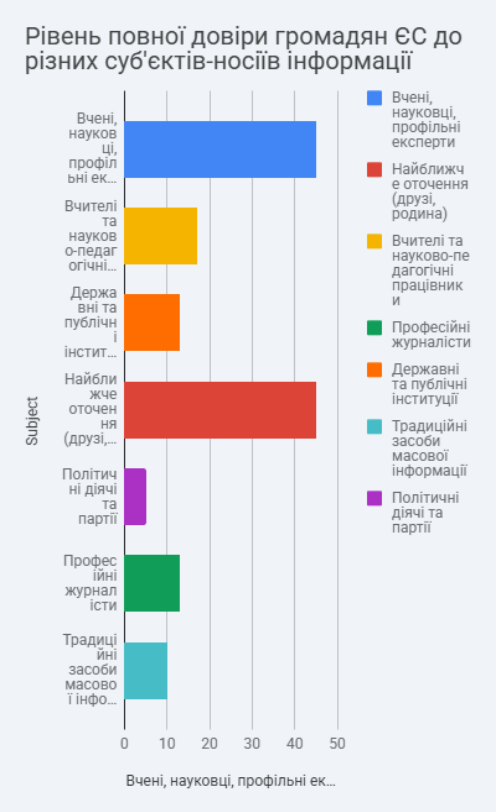
Категорія підписантів	Ключові організації та компанії	Тип діяльності	Рівень впливу	Основні зобов'язання
Глобальні технологічні платформи (VLOPs)	Google (вкл. YouTube), Meta (Facebook, Instagram), TikTok, Adobe.	Розповсюдження контенту, реклама, модерація.	Глобальний	Прозорість алгоритмів, боротьба з дезінформацією.
Спеціалізовані платформи та сервіси	Vimeo, Twitch, WhoTargetMe, Dailymotion.	Хостинг відео, стрімінг, таргетована реклама.	Регіональний/ Глобальний	Забезпечення доброчесності платформи, моніторинг контенту.
Рекламний сектор та технічні провайдери	IAB Europe, WFA (World Federation of Advertisers), DoubleVerify, Integral Ad Science.	Управління рекламними кампаніями, верифікація реклами, вимірювання.	Глобальний	Прозорість розміщення політичної реклами, запобігання шахрайству.
Організації громадянського суспільства та NGO	Reporters Without Borders (RSF), Global Disinformation Index (GDI), Lighthouse Reports.	Моніторинг, звітність, адвокація.	Глобальний	Аудит виконання Кодексу, незалежна оцінка.
Фактчекінгові та аналітичні структури	NewsGuard, Logically, Maldita.es, VoxCheck (партнерська мережа).	Верифікація інформації, аналіз дезінформації	Регіональний	Надання даних для підвищення медіаграмотності.
Дослідницькі та технічні стартапи	Factmata, Kinzen, Vubble, Teyit.	Розробка інструментів для боротьби з дезінформацією	Глобальний	Впровадження інновацій, співпраця з дослідниками.

Джерело: Transparency Centre of the Code of Practice on Disinformation. European Commission. 2026. URL: https://disinformationcode.eu/signatories

Додаток М

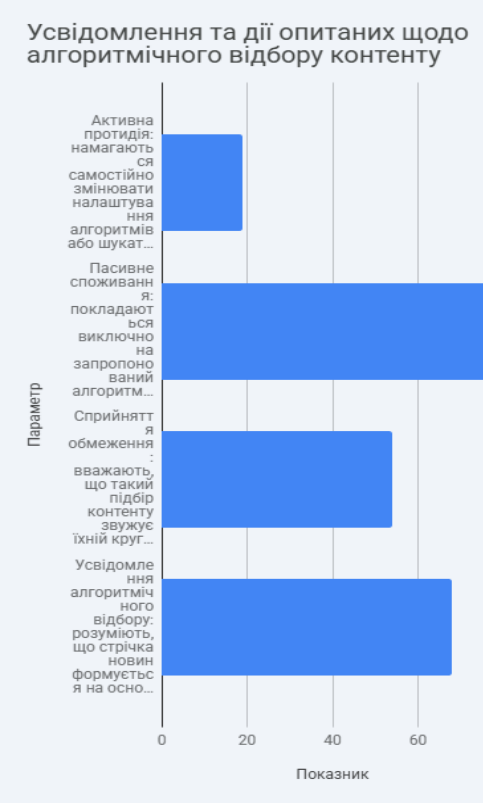
АНАЛІЗ ПОВЕДІНКОВИХ ПАТТЕРНІВ КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ ЄС ПРИ ЗІТКНЕННІ З ПІДОЗРІЛИМ КОНТЕНТОМ, 2025

Малюнок Ж.1. Методи верифікації



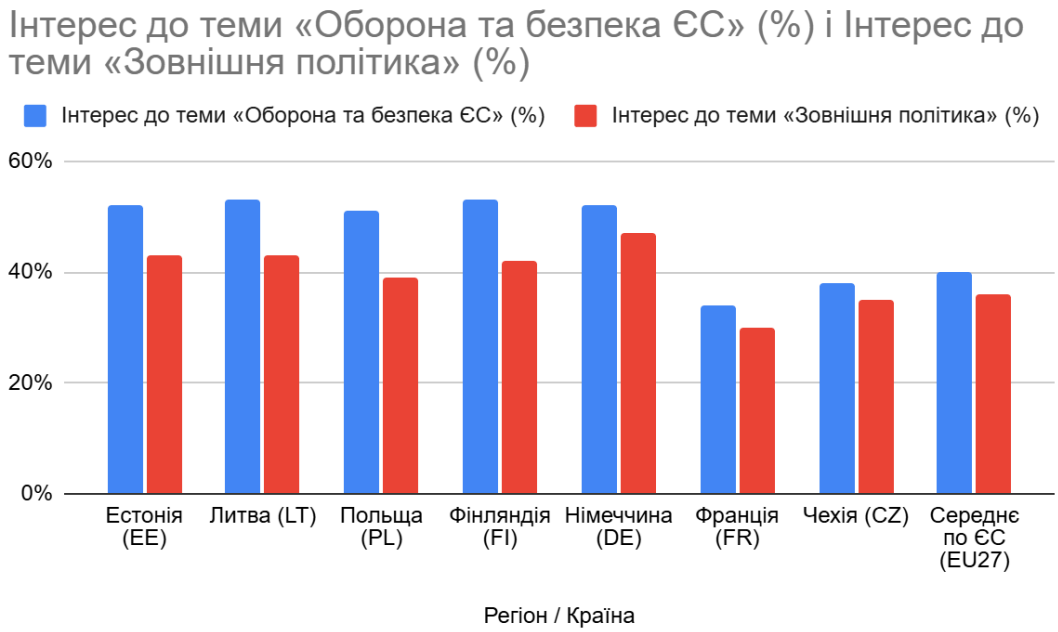
Малюнок Ж. 2. Рівень довіри до носіїв інформації

Малюнок Ж.3. Рівень впевненості у здатності верифікації



Малюнок Ж.4. Усвідомлення алгоритмів протидії

Малюнок Ж.5. Занепокоєння поширенням та впливом дезінформації та ШІ

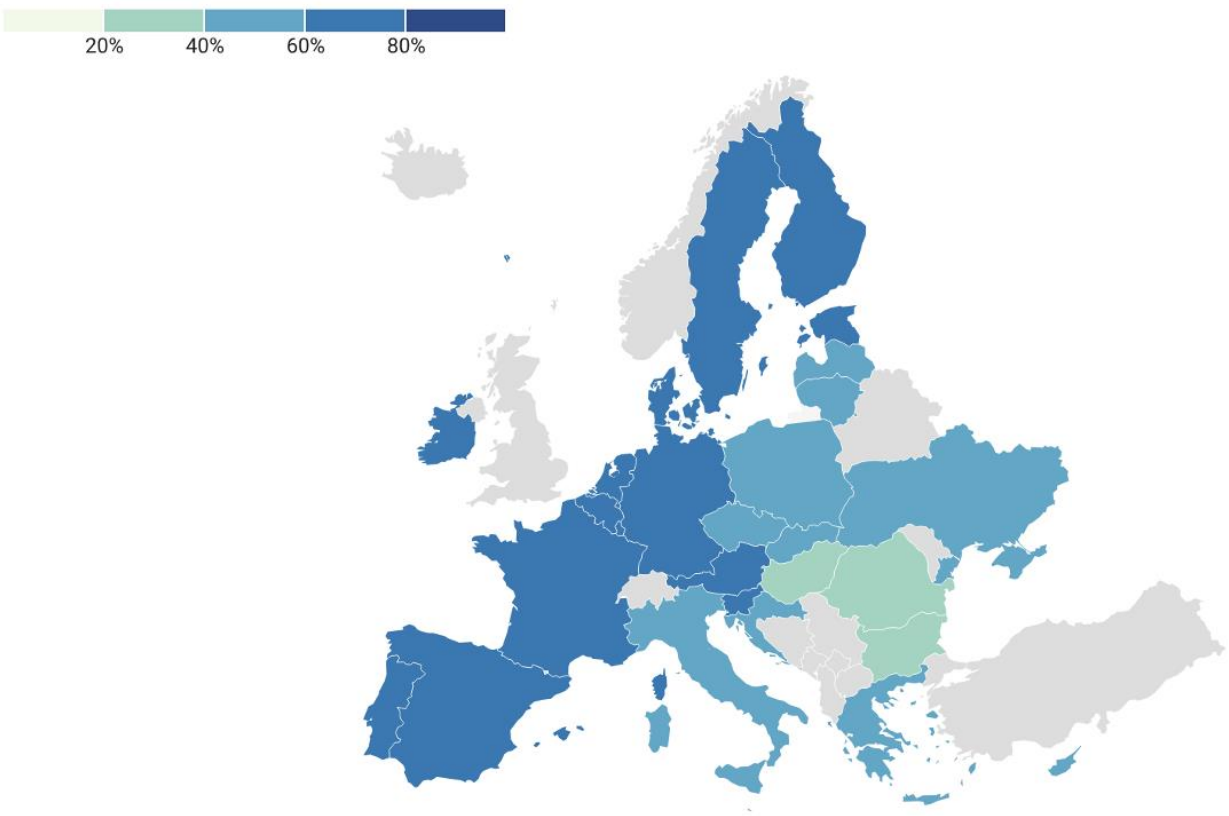


Малюнок Ж.6. Інтерес до безпекових питань серед громадян ЄС

Джерело: Flash Eurobarometer FL014EP. URL: https://data.europa.eu/data/datasets/s3592_fl014ep_eng?locale=en

Додаток Н

РЕЙТИНГ МЕДІАГРАМОТНОСТІ MEDIA LITERACY INDEX, 2026



Малюнок Н.2. Порівняльний аналіз рейтингів медіаграмотності держав-членів ЄС, 2026

Джерело: Media Literacy Index 2026. https://osis.bg/wp-content/uploads/2026/01/Media-Literacy-Index-2026.pdf

Додаток П

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці у виданнях, включених до переліку наукових фахових видань України:

4. Стьопкін А. Інституціоналізація політики протидії дезінформації в Європейському Союзі. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2022. Том 10. С. 196–208.
5. Стьопкін А. Особливості концептуалізації поняття дезінформація в сучасній політичній науці. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2024. Том 15. С. 320–336.
6. Стьопкін А. Особливості національних моделей політики протидії дезінформації в державах-членах ЄС. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2025. Вип. 4(24). С. 115–137.

Наукові праці, які засвідчують апробацію матеріалів дисертації

9. Стьопкін А. О. Європейські інструменти спротиву дезінформації. *Розвиток політичної науки: європейські практики та національні перспективи: матеріали Міжнародної науково-практичної конференції, Чернівці, 28 червня 2022 року*. Чернівці: Технодрук, 2022. С. 195–196.
10. Стьопкін А. О. Стратегічні комунікації НАТО як інструмент реалізації політики протидії дезінформації РФ. *Збірник матеріалів IV Всеукраїнської науково-практичної конференції «Політичні процеси сучасності: глобальний та регіональний виміри»*. ІІ частина. Івано-Франківськ: Прикарпатський національний університет імені Василя Стефаника, 2022. С. 377–386.
11. Стьопкін А. Перспективи формування онлайн-екосистеми як інструменту політики протидії дезінформації. *Розвиток політичної науки: європейські практики та національні перспективи: матеріали Міжнародної науково-практичної конференції, Чернівці, 14 червня 2023 року*. Чернівці : Технодрук, 2023. С. 114–117.
12. Стьопкін А. О. Особливості інтеграції інструментів формування медіакомпетентності до інформаційно-комунікаційного механізму протидії

дезінформації в умовах російсько-української війни. *Інтернет-конференція «Україна в координатах Східного партнерства: пошук геополітичних пріоритетів крізь призму національної безпеки».* Львів: Видавництво Львівської політехніки, 2023. С. 42–44.

13. Стьопкін А. О. Наближення політики протидії дезінформації України до принципів та стандартів ЄС. *Розвиток політичної науки: європейські практики та національні перспективи: матеріали Міжнародної науково-практичної конференції, Чернівці, 29 травня 2025 року*. Чернівці: Технодрук, 2025. С. 106–109.

Додаток Р

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

1. XII Міжнародна науково-практична конференція «Розвиток політичної науки: європейські практики та національні перспективи» (м. Чернівці, 28 червня 2022 року). Форма участі - очна, з публікацією тез.
2. IV Всеукраїнська науково-практична конференція «Політичні процеси сучасності: глобальний та регіональний виміри» (м. Івано-Франківськ, 27-28 жовтня 2022 року). Форма участі - дистанційна, з публікацією тез.
3. XIII Міжнародна науково-практична конференція «Розвиток політичної науки: європейські практики та національні перспективи» (м. Чернівці, 14червня 2023 року). Форма участі - очна, з публікацією тез.
4. Інтернет-конференція «Україна в координатах Східного партнерства: пошук геополітичних пріоритетів крізь призму національної безпеки» (м. Львів, 24 березня 2023 року). Форма участі - дистанційна, з публікацією тез.
5. XIV Міжнародна науково-практична конференція «Розвиток політичної науки: європейські практики та національні перспективи» (м. Чернівці, 29 травня 2025 року). Форма участі - очна, з публікацією тез.
6. Конференція Сучасні тенденції регіональної співпраці: україно-румуно-молдовський вимір (м. Чернівці 24 травня 2024 р.). Форма участі - очна, без публікації тез.
7. Міжнародна науково-практична конференція «Протидія російським інформаційно-психологічним впливам в умовах повномасштабної російсько-української війни: механізми та можливі рішення» (м. Чернівці, 11 квітня 2025 р.). Форма участі - дистанційна, без публікації тез.
8. Проєкт «EU Strategic Communications: Counteraction to Destructive Influences» (Волинський національний університет імені Лесі Українки, 2024 р., сертифікат)
9. Тренінг «Протидія ЄС зовнішньому інформаційному маніпулюванню та втручанню». Волинський національний університет імені Лесі Українки, 2025 р., сертифікат)

10. Проєкт «Політика пам’яті та гібридні загрози: інструменти РФ і вплив на європейський популізм». (Карпатський національний університет імені Василя Стефаника, з 1 січня 2026 р., участь триває).