Федунь Олександра Василівна
Милян Софія Андріївна

Трансформація підходів Європейського Союзу до протидії дезінформації (2014–2026)

УДК 327(4-ЄС):316.776.23-048.66(470)]»201/202»
DOI https://doi.org/10.24195/2414-9616.2026-2.29

Федунь Олександра Василівна
кандидат географічних наук,
доцент кафедри європейських
та регіональних студій
Львівського національного університету
імені Івана Франка
вул. Університетська, 1, Львів, Україна
ORCID: 0000-0003-3182-0725

Милян Софія Андріївна
магістр освітньої програми
«Європейські студії»
Львівського національного університету
імені Івана Франка
вул. Університетська, 1, Львів, Україна
ORCID: 0009-0004-3072-4154

У статті досліджені особливості становлення та динамічного розвитку політики Європейського Союзу у сфері протидії дезінформації. З 2014 року проблема поширення російських маніпулятивних наративів у європейському медіапросторі набула якісно нового змісту: трактується не як комунікаційний виклик та елемент «м'якої» сили, а як гібридна загроза демократичним інститутам і безпеці. Запропонована періодизація діяльності ЄС у сфері протидії дезінформації на основі низки критеріїв: ідентифікація та оцінка реальних і потенційних інформаційних загроз, визначення цілей і принципів політики у сфері стратегічних комунікацій, формування правового та інституційного механізмів, використання практичних інструментів протидії дезінформації. У межах досліджуваного періоду (2014–2026) виокремлено чотири етапи. Вони відображають послідовну трансформацію підходів ЄС до протидії дезінформації в кореляції з реконцептуалізацією інформаційних загроз, зміною пріоритетів, стратегічних цілей та інструментів, посиленням міжінституційної координації й управління системними ризиками. Обґрунтовано, що в 2014–2017 роках переважав ситуативно-адаптативний підхід, 2018–2019 – стратегічний, 2020–2021 – багаторівневий та інтегрований, 2022–2026 – міжсекторальний. Проаналізовано низку запроваджених механізмів та інструментів ЄС на кожному етапі, зокрема таких як: План дій проти дезінформації, Кодекс практики щодо дезінформації, Акт про цифрові послуги та ін. Наголошено на особливій ролі України, яка є стратегічним партнером ЄС, ділиться власним досвідом та надає верифіковану доказову базу для антиросійських санкцій. Зроблено висновок, що усвідомлення онтології загрози, яку становить навмисна іноземна маніпуляція інформацією, зумовило еволюцію інформаційної політики Європейського Союзу від ліберальної моделі забезпечення свободи слова до імперативного регулювання та системної протидії дезінформації з використанням інституційних, комунікаційних та регуляторних механізмів.

Ключові слова: *дезінформація, інформаційні загрози, підхід, протидія, політика, безпека, ЄС.*

Вступ. У сучасній архітектурі міжнародної безпеки інформаційні загрози набувають особливого значення. Виступаючи інструментом гібридної агресії, вони суттєво впливають на політичні процеси, державний суверенітет, соціальну стабільність і рівень довіри громадян до влади. З 20 лютого 2014 року російська збройна агресія супроводжується інформаційними атаками, що спрямовані не лише на Україну, але й на держави-члени ЄС. Росія тривалий час використовує інформацію як зброю з метою посіяти розкол усередині Євросоюзу та дискредитувати підтримку України. Тому проблема поширення дезінформації у міжнародному контексті, яка набула якісно нового змісту, перейшла з гуманітарної сфери в безпекову. У Європейському Союзі її перестали розглядати виключно як комунікаційний виклик, а почали трактувати як системну загрозу демократичним інститутам, виборчим процесам і спільній безпеці. Це зумовило перехід від ситуативного реагування на загрозливі інформаційні кампанії до концепції формування комплексної політики ЄС в сфері протидії дезінформації.

Російська агресія проти України актуалізувала питання захисту інформаційного простору держав і регіонів, спонукала ЄС до активного реагування на поширення дезінформації, яку офіційно визнали гібридною загрозою європейській безпеці та демократичним процесам. Безпрецедентний масштаб маніпуляцій і втручання Росії в інформаційний простір змусили ЄС фундаментально переглянути стратегію інформаційної безпеки. Цей процес супроводжувався визначенням нових цілей, проголошенням відповідних принципів, формуванням правового регулювання, створенням спеціальних механізмів та інструментів. Проблеми поширення прокремлівських дезінформаційних наративів стали предметом не лише стратегічних комунікацій, але й регуляторної, цифрової та безпекової політики Союзу. У процесі скоординованої взаємодії з ООН, НАТО, ОБСЄ, G7 та іншими партнерами Євросоюз став провідним актором у формуванні міжнародних стандартів протидії дезінформації та стратегічного стримування інформаційних загроз.

Сучасні наукові праці зарубіжних та українських дослідників переважно зосереджені на вивченні загроз інформаційній безпеці та спеціальних інструментів Європейського Союзу для боротьби з дезінформацією. Проте поза увагою вчених залишається концептуальний аналіз еволюції підходів у цій сфері на різних етапах у контексті переосмислення онтології загроз, інституціалізації протидії

дезінформації, її інтеграції в безпекову та цифрову політику для посилення інформаційної стійкості ЄС.

Мета полягає у виявленні чинників та ознак трансформації підходів Європейського Союзу до протидії дезінформації після початку російської агресії проти України у 2014 році, що передбачає аналіз реконцептуалізації інформаційних загроз і порівняння пріоритетів, стратегічних цілей та інструментів. Дослідження спрямоване на обґрунтування періодизації, яка розкриває еволюцію діяльності Євросоюзу у сфері протидії дезінформації, перехід від ситуативного реагування до розробки комплексної стратегії та формування політики міжінституційної координації, впровадження багаторівневого і міжсекторального підходів ЄС до протидії дезінформації.

Методи дослідження. Під час дослідження використано низку методів наукового пізнання, зокрема історичний, порівняльний, періодизації, критичного аналізу та синтезу. Історичний метод дав змогу простежити етапи розвитку політики Європейського Союзу у сфері протидії дезінформації. Застосування порівняльного методу сприяло виявленню відмінностей та особливостей діяльності ЄС на різних етапах. Метод періодизації допоміг структурувати процес трансформації політики ЄС за етапами. На основі критичного аналізу виявлено як у результаті інтерпретації фактів про російську пропаганду Євросоюз змінив підходи до інформаційної політики, наприклад, щоб захистити ліберальні цінності застосував нелібералні прийоми (обмежувальні заходи, заборони та ін.). Метод синтезу застосований для виявлення трансформації підходів ЄС до протидії дезінформації.

Результати дослідження. У сучасному інформаційному просторі дезінформація перестала бути локальним або ізольованим явищем і перетворилася на системний інструмент політичного, гібридного та стратегічного впливу на окремі держави, регіони та міжнародні організації [11]. Цей процес став можливим завдяки стрімкому розвитку цифрових технологій, популярності соціальних медіа та використання алгоритмічних систем, які формують нову динаміку поширення інформації. Як наслідок, розповсюдження контенту відбувається миттєво, а його вплив на суспільну думку, політичні процеси та рівень довіри громадян до інституцій є значним і довготривалим. У цьому контексті інформаційна безпека стає невід'ємною складовою національної та регіональної політики, а ефективні механізми протидії дезінформації перетворюються на ключовий елемент сучасних стратегій безпеки [11].

У політичному дискурсі дезінформація визначається як навмисне поширення неправдивої або маніпулятивної інформації з метою введення громадськості в оману та досягнення політичних або стратегічних цілей [24]. На відміну від неправдивої інформації, яка може поширюватися ненавмисно, дезінформація є свідомим актом спотворення інформаційного середовища з боку певних суб'єктів. Протидія дезінформації – це сукупність політичних, технологічних та освітніх заходів, спрямованих на виявлення, аналіз і зменшення впливу спеціально створеної неправдивої інформації, що має потенціал завдати суспільної або політичної шкоди [1].

Незаконна анексія Криму державою-агресором у лютому 2014 року, розгортання збройного протистояння на сході України, збиття МН17 над Донбасом 17 липня 2014 року супроводжувалися масштабними кампаніями з поширення кремлівської дезінформації з метою виправдати війну, дестабілізувати суспільно-політичну ситуацію як в Україні, так і державах ЄС.

Російська агресія продемонструвала, що пропаганда, маніпулятивні наративи та медіа-інструменти активно використовуються як важлива складова гібридних стратегій, спрямованих на формування суспільної думки та перебіг політичних процесів на національному, регіональному та глобальному рівнях. На цьому тлі ЄС почав розглядати дезінформацію як чинник, що істотно впливає на демократичні інститути та систему європейської безпеки, а не лише як проблему медіа-середовища.

Зазначимо, що спочатку Євросоюз робив ставку на дипломатичний діалог і побудову довіри з державою-агресором і не сприймав дезінформацію як пряму загрозу власній безпеці. До 2014 року ЄС зосереджувався на питаннях впровадження медіастандартів, підтримки свободи слова та доступу до публічної інформації, а поширення дезінформації вважав проблемами окремих держав-членів. Інформаційні кампанії більшою мірою розглядалися як елемент «м'якої сили», особливо у сферах культури та дипломатичної комунікації, а не як системна загроза безпеці.

Україна, яка перша стала об'єктом агресивної інформаційної війни Росії, надавала докази технологічних й психологічних атак, наголошуючи, що інформація є не лише засобом впливу, а й потенційною зброєю в умовах гібридного конфлікту. Проте цей меседж сприймався як думки експертів, тому до певного часу не знаходив достатнього відгуку в європейському істеблішменті та у стратегічних документах Євросоюзу, відповідно й не призвів до негайних масштабних і рішучих змін у європейській політиці.

Лише поступове усвідомлення онтології загрози, яку становить навмисна іноземна маніпуляція інформацією, змусило ЄС переглянути існуючі підходи та перейти від ліберальної моделі забезпечення свободи слова до імперативного регулювання та системної протидії дезінформації з використанням інституційних, комунікаційних і регуляторних механізмів. Сучасна інформаційна політика Євросоюзу ставить за мету захист демо-

кратичних цінностей, регулювання медіасередовища, протидію дезінформації та забезпечення стійкості.

У результаті дослідження зміни пріоритетів, політико-правових та інституційних механізмів простежуються певні відмінності, тому процес розвитку діяльності ЄС у сфері протидії інформаційним загрозам доцільно структурувати, виділивши чотири етапи:

1) 2014–2017 – етап, на якому ЄС переходить від ліберальних стандартів свободи слова до активного захисту інформаційного простору, включає проблематику інформаційних загроз до порядку денного Європейської Ради, виявляє та реагує на дезінформацію як загрозу європейським цінностям і безпеці.

2) 2018–2019 роки – етап, на якому інформаційні загрози визнаються системними, формується довгострокова стратегія ЄС щодо протидії дезінформації, створюється регуляторна рамка та інструментарій.

3) 2020–2021 роки – етап, на якому відбувається інтеграція протидії дезінформації у цифрову, безпекову та демократичну політику, налагоджується структурована взаємодія ЄС з міжнародна партнерами.

4) 2022–2026 роки – етап, коли на основі поєднання безпекового, цифрового та санкційного вимірів, посилення міжінституційної координації та управління системними ризиками відбувається перехід до моделі інформаційної стійкості ЄС та стратегічного стримування у тісній взаємодії з державами-членами, Україною та міжнародними організаціями, такими як НАТО, ОБСЄ, G7 та ін. партнерами.

Основними критеріями запропонованої періодизації визначені наступні: ідентифікація та оцінка реальних і потенційних інформаційних загроз, зміна підходів Євросоюзу до дезінформації,визначення цілей і принципів політики у сфері стратегічних комунікацій, формування правового та інституційного механізмів, використання практичних інструментів протидії дезінформації. Відправною точкою формування комплексної політики стало розгортання інформаційної війни Росії проти України в 2014 році як складової гібридної агресії.

У таблиці 1 наведено основні підходи на кожному з вищезгаданих етапів, зазначено конкретні механізми й інструменти, запроваджені на рівні ЄС у відповідь на актуальні інформаційні загрози.

На першому етапі розвитку діяльності ЄС у сфері протидії дезінформації, який тривав з 2014 по 2017 рік, переважав ситуативно-адаптативний підхід, спрямований на реагування та пристосування до актуальних на той час гібридних загроз. На цьому етапі Євросоюз визнав російську пропаганду як зовнішньополітичний виклик для безпеки. Розпізнавання та оцінка інформаційних загроз, усвідомлення їх масштабів призвели до формування первинних механізмів реагування. Проте такі дії мали несистемний характер.

Уперше про необхідність «протидіяти постійним дезінформаційним кампаніям Росії» зазначено у п. 13 висновків Європейської Ради від 20 березня 2015 року, де запропоновано у стислі терміни підготувати план дій у сфері стратегічних комунікацій [13]. У результаті тісної співпраці Верховного представника з інституціями ЄС та державами-членами у квітні того ж року створена Оперативна робоча група зі стратегічних комунікацій у Східному регіоні **(**East StratCom Task Force (ESTF) при Європейській службі зовнішніх справ (ЄСЗС) (European External Action Service – EEAS**).** Основні завдання цієї групи включають виявлення, аналіз і публічне спростування дезінформації, спрямованої проти держав ЄС та країн Східного партнерства. Заснування ESTF фактично ознаменувало офіційне визнання того, що необхідно цілеспрямовано реагувати на загрози російських маніпулятивних наративів і запобігати їх деструктивному впливу на суспільно-політичні процеси у державах ЄС.

Для протидії безперервним інформаційним кампаніям Росії у 2015 році запущений флагманський проєкт ESTF EUvsDisinfo (Платформа ЄС проти дезінформації)**.** Ця платформа здійснює постійний моніторинг інформаційного простору, фіксує випадки дезінформації та поширює аналітичні матеріали щодо маніпулятивних інформаційних наративів. За десять років роботи EUvsDisinfo виявлено та спростовано майже 20 тис. випадків дезінформації [17].

У 2016 році Євросоюз офіційно визнав Росію джерелом дезінформації, що закріплено в положеннях Спільного підходу до протидії гібридним загрозам (Joint Framework on Countering Hybrid Threats – a European Union Response). Відтоді ЄС перейшов до розбудови координації дій між державами-членами, що передбачає посилення стратегічних комунікацій та підвищення стійкості інформаційного середовища [12].

Таким чином, у 2015–2017 роках у результаті реконцептуалізації інформаційних загроз Європейський Союз основну увагу приділяв моніторингу маніпулятивного інформаційного контенту та налагодженню взаємодії між державами-членами. Проблема деструктивного впливу дезінформації на суспільно-політичні процеси вперше була винесена на порядок денний Євросоюзу. Концентрація зусиль ЄС на створенні спеціальних інструментів стратегічних комунікацій сприяла первинній інституціоналізації протидії російській дезінформації.

Другий етап охоплює 2018–2019 роки й характеризується переходом від реактивних заходів реагування на постійні інформаційні загрози до розробки стратегії та системної політики. ЄС розпочав формування комплексної нормативно-правової

Таблиця 1

Підходи Європейського Союзу до протидії дезінформації (2014–2026)

Етап	Роки	Підхід	Характеристика змін	Механізми та інструменти
I етап	2014–2017	Ситуативно-адаптивний	Визнання інформаційних загроз та оцінка ризиків; визначення дезінформації як елементу гібридних загроз безпеці ЄС, оперативне реагування; первинна інституціоналізація.	East Strategic Communication Task Force (2015); EUvsDisinfo (2015); Joint Framework on Countering Hybrid Threats – a European Union Response (2016)
II етап	2018–2019	Стратегічний	Формування стратегії ЄС у сфері в сфері протидії дезінформації, створення нормативно-регуляторної основи та інституційного механізму, посилення міжвідомчої співпраці, залучення онлайн-платформ, підвищення прозорості політичної реклами.	Report of the High-Level Expert Group on Fake News and Online Disinformation (2018); Communication on Tackling Online Disinformation (2018), Communication on Securing Free and Fair European Elections (2018); Action Plan against Disinformation (2018); EU Code of Practice on Disinformation (2018); Rapid Alert System (2019)
III етап	2020–2021	Багаторівневий Інтегрований	Нормативно-правове регулювання, закріплення стандартів, координація; інтеграція протидії дезінформації у цифрову та безпекову політику ЄС; багаторівнева взаємодія; перехід до регуляторних рішень.	COVID-19 Disinformation Monitoring Programme (2020); European Digital Media Observatory (EDMO) (2020); European Democracy Action Plan (2020); EU Code of Practice on Disinformation (ongoing revision)
IV етап	2022 – 2026	Міжсекторальний	Перехід до моделі інформаційної стійкості та стратегічного стримування; поєднання безпекового, цифрового та санкційного вимірів, посилення міжінституційної координації та управління системними ризиками; регулювання діяльності онлайн-платформ і посередників (соціальні мережі, маркетплейси), пошукових систем на основі нових вимог і правил; посилення координації дій з ООН, НАТО, ОБСЄ, Радою Європи, G7 та іншими міжнародними партнерами.	Implementation of Digital Services Act (2022); Code of Practice on Disinformation (2022); Integration of FIMI into the EU Strategic Compass; Integration of the Code of Practice on Disinformation into the DSA (2025); Code of Conduct under the Digital Services Act (2025); Regulation on Transparency and Targeting of Political Advertising (2025); Restrictive Measures Against Individuals Over Information Manipulation (CFSP Sanctions on FIMI Actors) (2026); **Annual EEAS Reports on Foreign Information Manipulation and Interference**

Джерело: складено авторами.

та інституційної бази для запобігання й протидії дезінформації. Важливим чинником цих змін стало визнання того, що кампанії з поширення іноземними державами маніпулятивної інформації підривають довіру до демократичних інституцій і впливають на політичні процеси, зокрема на вибори, і що їх також слід розглядати у контексті стратегій гібридного впливу.

У 2018 році незалежна група експертів опублікувала «Звіт високого рівня експертної групи з питань фейкових новин та онлайн-дезінформації» (Report of the High-Level Expert Group on Fake News and Online Disinformation), в якому вказано на основні ризики поширення дезінформації в цифровому середовищі та надано рекомендації щодо підвищення прозорості онлайн-платформ, розвитку механізмів перевірки фактів та посилення медіа грамотності [10]. На основі практичних рекомендацій експертів Європейська комісія розробила та опублікувала у квітні 2018 року «Комюніке щодо протидії онлайн-дезінформації: європейський підхід» (Communication on Tackling Online Disinformation: A European Approach) [6]. Цей документ визначив основні напрями політики ЄС з метою протидії дезінформації, зокрема акцентував на необхідності посилення співпраці між державними органами, громадянським суспільством, науковими установами та онлайн-платформами.

Безпрецедентним викликом для ЄС виявилося зовнішнє втручання у політичні та виборчі процеси. Тому на захист запланованих на 2019 рік виборів до Європарламенту у квітні 2018 року Європейська комісія ухвалила «Комюніке щодо забезпечення вільних і чесних європейських виборів» (Communication on Securing Free and Fair European Elections). Реалізація цього пакету заходів допомогла ефективно протидіяти кібератакам, іноземному інформаційному втручанню та маніпуляціям [5].

Переломним моментом у зміні підходів ЄС став «План дій проти дезінформації» (Action Plan against

Disinformation), ухвалений у грудні 2018 року. Цей документ доповнив попередні напрацювання Євросоюзу, поєднавши дипломатичні зусилля ЄСЗС з регуляторними інструментами Європейської комісії та оперативною взаємодією держав-членів. Імплементація Плану дій забезпечила посилення аналітичних можливостей інституцій Євросоюзу, розширення діяльності відділу стратегічних комунікацій ЄСЗС та поглиблення співпраці з міжнародними партнерами.

Незважаючи на існуючі інструменти, на той час виникла гостра потреба налагодження взаємодії євроінституцій з приватним сектором (цифровими платформами і технологічними компаніями) для розробки добровільних стандартів боротьби з фейками. Відповідно Єврокомісія, залучивши провідних учасників цифрового ринку, створила такий інструмент як Кодекс практики ЄС щодо дезінформації (EU Code of Practice on Disinformation), що у 2018 році заклав основу для саморегулювання. Провідні онлайн-платформи (Google, Meta, Twitter) та інші компанії, які підписали кодекс, добровільно прийняли зобов'язання підвищити прозорість політичної реклами, обмежити поширення маніпулятивного контенту та боротися з бот-мережами [3].

Для поєднання напрацювань Плану дій проти дезінформації і практичних зобов'язань онлайн-платформ відповідно до Кодексу практики Європейська служба зовнішніх дій у березні 2019 року створила Систему швидкого оповіщення щодо дезінформації (Rapid Alert System, RAS). Цей механізм забезпечив оперативний обмін між інституціями ЄС та державами-членами інформацією про діяльність, пов'язану з дезінформацією, а також посилив їхню здатність діяти в режимі реального часу з метою оперативного реагування на інформаційні загрози [19].

Отже, у 2018–2019 роках імплементація Плану дій проти дезінформації забезпечила перехід до системної розбудови інституційного механізму, до якої долучилися основні інституції ЄС та держави-члени. Застосування стратегічного підходу сприяло формуванню стратегічної рамки, що визначає довгострокові цілі, пріоритети, принципи та регуляторні інструменти для реалізації політики Європейського Союзу щодо протидії дезінформації.

Третій етап охоплює 2020–2021 роки й характеризується переходом до багаторівневого та інтегрованого підходів у сфері стратегічних комунікацій. З 2020 року протидія дезінформації поступово інтегрувалася в галузеві політики ЄС, зокрема цифрову, безпекову та політику захисту демократичних процесів. Якщо на попередньому етапі Євросоюз формує стратегічні рамки та базові інституційні механізми реагування, то у 2020–2021 роках основну увагу приділяє багаторівневим взаємодіям, посиленню координації між інституціями, державами-членами та міжнародними партнерами.

Пандемія COVID-19 висвітлила глобальні масштаби масового поширення неправдивої інформації та стала своєрідним тестом для ЄС, який виявив недостатність наявних інструментів (East StratCom Task Forse, ін.) для боротьби з дезінформацією та емоційним контентом, що загрожує не лише політичним процесам, але й життю та здоров'ю громадян. Тому для протидії поширенню маніпулятивної інформації Європейська комісія у 2020 році запустила Програму моніторингу дезінформації щодо COVID-19 (Disinformation Monitoring Programme). Впровадження такої ініціативи забезпечило регулярний моніторинг онлайн-платформ, а також звітування про вжиті заходи, спрямовані на обмеження масового поширення недостовірної інформації [7].

У 2020 році в процесі підготовки документу з питань спільної безпеки та оборони «Стратегічний компас», ЄС провів перший комплексний аналіз усіх загроз і викликів. Досвід з часів пандемії привернув увагу до проблеми уразливості суспільства, нездатного протистояти деструктивним впливам шкідливого контенту. Як наслідок, вже під час наступного етапу Євросоюз розпочав роботу над стратегічною розбудовою інформаційної стійкості.

Своєчасне виявлення та спростування дезінформації в європейському онлайн-просторі, координація відповідей на загрози, підвищення медіаграмотності громадян потребують проведення незалежних і високоякісних досліджень. Для цього Єврокомісія відповідно до Кодексу практики ЄС (2018) у 2020 році створила Європейську обсерваторію цифрових медіа (European Digital Media Observatory, EDMO). Ця найбільша міждисциплінарна мережа сьогодні складається з 15-ти національних і регіональних центрів у 28-ми країнах. Вони об'єднують наукові установи, дослідницькі центри, організації з перевірки фактів, а також зацікавлених експертів і фахівців [15].

Зростання кібератак і часті випадки зовнішнього втручання у політичні процеси в межах ЄС вимагали відповідних рішень. Саме тому Європейська комісія ініціювала та розробила, а в 2020 році ухвалила Європейський план дій щодо захисту демократії (European Democracy Action Plan). Ця стратегічна ініціатива включає широкий перелік заходів для підвищення прозорості політичної реклами, захисту вільних і чесних виборів, підтримки незалежних медіа та боротьби з маніпулюванням інформацією, що може вплинути на перебіг та результати виборчого процесу [14].

Важливим напрямом діяльності Євросоюзу в контексті захисту від інформаційних загроз є створення нових правил цифрового регулювання з урахуванням європейських цінностей. Тому на цьому етапі для підвищення безпеки користувачів і регулювання діяльності онлайн-платформ Єврокомісія, Європарламент та Рада ЄС понад два роки працювали над розробкою одного з наймасштаб-

ніших законодавчих проєктів ЄС – Актом про цифрові послуги. Його первинний проєкт представили у грудні 2020 року, а ухвалили після внесення численних правок вже у 2022 році.

У результаті координації зусиль основних інституцій ЄС та держав-членів у 2020–2021 роках політика протидії дезінформації стала більш інтегрованою та нормативно закріпленою. Запобігання маніпулюванню інформацією стало невід'ємною частиною європейської політики у сферах цифрових технологій, безпеки та демократії.

Четвертий етап політики протидії ЄС дезінформації триває з 2022 року й дотепер. Цей етап характеризується поєднанням безпекового, цифрового та санкційного вимірів, посиленням міжінституційної координації та управління системними ризиками. Відбувається перехід до міжсекторальної моделі управління інформаційними загрозами в ЄС, яка передбачає використання санкційних механізмів. Міжсекторальна взаємодія побудована як багаторівнева мережа, що об'єднує інституції ЄС, онлайн-платорми, експертів і громадянське суспільство. На відміну від попередніх етапів, під час яких закладено інституційно-правові основи політики протидії дезінформації, особливістю четвертого етапу є спрямованість Європейського Союзу на забезпечення інформаційної стійкості та стратегічне стримування зовнішнього інформаційного впливу в тісній співпраці з міжнародними партнерами.

Переломним моментом у трансформації політичних підходів ЄС стала повномасштабна війна Росії проти України у 2022 році, яка супроводжувалася посиленням вже наявних операцій агресора щодо навмисного втручання в інформаційний простір європейських держав. У відповідь на це ЄС посилив заходи протидії іноземним інформаційним маніпуляціям, крім того включив ці питання до безпекової політики. Одним із основних інструментів, який встановив суворіші правила та контроль задля існування безпечнішого цифрового простору, є ухвалений Європейським парламентом і Радою ЄС у жовтні 2022 року Акт про цифрові послуги (Digital Services Act, DSA), що набув чинності з лютого 2024 року. Важливе значення документу полягає у тому, що він визначив правила функціонування онлайн-платформ, соціальних мереж, пошукових систем та інших цифрових посередників. DSA зобов'язав великі онлайн-платформи й сервіси хостингу оцінювати та зменшувати системні ризики, пов'язані з поширенням незаконного контенту, маніпулятивної інформації та втручання у демократичні процеси.

Зміни характеру інформаційних загроз потребували як створення нових, так і удосконалення вже діючих механізмів та інструментів для того, щоб відповідати новим викликам й забезпечити ефективність запланованих заходів протидії. Так, на основі низки рекомендацій Європейська Комісія у 2022 році підтримала оновлений (посилений) Кодекс практики щодо дезінформації, який розвиває початкову версію 2018 року [4]. Цей документ розширив зобов'язання онлайн-платформ у сферах прозорості алгоритмів, відмови від монетизації контенту, що містить дезінформацію, та співпраці з організаціями з перевірки фактів. У 2025 році оновлений Кодекс практики офіційно інтегрували у рамки вищезгаданого акту DSA з метою посилення спільної відповідальності технологічних компаній за виконання прийнятих зобов'язань. Загалом активні та послідовні дії ЄС стосовно запобігання і протидії дезінформації підвищують стандарти прозорості та підзвітності платформ, що значною мірою посилює безпеку всього цифрового простору.

Від 2022 року Євросоюз приділяє щоразу більшу увагу регулюванню політичної реклами в цифровому середовищі. У цьому контексті важливим кроком стало ухвалення у березні 2024 року Регламенту (ЄС) 2024/900 про прозорість і таргетування політичної реклами ((EU) 2024/900 on Transparency and Targeting of Political Advertising) [20]. Основні положення регламенту, які почали застосовуватися з 10 жовтня 2025 року, встановили нові вимоги до прозорості фінансування, ідентифікації замовників та використання механізмів таргетування політичної реклами як в онлайн, так і в офлайн-середовищі.

Варто наголосити на важливій ролі України, яка від початку російської агресії переконувала світове співтовариство у необхідності визнання дезінформації як складової воєнної стратегії, вимагала ухвалення санкцій проти кремлівських пропагандистів. Українські експерти надали верифіковану доказову базу, яка дозволила ЄС вперше в історії в березні 2022 року призупинити ліцензії на мовлення російських державних каналів RT і Sputnik через системне маніпулювання ними інформацією. Згодом санкції запровадили й проти низки інших ворожих ЗМІ. Українські аналітичні центри й установи, зокрема Центр протидії дезінформації (орган Ради національної безпеки і оборони України), ретельно виявляють і спростовують ворожі фейки, збирають доказову базу, аналізують поточні та прогнозовані загрози національній безпеці, діляться досвідом з партнерами про застосування власних методів моніторингу гібридних загроз й запобігання ворожим наративам. Сьогодні Україна стала активним учасником формування європейської політики стійкості.

Ефективним елементом політики ЄС є механізм санкцій проти суб'єктів, які беруть участь у маніпулюванні інформацією. Наприклад, у січні 2026 року ЄС запровадив спеціальні обмежувальні заходи проти осіб за маніпулювання інформацією, а саме обмежувальні заходи ЄС щодо осіб, причетних до маніпулювання інформацією (санкції

CFSP проти акторів FIMI) (Restrictive Measures Against Individuals Over Information Manipulation (CFSP Sanctions on FIMI Actors)), що спрямовані на боротьбу з іноземними суб'єктами, які проводять операції з поширення дезінформації [22]. На відміну від попередніх механізмів, санкції передбачають індивідуальну відповідальність суб'єктів, зокрема заморожування активів, обмеження доступу до ресурсів ЄС та заборону на в'їзд.

Санкційний механізм є логічним продовженням концепту «іноземного маніпулювання інформацією та втручання» – FIMI (Foreign Information Manipulation and Interference), що охоплює моделі маніпулятивної поведінки (тактику, техніку та процедури), які використовують зловмисники з метою введення в оману. FIMI широко використовується в офіційних політичних документах і правових актах, зокрема включений у «Стратегічний компас ЄС» (2022), який є планом дій ЄС, спрямованим на посилення спільної безпеки та оборони до 2030 року [23].

Європейська служба зовнішніх справ продовжує виконувати аналітичну та координаційну роль у протидії загрозам. Вона регулярно здійснює моніторинг інформаційного простору та публікує зведені аналітичні матеріали. Зокрема, у березні 2026 року у 4-му звіті щодо маніпулювання інформацією та втручання з боку іноземних держав (FIMI EEAS Report on Foreign Information Manipulation and Interference) проаналізовані основні тенденції та інструменти інформаційного впливу. У ньому наведені нові дані про масштаби FIMI на основі розслідування 540 інцидентів упродовж 2025 року. Ці випадки стосувалися 10500 каналів соціальних мереж і веб-сайтів, які використовувалися для створення та поширення маніпулятивного контенту [9].

Таким чином, сучасний етап політики Європейського Союзу щодо протидії дезінформації характеризується переходом до комплексної моделі управління інформаційними ризиками. Вона поєднує регуляторні механізми, санкційні заходи, координацію у сфері безпеки та співпрацю з міжнародними партнерами. Посилення нормативного регулювання у сфері протидії дезінформації та розбудова міжсекторальної взаємодії підвищує стійкість інформаційного простору до сучасних і потенційних загроз. Сьогодні ЄС виступає у ролі глобального лідера, об'єднуючи зусилля у сфері інформаційної безпеки та оперативного реагування на загрози з ООН, НАТО, ОБСЄ, Радою Європи, G7, а також з окремими державами, зокрема з Україною.

Висновки. У результаті проведеного дослідження обґрунтовано, що поширення маніпулятивних наративів у європейському медіапросторі від початку російської агресії проти України в 2014 році зумовило переосмислення онтології інформаційних загроз. Відповідно питання захисту від дезінформації та пропаганди, визнаних інструментом гібридного впливу, були включені до порядку денного Європейського Союзу. Це сприяло переходу від ліберальної моделі забезпечення свободи слова до імперативного регулювання у сфері стратегічних комунікацій.

Запропонована періодизація дозволила обґрунтувати трансформацію підходів ЄС у процесі становлення і розвитку політики системної протидії дезінформації від 2014 до 2026 року. Зокрема, у 2014–2017 роках Євросоюз оперативно реагував на російські дезінформаційні кампанії як на гібридну загрозу європейській безпеці та демократії, визначив нові цілі та пріоритети, застосовуючи ситуативно-адаптативний підхід. На основі стратегічного підходу ЄС у 2018–2019 роках розробив стратегію запобігання та протидії дезінформації, створюючи нормативно-регуляторну основу та інституційний механізм. У 2020–2021 роках налагодилася багаторівнева координація між інституціями ЄС, державами-членами і приватним сектором. Відповідно до інтегрованого підходу нормативно закріплена на той час політика протидії дезінформації узгоджується з іншими спільними політиками, передусім із цифровою та безпековою. У 2022–2026 роках міжсекторальна взаємодія спрямована на забезпечення інформаційної стійкості Європейського Союзу, стратегічне стримування зовнішнього інформаційного впливу та управління системними ризиками в тісній співпраці з міжнародними партнерами.

Отже, на сучасному етапі ЄС виступає у ролі глобального лідера, який об'єднує зусилля ООН, НАТО, ОБСЄ, Ради Європи, G7, а також України та інших держав для посилення інформаційної безпеки в умовах гібридних загроз. Перспективи подальших досліджень стосуються вивчення ролі України в європейській політиці протидії дезінформації, враховуючи її унікальний досвід та участь у формуванні нових стандартів стійкості.

REFERENCES:

1. Action Plan against Disinformation. (2018). European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018JC0036

2. Center for Countering Disinformation. (2026). Official website of the Center for Countering Disinformation under the National Security and Defense Council of Ukraine. URL: https://cpd.gov.ua/

3. Code of Practice on Disinformation. (2018). European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

4. Code of Practice on Disinformation (Strengthened Code). (2022). European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

5. Communication on Securing Free and Fair European Elections. (2018). European Commission. URL: https://commission.europa.eu/publications/securing-free-and-fair-european-elections_en

6. Communication on Tackling Online Disinformation. European Commission. (2018). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

7. COVID-19 Disinformation Monitoring Programme. (2020). European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/covid-19-disinformation-monitoring

8. Digital Services Act Package. European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

9. EEAS. (2026). Report on Foreign Information Manipulation and Interference. European External Action Service. URL: https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

10. European Commission. (2018). A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Expert Group on Fake News and Online Disinformation. URL: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

11. European Commission. (2022). Countering Information Manipulation and Disinformation: EU Actions. URL: https://commission.europa.eu/topics/countering-information-manipulation_en

12. European Commission, (2016). High Representative of the Union for Foreign Affairs and Security Policy. Joint Framework on Countering Hybrid Threats – a European Union Response. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

13. European Council. European Council Conclusions (2015). URL: https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

14. European Democracy Action Plan. European Commission. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

15. European Digital Media Observatory (EDMO). European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory

16. European External Action Service (EEAS). (2026). Official website. URL: https://www.eeas.europa.eu

17. EUvsDisinfo. EUvsDisinfo Project. URL: https://euvsdisinfo.eu/about/

18. Questions and Answers about the East StratCom Task Force. (2021). European External Action Service. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en

19. Rapid Alert System against Disinformation. (2019). European External Action Service. URL: https://www.eeas.europa.eu/eeas/factsheet-rapid-alert-system

20. Regulation on Transparency and Targeting of Political Advertising. European Parliament and the Council of the European Union. (2024). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R0900

21. Report of the High-Level Expert Group on Fake News and Online Disinformation. (2018). European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

22. Restrictive Measures Against Individuals over Information Manipulation (CFSP Sanctions on FIMI Actors). (2026). Council of the European Union. URL: https://www.consilium.europa.eu/en/press/press-releases/2026/01/29/russian-hybrid-threats-council-sanctions-six-individuals-over-information-manipulation-activities/

23. Strategic Compass for Security and Defence – For a European Union that Protects its Citizens, Values and Interests. (2022). European External Action Service (EEAS). URL: https://www.consilium.europa.eu/en/policies/strategic-compass/

24. Wardle C., Derakhshan H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. Council of Europe Report. URL: https://rm.coe.int/information-disorder-report-2017/1680766412

The transformation of the European Union's approaches to countering disinformation (2014–2026)

Feduń Oleksandra Vasylivna

PhD in Geographical Science,
Associate Professor at the Department
of European and Regional Studies
Ivan Franko National University of Lviv
Universytetska str., 1, Lviv, Ukraine
ORCID: 0000-0003-3182-0725

Mylian Sofiia Andriivna

Master at the Education Program
"European Studies"
Ivan Franko National University of Lviv
Universytetska str., 1, Lviv, Ukraine
ORCID: 0009-0004-3072-4154

The article examines the features of the formation and dynamic evolution of the European Union's policy in the field of countering disinformation. Since 2014, the spread of Russian manipulative narratives within the European media landscape has acquired a qualitatively new dimension: it is interpreted not merely as a communication challenge or an element of «soft power», but as a hybrid threat to democratic institutions and security. The author proposes a periodization of the EU's anti-disinformation activities based on a set of criteria, including: the identification and assessment of real and potential information threats; the definition of strategic communication policy goals and principles; the development of legal and institutional frameworks; and the application of practical countermeasures. Within the scope of the period under study (2014–2026), four distinct stages are identified. These stages reflect a consistent transformation of the EU's approaches to countering disinformation, in correlation with the reconceptualization of information threats, shifting priorities, strategic goals, and instruments, as well as strengthened inter-institutional coordination and systemic risk management. The study substantiates that the EU transitioned from a situational-adaptive approach (2014–2017) to a strategic one (2018–2019), followed by a «multi-level and integrated» approach (2020–2021), and finally, a cross-sectoral approach (2022–2026). The article analyzes key EU mechanisms and instruments, such as the Action Plan against Disinformation, the Code of Practice on Disinformation, and the Digital Services Act. Furthermore, it highlights Ukraine's vital role as a strategic partner that provides verified evidence for anti-Russian sanctions and shares unique expertise in countering information warfare. The study concludes that a deeper understanding of the nature of foreign information manipulation has transformed EU policy from a liberal model of ensuring freedom of speech toward a more normative and systematic regulatory framework aimed at countering disinformation through institutional and communicative mechanisms.

Key words: *disinformation, information threats, strategic approach, countermeasures, policy, security, European Union.*

Дата першого надходження статті до видання: 12.03.2026
Дата прийняття статті до друку після рецензування: 15.04.2026
Дата публікації (оприлюднення) статті: 21.05.2026