

УДК 327:316.776.23-048.66(470)
DOI <https://doi.org/10.32782/2663-6170/2026.46.17>

КОМПЛЕКС ІНСТРУМЕНТІВ ЄС У СФЕРІ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ: ЗАГАЛЬНОЄВРОПЕЙСЬКИЙ ТА НАЦІОНАЛЬНИЙ РІВНІ

THE EU ANTI-DISINFORMATION TOOLKIT: PAN-EUROPEAN AND NATIONAL LEVELS

Білоусов М.В.,

orcid.org/0000-0002-1008-9649

*аспірант кафедри міжнародних відносин та зовнішньої політики
Чорноморського національного університету імені Петра Могили*

Зважаючи на те, що дезінформація не має конкретного визначення і є багатограним явищем, яке виходить за рамки фейкових новин і яке неможливо ігнорувати як виклик демократичним цінностям ЄС, автор зацікавив, що боротьба з дезінформацією в ЄС координується на наднаціональному (загальноєвропейському) та національному рівнях. На першому етапі дослідження було проаналізовано нормативно-правові акти, інституційні механізми, стратегічні комунікації, технологічні та операційні, освітні і соціальні засоби, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні. На другому – визначено, що хоча ЄС встановлює загальні стандарти політики у сфері боротьби з дезінформацією, забезпечення виконання та локалізовані заходи реагування здійснюються на рівні держав-членів ЄС. Автором конкретизовано, які саме законодавчі ініціативи, національні інституції, національні стратегії та механізми співпраці з громадським суспільством, входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на національному рівні. Головні європейські інституції (Європейська служба зовнішніх дій, Аналітичний центр ЄС із питань протидії дезінформації, Європейська обсерваторія цифрових медіа) та національні комунікаційні служби Франції (VIGINUM), Німеччини (BSI), Фінляндії (KAVI) і Чехії (PSSI, CTHH, BIS, NUKIB) тісно співпрацюють з метою виявлення та нейтралізації інформаційних загроз.

Такі країни-члени ЄС, як Франція, Німеччина і Чехія, використовують різні підходи у сфері боротьби з дезінформацією: від жорсткого законодавчого регулювання соцмереж до спеціалізованого моніторингу гібридних загроз. Було продемонстровано чому досвід Фінляндії у сфері боротьби з дезінформацією, який базується на концепції «загальної безпеки», визнано одним із найефективніших у світі: країна досягла такого рівня у цій сфері завдяки тому, що об'єднала зусилля уряду, освіти та суспільства, зробивши ставку на проактивність, а не на цензуру. Головний пріоритет Фінляндії – це розвиток критичного мислення у населення починаючи з дитячого садка та школи.

Ключові слова: дезінформація, комплекс інструментів, загальноєвропейський рівень, національний рівень, Європейський Союз, РФ, Фінляндія, Франція, Німеччина, Чехія.

Given that disinformation has no specific definition and is a multifaceted phenomenon that goes beyond fake news and cannot be ignored as a challenge to the EU's democratic values, the author emphasized that the fight against disinformation in the EU is coordinated at the supranational (pan-European) and national levels. The first stage of the study analysed the legal and regulatory framework, institutional mechanisms, strategic communications, technological and operational, educational and social tools that comprise the EU's set of instruments for combating disinformation at the pan-European level. The second stipulates that while the EU sets common policy standards in the area of combating disinformation, enforcement and localised responses are carried out at the level of EU Member States. The author specifies which legislative initiatives, national institutions, national strategies, and mechanisms for cooperation with society are included in the EU's set of instruments for combating disinformation at the national level. The main European institutions (the European External Action Service, the EU DisinfoLab, the European Digital Media Observatory) and the national communications services of France (VIGINUM), Germany (BSI), Finland (KAVI) and the Czech Republic (PSSI, CTHH, BIS) threats.

EU member states such as France, Germany, and the Czech Republic are using different approaches to combating disinformation, ranging from strict legislative regulation of social media to specialized monitoring of hybrid threats. It was demonstrated why Finland's experience in combating disinformation, based on the concept of "common security", is recognized as one of the most effective in the world: the country has achieved this level of effectiveness by combining the efforts of government, education, and society, emphasizing proactivity over censorship. Finland's top priority is developing critical thinking in its population, starting in kindergarten and school.

Key words: disinformation, set of tools, Pan-European level, national level, European Union, Russian Federation, Finland, France, Germany, Czech Republic.

Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0



Постановка проблеми. У наш час, наслідки дії дезінформації на суспільство дедалі більше привертають увагу представників політичних та юридичних кіл Європейського Союзу (далі – ЄС). Однак, ЄС почав зосереджуватися на потребі боротьби з дезінформацією тільки з початком російської пропаганди щодо анексії Криму. Європейська Рада вперше згадала про дезінформацію як джерело занепокоєння у своїх висновках від березня 2015 р., наголосивши на «необхідності кинути виклик постійним дезінформаційним кампаніям Росії» та закликавши Високого представника «підготувати до червня план дій щодо стратегічної комунікації» і створити «комунікаційну команду» [29]. Після цього в ЄС почала зростати стурбованість щодо дезінформаційних кампаній. Так, у Повідомленні Європейської Комісії (далі – ЄК) від 2018 р. було вказано, що: «Дезінформація – це перевірено неправдива або оманлива інформація, яка створюється, оприлюднюється та поширюється з метою отримання економічної вигоди або навмисного обману громадянськості та може завдати шкоди останній» [26]. Тож в інституціях ЄС прийшли до висновку, що дезінформація становить реальну загрозу належному функціонуванню національних та загальноєвропейських демократичних систем і підриває довіру громадян до інституцій та демократичних процедур. А також, що дезінформація заважає громадянам отримувати справжні знання, тим самим перешкоджаючи їхній здатності приймати обґрунтовані рішення.

Варто зазначити, що комплекс інструментів ЄС у сфері боротьби з дезінформацією є багаторівневим і поєднує загальноєвропейські механізми з національними політиками держав-членів ЄС. Інструментарій ЄС у вищезазначеному напрямку працює на основі загальноєвропейського підходу, інтегруючи юридично обов'язкові правила, галузеві кодекси та заходи з розбудови потенціалу. Інструментарій встановлює бар'єри для онлайн-платформ, водночас надаючи національним органам держав-членів ЄС та незалежним органам, які здійснюють перевірку фактів можливості виявляти і протидіяти іноземному втручанням та внутрішній дезінформації. Комплекс інструментів ЄС у сфері боротьби з дезінформацією охоплює як спеціалізовані аналітичні підрозділи, так і системні законодавчі акти, які зобов'язують цифрові платформи керувати інформаційними ризиками.

У свою чергу, боротьба з дезінформацією на внутрішньому рівні держав-членів ЄС спирається на єдину загальноєвропейську базу (зокрема, Акт про цифрові послуги та Кодекс практики проти дезінформації), але реалізується через національні стратегії кожної країни-учасниці ЄС. Не зважаючи на те, що Брюссель задає загальний правовий вектор (наприклад, ухвалюючи директиви для уні-

фікації покарань), профілактика та нейтралізація загроз залишається в зоні відповідальності внутрішніх інституцій кожного окремого національного уряду.

Аналіз останніх досліджень і публікацій. Під час написання статті автор використовував напрацювання вітчизняних та європейських науковців. Серед українських дослідників, найбільшу увагу вивченню інструментарію ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні приділяли Н. П. Карпчук [4], Г. Рожкова [8], О. А. Самчинська [9], А. Стюпкін [10], В. І. Сухоруков [11], В. Т. Хакімова [15], Р. Черниш [16]. Вищезазначені науковці зосереджувалися на вивченні нормативно-правового аспекту інструментарію ЄС у сфері боротьби з дезінформацією. Науковці О. В. Федунь та С. А. Милян [12] здійснюють комплексний аналіз трансформації підходів ЄС до протидії дезінформації (2014-2026 рр.) і приходять до висновку, що усвідомлення реальних наслідків загрози, яку становить іноземна маніпуляція інформацією, зумовило еволюцію інформаційної політики ЄС від ліберальної моделі забезпечення свободи слова до системної протидії явищу дезінформації з використанням інституційних, комунікаційних та регуляторних механізмів. Н. Матвійчук, Л. Корнійчук [5], А. Зіненко, І. Свобода, Т. Дерещук, Н. Шевченко, М. Шаповаленко [44] вивчали інструментарій ЄС у сфері боротьби з дезінформацією на національному рівні. Європейські дослідники J. Bayer [21], K. Bleyer-Simon, E. Brogi, I. Nenadić, T. Nesovic [22] вивчали досвід Німеччини у сфері боротьби з дезінформацією. А. К. Cianciara [24], N. Hénin [33], M. R. Sauvé, A. Coutant [40] зосередили увагу на французькій стратегії боротьби з цим явищем; D. Saari, P. Moilanen, M. Hautala [39] розкрили процес боротьби з дезінформацією у Фінляндії. L. Cabada [23], T. Kolomazník [34] розкривають підхід Чеської Республіки до побудови стійкого суспільства проти дезінформаційних наративів.

Виділення не вирішених раніше частин загальної проблеми. Актуальність обраної проблематики посилюється недостатньою розробкою тематики та невисоким ступенем висвітлення у вітчизняній науковій школі і потребує детального аналізу. Слід зазначити, що поза увагою науковців та практиків залишається низка критичних аспектів, а саме: 1) недостатньо вивчено механізми подолання розриву між загальноєвропейськими стратегіями та їхньою різною за ефективністю реалізацією на рівні окремих держав-членів ЄС; 2) потребує детальнішого аналізу баланс між жорстким регулюванням контенту (згідно з Digital Services Act, далі – DSA) та захистом фундаментальних прав громадян на свободу слова; 3) проблема адаптації європейського законодавства до стрімкого розвитку генеративного штучного

інтелекту (далі – ШІ) не є повністю розкритою; 4) порівняння досвіду окремих країн ЄС (наприклад, досвіду Франції, Німеччини та Фінляндії) дозволить виявити найкращі практики адаптації загальноєвропейських директив до національного законодавства.

Формулювання цілей статті (постановка завдання). Метою статті є здійснення порівняльного аналізу комплексу інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському та національному рівнях.

Виклад основного матеріалу дослідження. Варто зазначити, що переломним моментом у трансформації політики інформаційної безпеки ЄС стала повномасштабна війна РФ проти України у 2022 р., яка супроводжувалася посиленням дезінформаційних операцій агресора щодо навмисного втручання в інформаційний простір держав-учасниць ЄС. У відповідь на цю загрозу ЄС посилив заходи протидії іноземним інформаційним маніпуляціям і включив ці питання до безпекової політики [12, с. 190].

Інструментарій ЄС у сфері боротьби з дезінформацією ґрунтується на триєдиному підході: законодавство, саморегуляція бізнесу та підвищення стійкості суспільства [9, с. 7]. Перш за все, автор статті вважає за доцільне проаналізувати які саме нормативно-правові акти, інституційні механізми, стратегічні комунікації, технологічні та операційні, освітні і соціальні засоби, входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні.

Протягом останніх кількох років ЄС ухвалив низку відповідних законодавчих актів у цій сфері. Слід виділити такі **нормативно-правові акти**, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні:

Європейський план дій проти дезінформації (2018 р.), який є базовою стратегією координації політики держав-членів ЄС у сфері боротьби з дезінформацією [20].

Юридично обов'язкові правила, зокрема, Акти цифрового регулювання, які вимагають від великих ІТ-платформ оцінювати та зменшувати ризики для громадських процесів, безпеки й свободи слова – Закон про цифрові послуги (DSA) [27], що встановлює обов'язки платформ щодо модерації контенту, прозорості та боротьби з незаконною інформацією. У випадку недотримання DSA порушникам загрожують багатомільйонні штрафи. Європейський акт про свободу медіа (далі – EMFA) [38], який захищає незалежні ЗМІ та журналістів від втручання держави та створює Європейську раду з медіа-послуг для координації національних регуляторів ЗМІ проти шахрайських медіа-сервісів поза ЄС. Цей Закон, прийнятий у квітні 2024 р., поетапно набув чинності у 2025 р.

і діє як єдиний стандарт для медійного простору.

Галузеві кодекси, зокрема, Кодекс практики щодо дезінформації (Code of Practice on Disinformation) [41], який включає добровільні зобов'язання великих платформ (Google, Meta, TikTok тощо) щодо видалення фейків; маркування контенту маніпулятивного характеру; обмеження монетизації дезінформації. У 2018 р. було узгоджено перший Кодекс практики щодо дезінформації, який об'єднав онлайн-платформи та технологічні компанії, що зобов'язалися вжити низку заходів для боротьби з дезінформацією, таких як переривання реклами, демонетизація постачальників дезінформації та зменшення її можливості пошуку. Потім, у 2022 р., ЄС сприяв Посиленому кодексу практики щодо дезінформації [6], який залучив більше учасників, включаючи широке коло зацікавлених сторін з громадянського суспільства, та передбачав більш детальні заходи і набір показників для оцінки рівнів впровадження [25].

Галузеві кодекси є добровільними зобов'язаннями для медіа та технологічних компаній щодо позбавлення фінансової вигоди розповсюджувачів фейків, розкриття політичної реклами та розширення можливостей фактчекерів [11, с. 363].

Європейський план дій щодо демократії – це стратегічний документ, прийнятий ЄК 3 грудня 2020 р., що комплексно захищає виборчі процеси від маніпуляцій, посилює захист журналістів та встановлює суворі правила прозорості політичної реклами [30].

Таким чином, Європейські акти та плани дій не запроваджують пряму цензуру, а зобов'язують цифрові платформи боротися з маніпуляціями. Вищезазначені документи вводять ключові правила для європейського інформаційного середовища, а саме: 1) демонетизація дезінформації; 2) прозорість політичної реклами; 3) боротьба з маніпуляціями; 4) захист виборів та дають можливість створити європейський «Щит демократії», покликаний захистити інформаційний простір як самого ЄС, так і його країн-партнерів (включаючи Україну) від маніпуляцій. Ці нормативно-правові акти об'єднують зусилля держав, громадянського суспільства та ІТ-гігантів для захисту демократичних інститутів.

Інституційні механізми, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні включають спеціалізовані інституційні підрозділи та мережі, зокрема:

Європейська служба зовнішніх дій (далі – ЄСЗД) здійснює координацію зовнішньої інформаційної політики ЄС. У складі ЄСЗД діють підрозділи, які аналізують та виявляють інформаційні маніпуляції.

Оперативна робоча група зі стратегічних комунікацій (East StratCom Task Force) працює

у складі ЄСЗД і займається викриттям та аналізом проросійських дезінформаційних кампаній, веде платформу EUvsDisinfo а також координує стратегічні комунікації ЄС [15, с. 157-158].

Система швидкого оповіщення (Rapid Alert System, RAS) є спеціальним механізмом, створеним для швидкого обміну даними між інституціями ЄС та державами-членами про загрози іноземного втручання та маніпуляції інформацією в режимі реального часу. RAS є важливим елементом загального підходу ЄС до боротьби з дезінформацією та одним із чотирьох стовпів Плану дій проти дезінформації, схваленого Європейською Радою у грудні 2018 р. [31].

Аналітичний центр ЄС із питань протидії дезінформації забезпечує збір даних та глибоку оцінку загроз. EU DisinfoLab – провідна незалежна неурядова організація, що спеціалізується на дослідженні, картографуванні та викритті складних дезінформаційних кампаній, спрямованих проти ЄС [28].

Група європейських регуляторів для аудіовізуальних медіапослуг (ERGA), яка об'єднує національних регуляторів для моніторингу дотримання стандартів медіаринку та протидії шкідливому контенту. Група сприяє гармонізації європейського медіапростору та імплементації Директиви про аудіовізуальні медіапослуги (AVMSD) [3].

Європейська обсерваторія цифрових медіа (EDMO) є незалежним європейським хабом, який об'єднує фактчекерів, науковців та експертів для боротьби з дезінформацією в ЄС та сусідніх державах. Зокрема, у 2025 р. було створено спеціальний регіональний хаб з метою підтримки України та Молдови, який покликаний посилити стійкість суспільства до ворожих інформаційних атак [32]. Головними напрямками діяльності EDMO є: 1) боротьба з дезінформацією: аналіз та відстеження фейків, у першу чергу тих, які пов'язані з російською гібридною війною та європейськими виборами; 2) медіаграмотність, зокрема, розробка настанов та рекомендацій для підвищення критичного мислення жителів Європи; 3) підтримка незалежної спільноти дослідників, які вивчають екосистему цифрових медіа [10, с. 200].

Також, ЄК планує створити *Європейський центр демократичної стійкості*, який буде включати органи для протидії маніпуляціям інформацією та дезінформації з боку РФ та інших авторитарних режимів. Це ініціатива ЄК, що є ключовою складовою безпекового пакету «Щит демократії». Метою та функціями майбутнього Центру є: 1) координація захисту від різноманітних гібридних атак та втручань у демократичні процеси ЄС; 2) створення єдиної платформи швидкого реагування, яка дозволить державам-членам ефективніше виявляти загрози та ділитися методологією їх нейтралізації [3]. У документі «Щит

демократії» у листопаді 2025 р. ЄК підтвердила своє зобов'язання щодо забезпечення дотримання законодавства ЄС проти основних платформ, але не оголосила про жодні нові конкретні ініціативи. Тож, залишається невідомим, чи буде це зобов'язання підтверджено на практиці, чи залишиться лише риторичним.

Стратегічні комунікації, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні представлені *проектом EUvsDisinfo*. Це публічний флагманський інструмент від ЄСЗД, який веде базу даних викритих дезінформаційних матеріалів та публікує аналітику щодо тактик і наративів прокремлівських медіа [1]. EUvsDisinfo виступає головним проектом ЄС, який створений для виявлення, аналізу та реагування на дезінформацію, що спрямована на держави-члени ЄС та країни Східного партнерства. На EUvsDisinfo покладені такі функції: 1) *моніторинг*: аналізує інформаційний простір та збирає приклади дезінформаційних кампаній (база даних налічує десятки тисяч кейсів); 2) *викриття*: публікує статті, звіти та аналітику, які розвінчують фейки та маніпуляції (зокрема, щодо війни РФ проти України); 3) *підвищення обізнаності*: допомагає медіа, журналістам та суспільству розпізнавати пропаганду та розвивати критичне мислення. Кампанії стратегічних комунікацій ЄС є скоординованими інформаційними, дипломатичними та безпековими ініціативами, які спрямовані на роз'яснення політик ЄС, зміцнення суспільної стійкості та системну протидію дезінформації. Основними напрямками таких кампаній є: протидія пропаганді, просування наративів ЄС, розвиток кризових комунікацій (наприклад, під час COVID-19 і війни РФ проти України) [4, с. 56].

Технологічні та операційні засоби, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні включають:

Моніторинг інформаційного простору (III, Big Data), який передбачає автоматизований аналіз великих масивів даних у реальному часі для виявлення підозрілих паттернів, скоординованих кампаній маніпуляцій та фейкових наративів (наприклад, через європейські дослідницькі хаби).

Системи раннього попередження (Rapid Alert System), які виступають оперативним механізмом, що дозволяє інституціям ЄС та державам-членам миттєво обмінюватися даними про нові загрози, інциденти втручання та атаки іноземних акторів.

Співпраця з Big Tech, а саме виявлення ботів, фейкових акаунтів та маркування III-контенту.

Освітні та соціальні засоби, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні включають: програми медіаграмотності (ЄС

активно фінансує ініціативи, які навчають громадян критично мислити, розпізнавати маніпуляції та перевіряти джерела інформації, наприклад, через щорічний Європейський тиждень медіаграмотності); підтримку незалежних ЗМІ (захист свободи слова та фінансова підтримка якісної журналістики розглядаються як головна протипаганда); фінансування досліджень і фактчекінгу (через EDMO, яка об'єднує фактчекерів, науковців та медіаекспертів для аналізу дезінформаційних трендів); формування «суспільної стійкості» до дезінформації (довгострокова стратегія, спрямована на те, щоб зробити суспільство менш вразливим до інформаційних операцій завдяки прозорості алгоритмів соцмереж та співпраці між урядами й громадським суспільством) [8].

Хоча ЄС встановлює загальні стандарти політики у сфері боротьби з дезінформацією, забезпечення виконання та локалізовані заходи реагування здійснюються на рівні держав-членів ЄС. Автор статті вважає за доцільне проаналізувати які саме законодавчі ініціативи, національні інституції, національні стратегії та механізми співпраці з громадським суспільством, входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на національному рівні.

Слід відмітити, що Фінляндія, Франція, Німеччина та Чехія найчастіше відзначаються як лідери у сфері медіаграмотності та стійкості до дезінформації європейськими та міжнародними інституціями, зокрема у щорічному дослідженні Media Literacy Index [43] від Інституту відкритого суспільства (Open Society Institute – Sofia). Ці країни регулярно входять до відповідних рейтингів за оцінками свободи медіа, освіти та довіри в суспільстві. Аналітичні центри (наприклад, European Policies Initiative) та європейські інституції використовують дані провідних організацій (наприклад, Freedom House) для оцінки того, наскільки ефективно суспільства провідних європейських країн здатні розпізнавати неправдиву інформацію та протидіяти їй.

На рівні європейських країн спостерігається **адаптація національного законодавства** до норм ЄС (DSA, GDPR тощо). DSA – це головний інструмент на рівні ЄС, який діє для всіх країн-членів. Незалежні регуляторні органи (Координатори цифрових послуг (DSC)), створені в кожній країні ЄС відповідно до Угоди про цифрові послуги для моніторингу дотримання платформою вимог, розгляду скарг користувачів та застосування штрафів у національному масштабі.

ЄС не має єдиного закону про криміналізацію дезінформації, розмежовуючи незаконний (тероризм, мова ворожнечі) та шкідливий контент (фейки). Протидія покладається переважно на DSA, який зобов'язує платформи стримувати ризики та Кодекс практики щодо дезінформації.

Проте низка країн ЄС впроваджує кримінальне покарання за поширення свідомо неправдивої інформації. Для боротьби з дезінформаційними викликами однією з перших національних політик, сформульованих у Німеччині у 2017 р., став так званий Закон про захист прав у мережах (NetzDG, також відомий як Закон про Facebook). Закон вимагав від постачальників соціальних мереж проактивно видаляти певні види проблемного контенту на основі положень кримінального кодексу. Ця вимога на ранньому етапі критикувалася громадянським суспільством за можливу шкоду свободі слова та свободі преси [22, с. 18].

У Франції та Німеччині кримінальне законодавство переважно фокусується на суміжних злочинах: розпалюванні ворожнечі, наклепі, маніпуляціях виборами або підбурюванні до вчинення злочинів за допомогою мережі Інтернет [16, с. 125].

Франція ухвалила спеціальний закон проти маніпуляцій інформацією під час виборів («Антифейковий» закон), який дозволяє суддям у прискореному порядку вимагати негайного видалення неправдивих фактів, які можуть вплинути на результати голосування [17]. Закон про мережеву правозахисну діяльність у Німеччині є одним із найсуворіших законів у Європі, який зобов'язує соціальні мережі швидко реагувати на скарги. Платформи повинні видаляти або блокувати відверто незаконний контент, розпалювання ворожнечі або фейки в термін від 24 годин до 7 днів [18].

Уряди провідних європейських країн, таких як Німеччина та Франція, доповнюють загальноєвропейські закони власними національними ініціативами для посилення стійкості інформаційного простору та підвищення медіаграмотності серед населення. Через постійні інформаційні атаки, обидві країни планують єдину систему раннього попередження для протидії маніпуляціям та пропаганді (зокрема, російським мережам) [22, с. 32].

Національні інституції, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією включають:

Національні регуляторні органи (НРО), до яких залучені місцеві органи з питань ЗМІ та мовлення, що співпрацюють з Європейською радою з медіапослуг для перегляду, моніторингу та забезпечення виконання правил проти державного або незаконного мовлення. Наприклад, Arcot у Франції створена шляхом злиття CSA та Hadopi, гарантує свободу комунікації, контролює плюралізм новин та координує свої дії з європейськими регуляторами для модерації проблемного контенту в Інтернеті, контролює дотримання стандартів у телерадіомовленні та протидіє мові ворожнечі [7].

Національні мережі перевірки фактів включають незалежні організації з перевірки фактів, що специфічні для кожної країни, часто фінансуються громадськими мовниками або дослідницькими

грантами, відповідають за швидке спростування місцевими мовами під час виборів та криз.

Національні цільові групи з надзвичайних ситуацій/готовності. Багато держав-членів ЄС співпрацюють із Системою швидкого оповіщення ЄСЗД, обмінюючись розвідувальними даними про активні кампанії з маніпуляції інформацією, спрямовані на їхні відповідні уряди та населення.

Специфіка викликів, що виникають через дезінформацію, має наслідки для захисту цінностей демократії. Це вимагає врахування поведінки не лише держав-членів ЄС, а й приватних суб'єктів.

Спеціалізовані урядові органи країн-учасниць ЄС відіграють важливу роль у захисті демократичних інститутів від іноземних інформаційних маніпуляцій. Вони роблять акцент на виявленні скоординованих кампаній впливу, фейкових мереж та ботоферм, залишаючи оцінку контенту та його спростування суспільству. Наприклад, у Франції у 2021 р. була створена VIGINUM – служба пильності та захисту від іноземного цифрового втручання, входить до Генерального секретаріату з питань оборони та національної безпеки. Так, VIGINUM успішно викрило масштабну російську мережу дезінформації під назвою Portal Kombat [24].

Також ЄС має комплексну багаторівневу екосистему кібербезпеки та інформаційної безпеки, яка координується на рівні загальноєвропейських агенцій та реалізується національними центрами кожної країни-члена згідно з єдиними стандартами (Директива NIS2) [42]. Мережа CSIRT країн ЄС створена директивою NIS, об'єднує національні групи реагування на комп'ютерні надзвичайні події (CSIRT/CERT) кожної країни-члена та CERT-EU (Команда реагування на інциденти для інституцій та агенцій ЄС), які обмінюються даними про загрози в реальному часі та координують дії під час кризових ситуацій. У кожній країні ЄС функціонують власні національні центри (NCC) та урядові команди реагування. Провідні з них розташовані у Німеччині (BSI – Федеральне відомство з інформаційної безпеки) та CERT-Bund; у Франції (ANSSI – Національне агентство з безпеки інформаційних систем) та CERT-FR [35].

На рівні окремих держав діють як урядові підрозділи стратегічних комунікацій, так і незалежні медіарегулятори, які борються з дезінформацією у традиційних та цифрових медіа. Франція та Німеччина є одними з лідерів в ЄС у протидії гібридним інформаційним загрозам. Міністерства оборони та урядові пресслужби цих країн мають окремі підрозділи, які займаються перевіркою фактів та координацією державних комунікацій. У Франції Генеральний секретаріат з оборони та національної безпеки (SGDSN) координує міжвідомчу політику, а у Німеччині координація здійснюється через Федеральне міністерство вну-

трішніх справ (BMI) та Федеральне відомство з охорони конституції (BfV), які виявляють та інформують громадськість про дезінформаційні атаки [21].

Національні стратегії, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією включають довгострокові стратегії протидії дезінформації. У Франції створюють міжвідомчі робочі групи за участю міністерств юстиції, оборони, закордонних справ та національних медіарегуляторів для розробки багаторівневих національних стратегій. У Німеччині через потужні інформаційні агентства акцентують увагу на підтримці якісної журналістики, оскільки випуск перевірених фактів вважається головним бар'єром для розповсюдження штучно згенерованого інформаційного шуму та діпфейків [44, с. 150-151].

Слід зазначити, що офіційна Національна стратегія Франції з боротьби проти маніпуляцій інформацією іноземного походження на 2026-2030 рр. [36] була опублікована Генеральним секретаріатом з оборони та національної безпеки Франції і фіксує перехід Парижа від тимчасового реагування на окремі фейки до побудови постійної системної архітектури безпеки та превентивного стримування в інформаційній сфері.

Необхідність прийняття стратегії зумовлена тим, що Франція стала головною мішенню російських дезінформаційних кампаній в Європі (після України) [33, с. 4-5]. Документ містить 15 оперативних завдань, які згруповані за 4 фундаментальними напрямками: 1) стійкість суспільства – мобілізація громадянського суспільства, науковців та медіа. Франція прагне підвищити критичне мислення громадян та створити стійкість демократичних дебатів до зовнішнього втручання; 2) відповідальність цифрових платформ та ШІ – взаємодія з IT-гігантами та розробниками генеративного ШІ. Франція визнає, що боротьба неможлива без зміни алгоритмічної та економічної архітектури соцмереж, які стимулюють швидке поширення контенту, що апелює до емоцій користувачів; 3) національний оперативний потенціал – розвиток спроможностей державних органів щодо раннього виявлення, технічного аналізу, точної атрибуції (встановлення автора атаки) та швидкої протидії цифровому втручання; 4) спільний простір знань із партнерами – консолідація зусиль на рівні ЄС, НАТО та країн G7 для захисту вільного, відкритого та безпечного інформаційного простору [40, с. 111-112].

Офіційні структури Франції, зокрема, агентство з моніторингу іноземного цифрового втручання VIGINUM, виділяють ключові виклики до 2030 р.. У першу чергу, це російські гібридні операції. Стратегія прямо визнає РФ головним джерелом загрози, яка просуває свій імперіалістичний і націоналістичний наратив, намагаючись роз-

колоти ЄС, підірвати підтримку України та дискредитувати уряд Франції. До 2030 р. ШП-контент (тексти, аудіо, відео) стане повсякденною банальністю. Це знижує довіру до будь-яких цифрових доказів. Франція планує впроваджувати технології цифрового маркування та водяних знаків для верифікації автентичних матеріалів. Третьою загрозою є втручання у вибори. Саме тому важливим є захист демократичних процесів від масової купівлі ботоферм і фальшивих акаунтів іноземними державами під час виборчих кампаній [14].

Також варто зазначити, що Фінляндія є світовим лідером у боротьбі з дезінформацією завдяки інтеграції медіаграмотності та обов'язкової шкільної програми, починаючи з дошкільної освіти. Системний підхід Фінляндії базується на розвитку критичного мислення, фактчекінгу та міжвідомчій співпраці, що дозволяє населенню ефективно розпізнавати маніпуляції та пропаганду.

Системний підхід Фінляндії базується на загальнонаціональному розумінні, що стійкість до дезінформації є питанням національної безпеки. Цей досвід визнано одним із найефективніших в ЄС та запозичується іншими країнами. Основними елементами успішної фінської моделі є: 1) наскрізна шкільна програма – критичне мислення та медіаграмотність не викладаються як окремий предмет, а інтегруються в усі дисципліни; 2) державна стратегія Фінляндії, яка передбачає координацію дій між урядом, ЗМІ, неурядовими організаціями (далі – НУО) та освітніми установами для підвищення стійкості суспільства до інформаційних загроз; 3) регулярна підготовка педагогів, які отримують інструменти для пояснення учням методів ведення інформаційних війн; 4) програми з медіаграмотності доступні не лише для молоді, а й для дорослих, включаючи курси для людей літнього віку; 5) співпраця з фактчекерами – державна підтримка незалежних журналістських ініціатив, спрямованих на викриття фейків у режимі реального часу [39].

Варто зазначити, що фіни мають високий рівень довіри до ЗМІ та державних інституцій, що ускладнює поширення дезінформації всередині країни. Адже, суспільство заохочує культуру перевірки інформації перед її поширенням. Також, протягом останніх років спостерігається посилення законодавства через підвищені ризики інформаційного тиску, в першу чергу, з боку РФ. Правоохоронні органи, такі як Поліція безпеки Фінляндії (SUPO), пропонують ініціативи щодо введення кримінальної відповідальності за скоєння цілеспрямованого інформаційного впливу та поширення дезінформації на користь іноземних держав. Національний медіарегулятор (KAVI) займається розвитком медіаграмотності серед населення, що є ключовим інструментом профілактики дезінформації [13].

Механізми співпраці з громадським суспільством, які входять до комплексу інструментів ЄС у сфері боротьби з дезінформацією на національному рівні включають: фактчекінгові організації, НУО та аналітичні центри, які відіграють ключову роль у виявленні ворожих інформаційних операцій, фіксації скоординованих маніпуляцій та просуванні медіаграмотності.

Наприкінці 2021 р. новий уряд прем'єр-міністра Петра Фіали розпочав у Чеській Республіці розробку нової комплексної стратегії протидії гібридним загрозам, включаючи дезінформацію. У 2022 р. уряд призначив Міхала Кліму для координації боротьби з фейковими новинами, підтримки незалежних медіа та розвитку медіаграмотності. Зокрема, було ухвалено Національну стратегію протидії гібридним загрозам [37] та План дій для боротьби з дезінформацією [19].

Саме Чехія створила одну з найефективніших моделей протидії дезінформації в Європі, яка базується на поєднанні дій спеціалізованих державних структур, законодавчих ініціатив, фактчекінгових проєктів та програм медіаграмотності [23, с. 372]. Країна розглядає російську та китайську пропаганду як головну загрозу національній безпеці. Так, у Чехії діє аналітичний центр, відомий своєю програмою Kremlin Watch. Організація системно документує інструменти російського впливу, навчає журналістів та випускає аналітичні звіти для політиків ЄС. PSSI (Prague Security Studies Institute) – чеський аналітичний центр, що спеціалізується на дослідженні економічних і мережевих механізмів пропаганди в ЄС [5, с. 21-22].

Після повномасштабного вторгнення РФ в Україну чеський уряд ініціював блокування низки проросійських веб-сайтів, які використовувалися як інструменти інформаційної війни. У лютому 2023 р. посаду урядового уповноваженого з питань ЗМІ було скасовано, а функцію координації стратегічних комунікацій передали Національному раднику з безпеки. З того часу Чехія продовжила фокусуватися на підвищенні стійкості суспільства та посиленні стратегічної комунікації, а також активно закликала технологічні платформи до маркування ШП-контенту [34, с. 46-47].

Слід зазначити, що у Чехії діють такі ключові національні державні служби та інституції у сфері боротьби з дезінформацією: 1) Центр протидії тероризму та гібридними загрозами (СТНН), який є спеціалізованим аналітичним та комунікаційним підрозділом Міністерства внутрішніх справ Чехії. Центр відстежує внутрішні та зовнішні загрози, викриває фейки, аналізує дезінформаційні кампанії (зокрема щодо внутрішньої безпеки та виборів); 2) Служба безпеки та інформації (BIS) – головне агентство внутрішньої розвідки та контррозвідки Чехії. Служба розслідує загрози,

пов'язані з іноземним шпигунством, впливом державних акторів (таких як РФ і Китай) та їхніми спробами підібрати ключі до демократичних інституцій; 3) Національне управління кібернетичної та інформаційної безпеки (NUKIB), яке є центральним адміністративним органом, який відповідає за безпеку в кібернетичному просторі та захист важливої інфраструктури, запобігаючи масованим цифровим атакам і мережевим маніпуляціям [34, с. 48-49].

На загальноєвропейському рівні Франція, Німеччина, Фінляндія і Чехія співпрацюють у межах EDMO та впроваджують оновлений Кодекс практики проти дезінформації, який вимагає від великих технологічних компаній прозорості та боротьби з ботами і дипфейками.

Висновки та перспективи подальших розвідок у цьому напрямі. Отже, дезінформація сама по собі не є історично новим явищем, її масштаби, резонанс та небезпеки різко посилюються завдяки можливостям, що пропонуються цифровим суспільством. Від моменту незаконної анексії Криму у 2014 р. та до початку повномасштабної війни РФ проти України у 2022 р., питання боротьби з дезінформацією в ЄС набуло особливої актуальності. Адже, дезінформація становить значну загрозу цінностям демократії, підриваючи здатність громадян ЄС приймати обґрунтовані та вільні політичні рішення.

Комплекс інструментів ЄС у сфері боротьби з дезінформацією на загальноєвропейському рівні включає: регуляторні інструменти (DSA, кодекси, законодавство); інституційні (EEAS, EDMO, StratCom); комунікаційні (стратегічні кампанії, EUvsDisinfo); технологічні (ШП-моніторинг, співпраця з платформами); освітні інструменти (медіаграмотність, суспільна стійкість).

Визначено, що ЄС використовує декілька загальних рамкових документів та директив для забезпечення підзвітності технологічних платформ та оптимізації реагування на загрози: Закон про цифрові послуги (DSA), який є фундаментом регуляторної стратегії ЄС та передбачає сувору оцінку ризиків, алгоритмічну прозорість та незалежний аудит для дуже великих онлайн-платформ та пошукових систем; Європейський закон про свободу ЗМІ (EMFA) – регламент ЄС, що встановлює спільні правила для захисту незалежності журналістів, редакційної свободи та медіаплюралізму в рамках ЄС; Кодекс практики щодо дезінформації, який окреслює зобов'язання щодо демонетизації дезінформації, забезпечення прозорості політичної реклами та боротьби з фейковими акаунтами. Заходи з розбудови потенціалу, а саме медіаграмотності та інституційної стійкості громадян ЄС передбачають: навчання громадян розпізнавати неправдивий контент; підтримку незалежної журналістики; фінансування факче-

кінгових мереж та координацію реакцій через Систему раннього попередження (EWCS).

У ході дослідження комплексу інструментів ЄС у сфері боротьби з дезінформацією на національному рівні автором з'ясовано, що кожна держава-член має власні інструменти для захисту інформаційного простору, а саме: 1) національні регулятори медіа, які співпрацюють з європейськими мережами для перевірки фактів та нагляду за дотриманням стандартів мовлення й соцмережами; 2) багато країн (наприклад, Франція та Німеччина) мають власні центри стратегічних комунікацій та агентства кібербезпеки. Ці спеціалізовані урядові структури виявляють іноземне втручання та координують оперативне реагування; 3) системи швидкого оповіщення, країни інтегровані в європейську Rapid Alert System, яка дозволяє миттєво ділитися даними про нові дезінформаційні кампанії між урядами; 4) державні органи фінансують національні освітні кампанії, що навчають громадян розпізнавати фейки, критично мислити та перевіряти джерела (програми з медіаграмотності).

Згідно результатів щорічного дослідження Media Literacy Index Фінляндія, Франція, Німеччина та Чехія визнані лідерами у сфері боротьби з дезінформацією, але кожна з цих країн використовує власні унікальні підходи – від розбудови суспільної стійкості до жорсткого регулювання та викриття мереж. Кожна з цих країн робить акцент на різних аспектах захисту інформаційного простору. Франція відзначається проактивним викриттям, а Німеччина робить ставку на технологічний контроль та законодавство. Франція і Німеччина активно розбудовують законодавство проти дезінформації, яке базується як на їхніх власних, національних законах, так і на масштабних європейських директивах, які зобов'язують цифрові платформи та соціальні мережі блокувати маніпуляції та забезпечувати прозорість. Фінляндія фокусується на профілактиці, вона є світовим лідером у сфері медіаграмотності, інтегруючи критичне мислення в шкільну програму з ранніх років. Чехія використовує потужний експертний потенціал громадянського суспільства. У країні ефективно працюють сильні неурядові аналітичні центри.

Таким чином, взаємодія загальноєвропейського і національного рівнів у сфері боротьби з дезінформацією полягає в тому, що ЄС задає правила, стандарти та здійснює загальне фінансування (EDMO, EUvsDisinfo, Big Data, Rapid Alert System), а національні уряди держав-членів ЄС реалізують ці політики через спільні механізми, фінансуючи впровадження проєктів на власному рівні. ЄС створює єдину законодавчу базу та інфраструктуру, тоді як національні уряди імплементують ці норми, здійснюють безпосередній нагляд

і впроваджують програми з медіаграмотності. українського досвіду протидії гібридній агресії
Перспективи подальших розвідок у цьому напрямі РФ у загальноєвропейську систему стратегічних
 полягають у дослідженні механізмів інтеграції комунікацій та безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Гуйван О. У Євросоюзі створили новий інструмент для протидії дезінформації. *Інтернет-видання «Суспільне Мовлення»*. 2022. 24 жовтня. URL: <https://suspilne.media/301846-u-evrosouzi-stvorili-novij-instrument-dla-protidii-dezinformacii/>
2. Європейська група регуляторів аудіовізуальних медіапослуг готується до реформування. *Національна рада України з питань телебачення і радіомовлення*. 2024. 17 квітня. URL: <https://webportal.nrada.gov.ua/yevropejska-grupa-regulyatoriv-audiovizualnyh-mediaposlug-gotuyetsya-do-reformuvannya/>
3. ЗМІ: ЄС планує створити орган для боротьби з російською дезінформацією. *Інтернет-видання «Європейська правда»*. 2025. 7 листопада. URL: <https://www.euointegration.com.ua/news/2025/11/7/7224411/>
4. Карпчук Н. П. Стратегічна комунікація ЄС як засіб у боротьбі з дезінформацією. *Політичне життя*. 2019. № 1. С. 52-58. DOI: 10.31558/2519-2949.2019.1.7
5. Матвійчук Н., Корнійчук Л. Інформаційна політика Чеської Республіки як інструмент забезпечення інформаційної безпеки під впливом російсько-української війни. *Міжнародні та політичні дослідження*. № 5 (11). 2025. С. 19-25. DOI: [https://doi.org/10.26642/sas-2025-5\(11\)-19-25](https://doi.org/10.26642/sas-2025-5(11)-19-25)
6. Оновлення кодексу ЄС щодо боротьби з дезінформацією: основні положення. *ТОВ «ЛІГА ЗАКОН»*. 2022. URL: https://jurliga.ligazakon.net/news/212519_onovlennya-kodeksu-s-shchodo-borotbi-z-deznformatsyu-osnovn-polozhennya
7. Регулятор з питань медіа Франції об'єднався з органом з питань регулювання мережі Інтернет в єдину інституцію для кращого виконання своїх повноважень. *Національна рада України з питань телебачення і радіомовлення*. 2022. 14 січня. URL: <https://webportal.nrada.gov.ua/regulyator-z-pytan-media-frantsiyi-ob-yednavsya-z-organom-z-pytan-regulyuvannya-merezhi-internet-v-yedynu-instytutsiyu-dlya-krashhogo-vykonannya-svoyih-povnovazhen/>
8. Рожкова Г. Інструменти ЄС у боротьбі з дезінформацією. *Stopfake.org*. 2018. URL: <https://www.stopfake.org/uk/instrumenty-yes-u-borotbi-z-dezinformatsiyeyu/>
9. Самчинська О. А. Правові вектори протидії дезінформації: досвід Європейського Союзу. *Форум права*. 2023. №4. С. 6–15. DOI: <http://doi.org/10.5281/zenodo.10114539>
10. Стьопкін А. Інституціоналізація політики протидії дезінформації в Європейському Союзі. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2022. № 10. С. 196–208. DOI: <https://doi.org/10.31861/mediaforum.2022.10.196-208>
11. Сухоруков В. І. Боротьба з дезінформацією в ЄС: правові інструменти та їх ефективність. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. Т. 2. Вип. № 4. 2025. С. 362-366. DOI: <https://doi.org/10.24144/2788-6018.2025.04.2.60>
12. Федунь О. В., Милан С. А. Трансформація підходів Європейського Союзу до протидії дезінформації (2014–2026). *Науковий журнал «Politicus»*. Вип. №2. 2026. С. 189-197. DOI: <https://doi.org/10.24195/2414-9616.2026-2.29>
13. Фінську молодь навчають виявляти дезінформацію. *Інформаційний Інтернет-ресурс «Голос Америки»*. 2024. URL: <https://www.holosameryky.com/a/finsku-molod-navchayut-vyavlyaty-desinformatsiyu/7912346.html>
14. Французька агенція VIGINUM: 193 сайтів розповсюджують російські фейки про війну в Україні. *Інформаційне агентство «Центр новин»*. 2024. URL: <https://www.centernews.com.ua/?p=439559>
15. Хакімова В. Т. Європейський Союз в епоху постправди: діяльність East StratCom Task Force. *Актуальні проблеми політики: зб. наук. пр.* Одеса: Гельветика, 2021. Вип. 67. С. 155–162. DOI: <https://doi.org/10.32837/app.v0i67.1166>
16. Черниш Р. Правовий досвід країн Європейського Союзу у сфері протидії поширенню фейкової інформації. *Підприємництво, господарство і право*. 2019. № 10. С. 123-128. DOI: <https://doi.org/10.32849/2663-5313/2019.10.21>
17. Act no. 2018-1202 of 22 December 2018 on the fight against the manipulation of information. *European Audiovisual Observatory*. URL: <https://merlin.obs.coe.int/article/8477>
18. Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act). *Bundesministerium der Justiz und für Verbraucherschutz*. 2017. URL: https://www.bmjbv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/NetzDG_engl.pdf?__blob=publicationFile&v=4&utm
19. Action Plan against Disinformation. *The free encyclopedia "Wikipedia"*. 2022. URL: https://en.wikipedia.org/wiki/Action_Plan_against_Disinformation
20. Action Plan on disinformation: Commission contribution to the European Council. *European Commission*. 13-14 December. 2018. URL: https://commission.europa.eu/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en
21. Bayer J. Policies and measures to counter disinformation in Germany: the power of informational communities. *Heinrich-Böll-Stiftung*. 2021. URL: <https://eu.boell.org/en/2021/10/13/policies-and-measures-counter-disinformation-germany-power-informational-communities>

22. Bleyer-Simon K., Brogi E., Nenadić I., Nesovic T. Policies to tackle disinformation in EU member states – part 2. *European Digital Media Observatory*. 2022. 43 p. URL: <https://edmo.eu/wp-content/uploads/2022/07/Policies-to-tackle-disinformation-in-EU-member-states-%E2%80%93-Part-II.pdf>
23. Cabada L. Struggle against Disinformation in the Czech Republic: Treading the Water. *Politics in Central Europe*. Vol. 19. No. 1S. P. 371-391. DOI: <https://doi.org/10.2478/pce-2023-0017>
24. Cianciara A. K. How to reconcile countering FIMI and protecting democratic values: the case of France. *EU-VALUES*. 2025. 12 of February. URL: <https://www.eu-values.eu/blog/how-to-reconcile-countering-fimi-and-protecting-democratic-values-the-case-of-france>
25. Coli M. The Role of the European Union in Protecting Democracy through Legislation: The Case of Disinformation. *European Papers – A Journal on Law and Integration*. Vol. 11. No. 1. 2026. P. 81–111. 2026. URL: https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2026_1_Martina_Coli_00863.pdf
26. 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. COM/2018/236 final. *European Union*. 2018. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52018DC0236>
27. Digital Service Act. *European Union*. 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>
28. EU DisinfoLab: From expertise to action against disinformation. *EU DisinfoLab*. 2026. URL: <https://www.disinfo.eu/>
29. European Council meeting (19 and 20 March 2015) – Conclusions. *European Council*. 2015. URL: <https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf>
30. European Democracy Action Plan: making EU democracies stronger. *European Commission*. 2020. URL: https://ec.europa.eu/commission/presscorner/detail/ga/ip_20_2250
31. Factsheet: Rapid Alert System. *European Union*. 2019. URL: https://www.eeas.europa.eu/node/59644_en
32. 15 Hubs Cover All 27 EU Member States as well as Moldova, Norway and Ukraine. *European Digital Media Observatory*. 2026. URL: <https://edmo.eu/about-us/edmo-hubs/>
33. Hénin N. Disinformation landscape in France. *EU DisinfoLab*. 2023. 7 p. URL: https://www.disinfo.eu/wp-content/uploads/2023/03/20230224_FR_DisinfoFS.pdf
34. Kolomazník T. Building Resilience Against Disinformation: Czech Perspective and Experience. 2025. *Studia de Securitate*. № 15(1). P. 44-58. DOI:10.24917/20820917.15.1.3
35. National Coordination Centres. *European Cybersecurity Competence Centre and Network*. 2026. URL: https://cybersecurity-centre.europa.eu/nccs_en
36. National strategy for countering foreign information manipulation for 2026-2030. *The Secretariat-General for National Defence and Security*. 2026. URL: https://www.sgdsn.gouv.fr/files/files/Publications/20260311_SNLMI_ENG.pdf
37. National Strategy for Countering Hybrid Interference. *Ministerstvo obrany ČR*. 2021. URL: <https://www.mo.gov.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf>
38. Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act). *European Union*. 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1083/oj/eng>
39. Saari D., Moilanen P., Hautala M. Disinformation landscape in Finland. *EU DisinfoLab*. 2023. URL: https://www.disinfo.eu/wp-content/uploads/2023/05/Finland_DisinfoFactsheet.pdf
40. Sauv   M-R., Coutant A. The French law against the manipulation of information during elections and the professional practices of journalists in the face of the phenomenon of “fake news”. *Les Enjeux de l’information et de la communication*. № 23/1A. 2023. P. 103-122. URL: <https://shs.cairn.info/journal-les-enjeux-de-l-information-et-de-la-communication-2023-S1-page-103?lang=en>
41. The 2022 Code of Practice on Disinformation. *European Commission*. 2022. URL: <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>
42. The NIS 2 Directive | Updates, Compliance. *NIS 2 Directive*. 2024. URL: <https://www.nis-2-directive.com/>
43. The Media Literacy Index 2026. Measuring Vulnerability of Societies to Disinformation. *Open Society Institute – Sofia*. January, 2026. URL: <https://osis.bg/wp-content/uploads/2026/01/Media-Literacy-Index-2026.pdf>
44. Zinenko A., Svoboda I., Dereshchuk T., Shevchenko N., Shapovalenko M. EU Policy on Countering Disinformation and its Impact on the Information Security of Member States. *Revista Jur  dica Portucalense*. 2026. № 1(39). P. 147–171. DOI: [https://doi.org/10.34625/issn.2183-2705\(39.1\)2026.ic-7](https://doi.org/10.34625/issn.2183-2705(39.1)2026.ic-7)

Дата першого надходження статті до видання: 14.07.2026
Дата прийняття статті до друку після рецензування: 25.08.2026
Дата публікації (оприлюднення) статті: 28.09.2026