Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА

РОБОТА МАГІСТРА

на тему: **«ІНФОРМАЦІЙНА БЕЗПЕКА ЄВРОПЕЙСЬКОГО СОЮЗУ В СУЧАСНИХ УМОВАХ»**

Виконала:
студентка 2-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Ільченко Лілія Олександрівна
(прізвище, ім’я, по батькові)

Керівник:
к.п.н., доц. Виговська Ольга Сергіївна
(науковий ступінь, вчене звання, прізвище, ім’я, по батькові)

Рецензент:
к.п.н., доц. Бєлоусова Наталія Борисівна
(науковий ступінь, вчене звання, прізвище, ім’я, по батькові)

ХАРКІВ – 2025 р.

Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ
завідувач кафедри

_____ _____ **Наталія ВІННИКОВА**
(Підпис) (ім'я, прізвище)

«02» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра

Ільченко Лілія Олександрівна
(прізвище, ім'я та по батькові)

1.Тема роботи «Інформаційна безпека Європейського Союзу в сучасних умовах» керівник роботи к.п.н., доц. Виговська Ольга Сергіївна

затверджені наказом по університету від «02» червня 2025 р. № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.

2. Строк подання здобувачем вищої освіти роботи 21листопада 2025 р.

3. Перелік питань, які потрібно розробити:
- поняття та структура інформаційної безпеки в системі міжнародних;
- Європейський Союз як актор у сфері глобальної та регіональної безпеки;
- гібридні загрози та зовнішні інформаційні впливи на ЄС;
- нормативно-правове регулювання інформаційної безпеки ЄС;
- роль інституцій ЄС у забезпеченні інформаційної стійкості;
- співпраця ЄС із державами-членами та міжнародними партнерами у сфері інформаційної безпеки;
- інструменти протидії сучасним гібридним інформаційним загрозам ЄС;
- проблеми імплементації стратегічних документів ЄС у сфері інформаційної безпеки;
- напрями вдосконалення політики інформаційної безпеки ЄС та її значення для України.

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	19.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	01.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

5. Дата видачі завдання: 02 червня 2025 року (зі змінами від 10.09.2025; 06.10.2025).

Здобувач вищої освіти _____ Лілія ІЛЬЧЕНКО
(підпис) (ім'я, прізвище)

Керівник роботи _____ Ольга ВИГОВСЬКА
(підпис) (ім'я, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми зумовлена стрімким розвитком цифрових технологій, глобалізаційних процесів та посиленням гібридних загроз, які дедалі більше впливають на стабільність європейського простору. У XXI столітті інформація стала не лише ресурсом, а й потужною зброєю, що здатна формувати громадську думку, впливати на політичні процеси й навіть визначати результати виборів. Саме тому питання захисту інформаційного простору Європейського Союзу (ЄС) набуло стратегічного значення, адже воно безпосередньо пов'язане з безпекою громадян, держав-членів та інституцій Союзу. Зокрема, події останніх років, серед яких кібератаки на критичну інфраструктуру, спроби втручання у виборчі процеси, дезінформаційні кампанії, спрямовані на послаблення єдності ЄС, засвідчили необхідність системної та колективної відповіді на подібні виклики. Варто зазначити, що інформаційна безпека нині розглядається не лише у військово-політичному, а й у соціально-комунікативному вимірі, адже саме через інформаційні потоки відбувається формування європейської ідентичності, довіри до інститутів влади та підтримки спільних цінностей. Водночас, у сучасних умовах розвитку штучного інтелекту, масового збору даних та інтернету речей перед ЄС постають нові ризики, пов'язані з кіберзлочинністю, приватністю особистої інформації та маніпуляцією даними. У зв'язку з цим особливого значення набуває удосконалення європейських стратегій кібербезпеки, зміцнення співпраці між державами-членами та створення ефективних механізмів реагування на загрози. Отже, дослідження проблеми інформаційної безпеки Європейського Союзу є надзвичайно актуальним, адже від рівня її забезпечення залежить не лише технологічна стійкість Європи, а й майбутнє демократичних цінностей, прав людини та міжнародного впливу ЄС у глобальному вимірі.

Ступінь вивченості теми є доволі значною, проте дослідницький інтерес до неї продовжує зростати у зв'язку з еволюцією цифрових технологій,

гібридних загроз та необхідністю оновлення нормативно-правових механізмів захисту даних. У працях вітчизняних і зарубіжних науковців простежується багатовимірність підходів до трактування сутності та механізмів забезпечення інформаційної безпеки. Зокрема, Голуб'як Н. та Голуб'як І. [1] визначають гібридні загрози як ключовий виклик безпековій політиці ЄС, наголошуючи на їхньому впливі на політичну стабільність і суспільну довіру. Дрига Д. [3] аналізує правові механізми функціонування інформаційної інфраструктури Союзу. Подібної позиції дотримується і Кавин С. [4], яка підкреслює роль гармонізації національних законодавств держав-членів у сфері кібербезпеки. У свою чергу, Прудникова О. [10; 11] комплексно досліджує сучасні виклики інформаційній безпеці ЄС, серед яких виокремлює дезінформаційні кампанії, кібератаки та політичні маніпуляції. Значний внесок у розробку теоретичних аспектів зробила Милосердна І. [8], розглядаючи інформаційну безпеку як складову національної безпеки та індикатор рівня демократичності суспільства. Зарубіжні науковці, такі як Бендєк і Портела [17], Мядзвєцкая і Вессель [20], а також Шмітц-Берндт і Коул [22], зосереджуються на питаннях кібердипломатії, зовнішньої політики ЄС у сфері цифрової безпеки та узгодженості регуляторної бази. Нарешті, дослідження Нолте, Ратейке та Фінк [21] демонструють інтеграцію вимог кібербезпеки в Акт додо штучного інтелекту ЄС, що свідчить про міжгалузевий підхід. Наукове осмислення теми поступово переходить від загальнотеоретичного рівня до практико-нормативного, охоплюючи як внутрішній, так і зовнішньополітичний вимір інформаційної безпеки ЄС. Подальші дослідження мають зосередитися на інтеграції технологічного, правового та соціального аспектів інформаційної безпеки, що дозволить створити більш цілісну та ефективну модель захисту інформаційного простору ЄС.

Мета дослідження – визначити інструменти забезпечення інформаційної безпеки Європейського Союзу в сучасних умовах.

Завдання дослідження:

– визначити поняття та структуру інформаційної безпеки в системі міжнародних відносин;

– розкрити роль Європейського Союзу у сфері глобальної та регіональної безпеки;

– виявити гібридні загрози та зовнішні інформаційні впливи на ЄС;

– визначити роль інституцій ЄС у забезпеченні інформаційної стійкості та нормативно-правове регулювання інформаційної безпеки ЄС;

– з’ясувати особливості співпраці ЄС із державами-членами та міжнародними партнерами у сфері інформаційної безпеки та інструменти протидії сучасним гібридним інформаційним загрозам ЄС;

– виокремити проблеми імплементації стратегічних документів ЄС у сфері інформаційної безпеки та напрями вдосконалення політики інформаційної безпеки ЄС та її значення для України.

Об’єкт дослідження – інформаційна безпека в міжнародних відносинах

Предмет дослідження – інформаційна безпека Європейського Союзу в умовах сучасних гібридних загроз і зовнішніх впливів.

Теоретико-методологічна база дослідження ґрунтується на поєднанні системного, структурно-функціонального, інституційного та порівняльного підходів. Саме системний підхід дозволяє розглядати інформаційну безпеку як цілісну, багаторівневу систему, що охоплює політичні, правові, технологічні та соціальні аспекти. У свою чергу, структурно-функціональний метод сприяє з’ясуванню взаємодії між інституціями ЄС, такими як Європейська комісія, Європейська служба зовнішніх дій та Агентство з кібербезпеки (ENISA) у процесі формування єдиної політики безпеки інформаційного простору. Крім того, використання інституційного підходу дозволяє визначити роль норм і регламентів, що закріплюють засади спільної інформаційної політики в межах Союзу. Порівняльний метод, своєю чергою, допомагає оцінити досвід держав-членів у протидії гібридним загрозам і кібератакам, а також виявити спільні тенденції та розбіжності у підходах до захисту цифрового суверенітету. Теоретичну основу становлять концепції національної та колективної безпеки,

доктрина «цифрового європейського суверенітету» та сучасні теорії міжнародних відносин, зокрема неореалізм, неолібералізм і конструктивізм, які пояснюють логіку поведінки ЄС у сфері інформаційної безпеки.

Інформаційна база дослідження охоплює широкий спектр джерел, що забезпечують комплексне розуміння сутності, структурних елементів та практичних аспектів функціонування інформаційної безпеки в межах ЄС. Передусім, до неї належать офіційні документи Європейського Союзу, зокрема Стратегія кібербезпеки ЄС, Європейська стратегія безпеки даних, рішення Ради ЄС та директиви Європейського парламенту, що регулюють питання цифрової безпеки, захисту персональних даних і протидії дезінформації. Важливе місце посідають аналітичні звіти Європейської служби зовнішніх дій, Європейської комісії та агентства ENISA, які висвітлюють актуальні тенденції й виклики у сфері інформаційної політики. Крім того, використано статистичні матеріали Євростату, дані Європейського центру боротьби з кіберзлочинністю, а також щорічні звіти НАТО і Ради Європи, що дозволяють простежити співпрацю ЄС із міжнародними партнерами. Значну цінність мають наукові публікації у фахових зарубіжних і українських виданнях, зокрема наукові статті, присвячені питанням інформаційного суверенітету, гібридних загроз, протидії пропаганді та розвитку цифрової дипломатії. До інформаційної бази також включено монографії провідних дослідників з міжнародної безпеки, офіційні виступи представників Європейської комісії, матеріали міжнародних конференцій, а також актуальні публікації провідних аналітичних центрів. У сукупності ці джерела створюють надійну емпіричну основу для глибокого аналізу політики Європейського Союзу у сфері інформаційної безпеки та визначення перспектив її подальшого розвитку в умовах глобальної цифрової трансформації.

Практичне значення отриманих результатів полягає в тому, що вони можуть бути використані для вдосконалення системи захисту інформаційного простору як на рівні ЄС, так і в межах окремих держав-членів. Зокрема, результати дослідження сприяють глибшому розумінню механізмів протидії

гібридним загрозам, дезінформації та кібератакам, що набули масштабного характеру у зв’язку з російсько-українською війною. Крім того, робота має практичне значення для розробки стратегічних документів у сфері кібер- та інформаційної безпеки. Водночас отримані висновки можуть бути корисними для формування національної політики України у сфері інформаційної безпеки, зокрема в контексті гармонізації законодавства з європейськими нормами. Практична цінність полягає також у можливості застосування результатів дослідження. у навчальному процесі Харківського національного університету імені В.Н. Каразіна та інших вищих навчальних закладів для підготовки навчальних курсів, практичних занять дисциплін з міжнародних відносин, європейської безпеки та інформаційних технологій у сфері політики, за програмами підготовки магістрів міжнародних відносин, суспільних комунікацій та регіональних студій.

Апробація дослідження була здійснена у вигляді публікації тез наукової доповіді для участі у Всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (м. Харків, 21 листопада 2025 р.), на тему: «Instruments for Implementing the European Union’s Information Security».

Структура роботи. Кваліфікаційна робота магістра складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічує 85 найменувань. Загальний обсяг роботи становить 85 сторінок, з яких основного тексту – 75 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

1.1. Поняття та структура інформаційної безпеки в системі міжнародних відносин

Інформаційна безпека є однією з ключових категорій сучасних міжнародних відносин, адже в епоху глобальної цифровізації саме інформація стала стратегічним ресурсом, порівнюваним із нафтою чи енергією XX століття [12]. Під поняттям інформаційна безпека розуміють стан захищеності інформаційного простору держави, міжнародних організацій чи окремих акторів від внутрішніх і зовнішніх загроз, що забезпечує стабільність політичних, економічних та соціальних процесів [2]. У контексті міжнародних відносин інформаційна безпека набуває міждержавного виміру, адже інформаційні потоки не знають кордонів, а отже, будь-яка загроза чи кібератака одразу має транснаціональний ефект. Становлення поняття інформаційної безпеки пов’язане з появою нових технологій у другій половині XX століття. Уже в 1970-1980-х рр., у період початку комп’ютеризації, провідні держави світу почали усвідомлювати, що дані можуть бути не менш важливими, ніж військові ресурси. Після закінчення «холодної війни» інформація перетворилася на інструмент впливу у політичній, економічній і культурній сферах. Саме в цей час у науковий обіг активно входить поняття інформаційна війна, що означає використання інформації для досягнення стратегічних цілей без застосування зброї [6]. У сучасних умовах інформаційна безпека визначається як здатність суб’єктів міжнародних відносин ефективно захищати власний інформаційний простір, гарантувати достовірність, доступність і цілісність інформації, а також протидіяти інформаційним впливам. Відповідно до визначень, що пропонуються у працях українських та зарубіжних дослідників, інформаційна безпека охоплює як технічні аспекти (кіберзахист, шифрування, кіберрозвідку), так і гуманітарні, пов’язані з комунікацією, свідомістю, медіа та культурою [17].

Структура інформаційної безпеки багаторівнева. Її можна розглядати у трьох вимірах: національному, регіональному та глобальному. На національному рівні йдеться про внутрішні механізми держави, спрямовані на захист критичної інформаційної інфраструктури, персональних даних громадян, державної таємниці, а також на забезпечення інформаційного суверенітету. Регіональний рівень передбачає координацію міждержавних дій, прикладом є політика ЄС щодо кібербезпеки, втілена у Стратегії кібербезпеки ЄС 2020 року, що стала відповіддю на зростання кібератак та дезінформаційних кампаній, зокрема з боку РФ [34]. Нарешті, глобальний рівень включає міжнародне співробітництво в рамках ООН, НАТО, ОБСЄ та інших структур, які формують загальні норми поведінки у кіберпросторі. З точки зору структури, інформаційна безпека складається з кількох взаємопов'язаних елементів. По-перше, це інституційний елемент, який включає державні органи, міжнародні організації, аналітичні центри, що відповідають за моніторинг, прогнозування та реагування на інформаційні загрози. Наприклад, у ЄС діє Європейське агентство з кібербезпеки (ENISA), засноване у 2004 році, що координує політику кіберзахисту між країнами-членами [13]. По-друге, правовий елемент охоплює нормативно-правові акти, конвенції, угоди, що регулюють інформаційну діяльність і визначають відповідальність за кібератаки. Одним із ключових документів у цій сфері стала Будапештська конвенція про кіберзлочинність 2001 року, до якої приєдналися понад 60 держав світу [7]. По-третє, важливим складником є технологічний елемент, що забезпечує технічні можливості для захисту інформаційних систем: шифрування, кіберрозвідка, захист від вірусних атак, моніторинг трафіку. Наприклад, після масштабних кібератак WannaCry у 2017 році та NotPetya у 2017 році (яка, за оцінками експертів, була спрямована проти України, але завдала шкоди понад 60 країнам), питання кіберзахисту стало пріоритетним для більшості держав світу [29]. Нарешті, гуманітарно-комунікаційний елемент охоплює протидію дезінформації, пропаганді, маніпуляціям у соціальних мережах і формування критичного мислення

громадян. У цьому контексті важливу роль відіграють програми з медіаграмотності, які активно підтримуються в межах ЄС та Ради Європи [4].

Слід зазначити, що інформаційна безпека не може існувати ізольовано, вона є складовою ширшої системи національної та міжнародної безпеки. Як наголошує В. Новицький, інформаційна безпека – це індикатор стабільності держави, її здатності протистояти гібридним викликам і маніпуляціям свідомістю громадян [14]. Звідси випливає необхідність розглядати інформаційну безпеку як комплексне явище, що включає політичні, правові, економічні та культурні аспекти. У міжнародному вимірі інформаційна безпека має двоїсту природу. З одного боку, це сфера співпраці, адже держави зацікавлені у зменшенні ризиків кіберзлочинності, терористичних загроз та порушення конфіденційності. З іншого – це поле конфронтації, у якому ведеться боротьба за вплив, перевагу в інформаційному просторі, домінування у наративах. Доказом цього стала масштабна інформаційна війна між РФ та Заходом, яка розгорнулася після 2014 року й особливо загострилася з початком повномасштабного вторгнення РФ в Україну у 2022 році [38].

Показовим прикладом взаємозв'язку інформаційної безпеки необхідно міжнародних відносин є створення у 2017 році в межах НАТО Центру передового досвіду стратегічних комунікацій у Ризі (STRATCOM COE). Його метою є підвищення спроможності союзників у сфері інформаційної протидії, виявлення фейкових кампаній та розробка стратегій комунікаційної стійкості [44]. Подібні ініціативи вказують на те, що інформаційна безпека стала не лише технічним, а й політичним інструментом – елементом «м'якої сили», який дозволяє державам впливати на міжнародну громадську думку. Особливого значення набуває і концепція інформаційного суверенітету, що означає право держави контролювати власний інформаційний простір. Країни, такі як Китай або РФ, трактують її доволі жорстко, обмежуючи зовнішні інформаційні впливи та встановлюючи контроль над інтернетом. Натомість у ЄС чи США наголос робиться на балансі між безпекою та правами людини [15]. Ця відмінність підкреслює, що структура інформаційної безпеки тісно

пов’язана з політичними режимами, культурними традиціями та рівнем демократичного розвитку. Не можна оминути увагою і роль приватного сектору в забезпеченні інформаційної безпеки. Компанії, такі як Microsoft, Google та інші, є не просто бізнес-структурами, а фактичними акторами міжнародних відносин, які впливають на баланс сил у кіберпросторі [51]. Наприклад, саме компанія Microsoft у 2022 році першою публічно повідомила про серію кібератак, спрямованих проти українських державних структур напередодні російського вторгнення.

У контексті структури інформаційної безпеки доцільно виділити ще один рівень – нормативно-етичний, що включає міжнародні принципи використання інформації. Спроби створити універсальні правила поведінки в кіберпросторі робляться з початку 2000-х років. ООН, починаючи з 2004 року, періодично створює Групи урядових експертів (UN GGE), які розробляють рекомендації щодо відповідальної поведінки держав у цифровому середовищі [34]. Інформаційна безпека як категорія міжнародних відносин має також соціально-психологічний вимір. Йдеться про те, як інформаційні потоки впливають на суспільну свідомість, формування наративів, довіру до інституцій [35]. Отже, інформаційна безпека – це не лише про технічний захист даних, а про стійкість суспільства до маніпуляцій і здатність держави діяти в умовах інформаційного тиску. Її структура включає нормативно-правовий, інституційний, технологічний, гуманітарний, соціально-психологічний та міжнародний рівні. Кожен із них взаємодіє з іншими, формуючи цілісну систему безпеки у глобальному інформаційному середовищі [6].

Водночас, як слушно зазначає Н. Голуб’як, сучасні гібридні загрози дедалі більше стирають межу між війною та миром, політичним і технологічним, реальним і віртуальним [1]. У результаті інформаційна безпека перетворюється на постійний процес адаптації до змінних умов – від технологічних інновацій до нових форм політичного впливу. Це означає, що структура інформаційної безпеки не є сталою, вона динамічно змінюється відповідно до розвитку інформаційного суспільства [12].

У сучасній системі міжнародних відносин дедалі більшої ваги набуває ще один важливий компонент структури інформаційної безпеки – економічний вимір, що охоплює вплив інформаційних технологій на розвиток національних економік, фінансову стабільність та інвестиційну привабливість держав. Зрештою, кіберінциденти можуть мати катастрофічні економічні наслідки: прикладом є атака NotPetya 2017 року, збитки від якої для світової економіки, за оцінками компанії Maersk та низки експертних центрів, перевищили 10 млрд доларів. Особливої ваги цей аспект набуває в умовах того, що економіка XXI століття дедалі активніше мігрує у цифрові формати [67]. То ж захист фінансових транзакцій, банківських систем та біржових платформ є життєво важливим для підтримання глобальної економічної стабільності. У цьому сенсі необхідно згадати і про роль міжнародних економічних організацій. Наприклад, Світовий банк та МВФ систематично включають питання цифрової стійкості та інформаційної безпеки у свої рекомендації державам, особливо тим, що проходять процеси трансформації чи постконфліктного відновлення. Наявність надійної системи кіберзахисту часто є однією з умов формування позитивного інвестиційного клімату, адже міжнародний бізнес прагне гарантій збереження комерційної таємниці та захисту інтелектуальної власності [22].

Так само вагомим елементом структури інформаційної безпеки є наративний компонент, адже, як відомо, у міжнародних відносинах важливо не лише те, що відбувається, а й те, як це подається світовій аудиторії. Держави створюють власні інформаційні наративи, що відображають їхню офіційну позицію, цінності та стратегічні інтереси. Наприклад, США активно просувають наративи про свободу інтернету, прозорість і відповідальність цифрових платформ. Натомість Китай формує наратив про «цифровий суверенітет», наголошуючи на праві держави самостійно регулювати інформаційний простір. Європейський Союз, зі свого боку, підкреслює важливість балансування між інноваціями, безпекою та правами людини [38]. Варто зазначити, що конкуренція наративів стала важливою складовою

геополітичної боротьби останнього десятиліття. Саме через інформаційні інструменти держави конкурують за вплив на глобальну аудиторію, формують міжнародний імідж та підтримують власні дипломатичні позиції. Для України це питання стало особливо критичним після 2014 року і, безперечно, набуло ще більшого значення після 24 лютого 2022 року. З посиленням російської агресії питання формування українського наративу про спротив, суверенітет, європейську інтеграцію та міжнародну солідарність стало ключовим у структурі національної інформаційної безпеки [4].

Окремої уваги потребує військовий аспект інформаційної безпеки, що тісно переплітається з концепціями гібридної війни та військово-інформаційних операцій. Практика останніх десятиліть доводить, що сучасні конфлікти супроводжуються масштабними кампаніями з дезінформації, психологічним тиском на військовослужбовців, використанням технологій радіоелектронної боротьби та кібератак на стратегічні об’єкти. У 2015-2016 роках Україна стала об’єктом кібератак на енергомережу, що призвели до масштабних відключень електроенергії, і це був один із перших задокументованих випадків успішної кібератаки на критичну інфраструктуру [26]. Відтак, військово-інформаційний компонент включає захист військових комунікацій, стійкість до психологічних операцій противника, протидію витоку даних, а також створення власного стратегічного комунікаційного потенціалу. Як показує досвід НАТО, ефективна інформаційна політика є такою ж важливою, як і традиційна оборонна стратегія. Саме тому Альянс з 2016 року визнав кіберпростір повноцінним театром воєнних дій, прирівнявши кібернапад до збройного нападу згідно зі статтею 5 Північноатлантичного договору [33].

Ще одним не менш значущим елементом структури інформаційної безпеки є культурно-ціннісний компонент, що охоплює питання збереження культурної ідентичності, мови, ціннісних орієнтирів та історичної пам’яті. У глобалізованому світі, де інформаційні потоки перетинають кордони зі швидкістю світла, культурна безпека стає невід’ємною частиною

інформаційної. Адже маніпуляції історичною пам’яттю, перекручення фактів, нав’язування альтернативної історичної інтерпретації можуть призвести до внутрішньої дестабілізації держав. Яскравим прикладом є російська практика «історичної війни», спрямованої не лише на виправдання власної зовнішньої агресії, а й на підрив єдності суспільств західних держав. Саме тому ЄС з 2015 року активно підтримує діяльність East StratCom Task Force, яка спеціалізується на викритті дезінформаційних наративів Кремля [35].

Слід наголосити на важливості медіаграмотності як елементу структури інформаційної безпеки. Адже, якими б ефективними не були державні механізми захисту, без підготовленого суспільства вони залишатимуться неповними. Високий рівень медіаграмотності дає змогу громадянам відрізняти достовірну інформацію від фейків, зменшує вразливість до маніпуляцій і робить суспільство більш стійким. Прикметно, що Фінляндія, яка сьогодні вважається однією з найбільш інформаційно стійких держав, ще з 2014 року впровадила масштабну національну програму з медіаосвіти, яка охоплює школи, університети та органи місцевої влади [85]. У сфері міжнародних відносин медіаграмотність також є важливою, адже вона визначає рівень стійкості держави до зовнішніх впливів, а також формує здатність оцінювати інформаційні потоки в контексті геополітичних реалій. У цьому сенсі інформаційна безпека виступає інструментом підтримання демократичної стабільності та формування зрілого громадянського суспільства.

Підсумовуючи, можна стверджувати, що структура інформаційної безпеки в системі міжнародних відносин є багатовимірною та динамічною. Вона не обмежується технічними аспектами кіберзахисту, а включає інституційний, правовий, технологічний, наративний, економічний, військово-інформаційний та культурно-гуманітарний компоненти. Кожен з них виконує свою роль, однак лише їхня взаємодія створює цілісну систему, здатну гарантувати ефективний захист інформаційного простору. У сучасному світі, де інформаційний фактор дедалі частіше визначає хід політичних подій, інформаційна безпека стає ключовою детермінантою стабільності,

міжнародної довіри та глобальної взаємодії. І саме тому вивчення її структури та сутності є визначальним для розуміння того, як функціонує сучасна система міжнародних відносин.

1.2. Європейський Союз як актор у сфері глобальної та регіональної безпеки

Європейський Союз упродовж останніх десятиліть поступово трансформувався з переважно економічного угруповання на повноцінного актора у сфері глобальної та регіональної безпеки, причому ця еволюція відбувалася не одномоментно, а як результат численних політичних, інституційних та стратегічних рішень [24]. Водночас ця еволюція ґрунтується на переконанні європейських держав, що безпека континенту та, ширше, світового порядку не може забезпечуватися виключно національними зусиллями. Саме тому, починаючи з Маастрихтського договору 1992 року, ЄС послідовно формує власну Спільну зовнішню та безпекову політику (СЗБП), яка, зрештою, стала фундаментом для створення Загальної політики безпеки та оборони (ЗПБО). Протягом 2000-х років, особливо після ухвалення Європейської безпекової стратегії 2003 року, відбулося розширення інструментів, що дозволили Союзу не лише реагувати на кризи, а й виконувати так звані «місії з підтримання миру» та інші види операцій, зокрема цивільні та військові [25]. Показовим є те, що ЄС, хоча й не є військовим блоком у класичному розумінні, активно використовує інструменти миротворчості, кризового менеджменту та дипломатичного посередництва. Наприклад, операція «Аталанта», започаткована у 2008 році для боротьби з піратством біля узбережжя Сомалі, стала важливим символом того, що ЄС здатний проєктувати стабільність за межі власних кордонів. Подібним чином, місії ЄС з підтримання верховенства права в Косові (EULEX Kosovo) та спостережна місія в Грузії, створена після війни 2008 року, продемонстрували готовність Євросоюзу відігравати активну роль у стабілізації найближчого сусідства. До речі, саме регіональне оточення: Східна Європа, Західні Балкани, Кавказ і,

значною мірою, Близький Схід є зонами, де ЄС найчастіше виступає як безпековий актор, адже нестабільність тут безпосередньо впливає на внутрішню політичну ситуацію в державах-членах [81].

З іншого боку, важливо підкреслити, що Європейський Союз, попри значні зусилля у сфері оборони, вибудовує свою безпекову ідентичність передусім через поєднання «м'якої сили», правових механізмів і дипломатії. Саме таке поєднання дозволяє ЄС відігравати роль «нормативної сили», тобто актора, що поширює стандарти демократичного управління, поваги до прав людини та верховенства права. Не випадково політичні умови, висунуті ЄС щодо країн-кандидатів на членство, фактично виконують функцію довгострокового стабілізаційного інструмента. Історія розширення 2004 року, коли до Союзу приєдналися десять держав Центральної та Східної Європи, наочно демонструє, що політика умовності здатна трансформувати посткомуністичні суспільства, роблячи їх більш стійкими до загроз і конфліктів. У цьому контексті ЄС виступає не лише як споживач безпеки, а як виробник стабільності у регіоні [70]. Однак із середини 2010-х років, коли світовий порядок став менш передбачуваним, а гібридні загрози більш системними, Європейський Союз був змушений переглянути власні стратегічні підходи [1]. Ухвалення Глобальної стратегії ЄС у 2016 році стало відповіддю на нові виклики, серед яких російська агресія проти України, терористична активність на Близькому Сході, міграційні кризи та активізація авторитарних держав у світовій політиці [19]. Відповідно до цієї стратегії, ЄС окреслив такі ключові пріоритети, як зміцнення стійкості сусідніх регіонів, розвиток оборонного потенціалу, розширення партнерств і формування «європейської стратегічної автономії». Останнє поняття, до речі, стало предметом інтенсивних наукових дискусій, адже воно передбачає здатність ЄС діяти незалежно, або принаймні з меншою залежністю від США, особливо у сфері оборони [24].

Не можна оминути увагою створення Постійного структурованого співробітництва (PESCO) у 2017 році. На його основі держави-члени

започаткували понад 60 проєктів у сфері оборонних спроможностей, від кібербезпеки до військової мобільності [13]. Хоча критики зауважують, що багато з цих проєктів просуваються повільно, сам факт їх запуску свідчить про безпрецедентну готовність ЄС будувати власну оборонну інфраструктуру. Тим більше, що паралельно функціонує Європейський оборонний фонд, який, починаючи з 2021 року, став фінансовою основою для інновацій у сфері оборонних технологій. Попри це, Європейський Союз продовжує опиратися на співпрацю з НАТО, адже саме Альянс залишається головним гарантом колективної оборони в Європі. Проте співвідношення між НАТО та ЄС не зводиться до конкуренції; радше йдеться про взаємодоповнюваність. Наприклад, ЄС активно займається забезпеченням кіберстійкості, боротьбою з дезінформацією та захистом критичної інфраструктури – сферами, де військові інструменти НАТО можуть бути недостатньо ефективними без підтримки цивільних механізмів [26]. Розслідування втручань у виборчі процеси у державах-членах після 2016 року, а також координація санкційної політики проти РФ після 2014 і особливо після 2022 року демонструють, що ЄС значною мірою взяв на себе відповідальність за формування спільної відповіді на гібридні загрози [38].

Особливою точкою відліку стала повномасштабна агресія РФ проти України у 2022 році. Саме вона, по суті, змусила Європейський Союз перейти від переважно дипломатичного реагування до активної підтримки держави, що стала жертвою агресії. Рішення про створення Європейського фонду миру, за рахунок якого ЄС фінансує постачання летального озброєння Україні, стало безпрецедентним [24]. Ніколи раніше Союз не фінансував поставок зброї у воєнні зони такої інтенсивності. Варто додати, що протягом 2022-2024 років ЄС не лише ухвалив більше десятка пакетів санкцій проти РФ, а й започаткував програму макрофінансової допомоги Україні, спрямовану на зміцнення економічної та інституційної стійкості. Однак роль ЄС як актора безпеки не обмежується військовими чи фінансовими аспектами. Передусім він залишається глобальним лідером у сфері регуляції цифрового простору,

захисту персональних даних та протидії дезінформації [4]. Прийняття Загального регламенту про захист даних (GDPR) у 2018 році, а також цифрових актів, Digital Services Act і Digital Markets Act, створили глобальні стандарти, які сьогодні впливають на діяльність технологічних компаній у всьому світі [66]. Такий підхід, відомий під назвою «Брюссельський ефект», є, фактично, інструментом забезпечення безпеки через право, оскільки підвищення прозорості, регулювання платформ та боротьба з маніпуляціями інформацією зменшують ризики гібридних атак [35].

У світлі цих трансформацій дедалі більшого значення набуває інституційна архітектура ЄС у сфері безпеки, оскільки вона фактично визначає здатність Союзу реагувати на кризи та координувати дії між державами-членами. Створення посади Високого представника ЄС із закордонних справ та політики безпеки, а також Європейської служби зовнішніх дій (ЄСЗД) у 2010 році значно зміцнило дипломатичний потенціал Союзу. Відтоді ЄСЗД виступає ключовим координатором зовнішньої політики, забезпечуючи злагодженість між позиціями держав-членів, діяльністю зовнішніх місій та участю ЄС у міжнародних організаціях [58]. До речі, ЄС має статус спостерігача в ООН, бере активну участь у роботі ОБСЄ й співпрацює з Африканським Союзом і Лігою арабських держав, що свідчить про його зростаючу дипломатичну присутність. Потрібно наголосити й на тому, що Євросоюз посилює свою роль у сфері економічної безпеки, яка нині стала невіддільною від загальної системи міжнародної безпеки [24]. Після 2020 року особливу увагу було приділено питанням енергетичної незалежності, диверсифікації постачання критичних ресурсів та зменшенню залежності від авторитарних держав у стратегічно важливих секторах. Прийняття Європейського акту про чіпи у 2023 році, спрямованого на розвиток власного напівпровідникового виробництва, продемонструвало прагнення ЄС забезпечити технологічний суверенітет. Крім того, після енергетичної кризи, спричиненої російським вторгненням в Україну, Союз значно прискорив перехід на відновлювані

джерела енергії та запровадив обмеження на імпорт російських енергоносіїв, що є важливим кроком у зміцненні внутрішньої стійкості.

Цікаво, що роль ЄС як безпекового актора дедалі частіше проявляється у сфері кіберстійкості та захисту цифрового інформаційного простору [13]. Після низки атак на критичну інфраструктуру держав-членів, зокрема кібератаки на парламент Фінляндії у 2020 році, ЄС ініціював посилення співпраці між національними кіберцентрами та започаткував Європейський центр компетенцій у сфері кібербезпеки [65]. Боротьба з дезінформацією, серед іншого, здійснюється через діяльність East StratCom Task Force, яка від 2015 року документує й аналізує операції російської пропаганди, спрямовані проти Європи [4]. Саме ці інструменти дозволяють ЄС бути важливим гравцем у сфері інформаційної безпеки, що, без перебільшення, є однією з ключових складових сучасної геополітики [38]. У регіональному вимірі особливої уваги заслуговує політика ЄС щодо країн Східного партнерства. Україна, Молдова та Грузія, попри різні траєкторії взаємодії з Євросоюзом, перебувають у зоні його стратегічних інтересів. ЄС, використовуючи різні інструменти, від Угод про асоціацію до програм безвізової лібералізації, стимулює реформи, сприяє економічному розвитку та підтримує демократичні інститути. У випадку України це набуло особливого значення після 2014 року й, безперечно, після 2022 року. Відповідно до рішень Європейської Ради від 2022 року, Україна отримала статус кандидата на членство, що фактично закріпило роль ЄС як гаранта її довгострокової безпеки та стабільності [25]. Поступове розширення оборонної допомоги, санкційної політики та інвестицій у відбудову відіграє важливу роль у формуванні безпекової інфраструктури усього європейського простору.

Суттєвою є також діяльність ЄС у напрямку мирного врегулювання конфліктів у світі. Наприклад, активна участь Союзу у переговорах щодо іранської ядерної програми (JCPOA) у 2015 році стала тому свідченням. Європейські дипломати, виконуючи роль посередників, сприяли підписанню угоди між Іраном і країнами «P5+1», що тимчасово знизило напругу на

Близькому Сході. Хоча у 2018 році США вийшли з угоди, ЄС і надалі намагається зберегти її життєздатність, що демонструє його прагнення до стабілізації глобального безпекового середовища через дипломатію. Не менш важливими є миротворчі ініціативи в Африці: місії у Малі, Центральноафриканській Республіці та Нігері, попри складності, залишаються інструментами, що дозволяють ЄС діяти як глобальний стабілізатор [24]. Окрема увага має бути приділена концепції «європейської стратегічної автономії», яка стала одним із ключових елементів дискурсу щодо майбутнього ЄС [25]. Її прихильники стверджують, що Союз повинен мати можливість самостійно реагувати на кризи, не покладаючись виключно на зовнішніх партнерів. Проте критики наголошують, що надмірна автономізація може поставити під загрозу трансатлантичні відносини, які є фундаментом європейської безпеки ще від часів Другої світової війни. Ця дискусія залишатиметься актуальною й надалі, особливо в умовах глобальної конкуренції між США та Китаєм, а також через непередбачуваність політичних змін по обидва боки Атлантики.

Зрештою, важливо підкреслити, що Європейський Союз як актор у сфері глобальної та регіональної безпеки вирізняється саме своєю комплексністю. Він поєднує економічні можливості з дипломатичними ресурсами, цивільні інструменти з військовими, а регуляторний підхід із проактивною політикою у стратегічно важливих регіонах [19]. На тлі загострення геополітичної конкуренції, ескалації конфліктів та поширення гібридних загроз така модель безпекової поведінки має очевидні переваги. ЄС не лише реагує на загрози, а й формує нові стандарти безпеки, які можуть стати основою для стабільного світового порядку у майбутньому.

Зазначимо, що Європейський Союз уже давно перестав бути виключно економічним інтеграційним проєктом. Він став багатовимірним актором безпеки, здатним впливати на глобальні та регіональні процеси через поєднання військових, політичних, економічних, правових та ціннісних інструментів. Його здатність формувати порядок денний, підтримувати

партнерів, реагувати на кризи й забезпечувати стабільність у сусідніх регіонах підтверджує, що ЄС дедалі більше наближається до статусу стратегічного актора в умовах швидких трансформацій міжнародної системи. Водночас, з огляду на зростання загроз і конкуренції між великими державами, Євросоюз і надалі зіштовхуватиметься з викликами, що вимагатимуть посилення внутрішньої солідарності, диверсифікації інструментів і прагматичного поєднання стратегічних амбіцій із реальними оборонними спроможностями. Проте, як показує досвід останніх років, ЄС уже продемонстрував готовність до такої еволюції, і це робить його одним із ключових чинників безпеки у сучасному світі.

1.3. Гібридні загрози та зовнішні інформаційні впливи на ЄС

Гібридні загрози та зовнішні інформаційні впливи на Європейський Союз у сучасних умовах постають одними з ключових викликів, що безпосередньо визначають ефективність функціонування європейської системи безпеки та стійкість політичних процесів всередині Союзу [1]. Хоча концепція гібридності не є новою, саме після 2014 року, а особливо після повномасштабного вторгнення Росії в Україну 24 лютого 2022 року, вона набула якісно іншого змісту, адже поєднання військових методів, кібератак, інформаційних операцій, енергетичного тиску, економічного шантажу та використання міграційних потоків стало невід’ємною частиною європейської реальності [26]. У зв’язку з цим ЄС вимушений адаптувати власні підходи, роблячи акцент на формуванні системи багаторівневої стійкості та удосконаленні механізмів реагування на інформаційно-психологічні впливи. При цьому, як показує практика останніх років, інформаційний компонент гібридних загроз є не лише допоміжним фактором, а й окремим центром стратегічного тиску, що здатний підривати єдність, політичну волю та демократичні процедури в державах-членах.

Серед найпомітніших проявів гібридних загроз варто виділити масштабні кампанії дезінформації, спрямовані на делегітимацію рішень

інституцій ЄС, дискредитацію підтримки України, розкол суспільств щодо санкційної політики та підживлення радикальних наративів. Такі кампанії, як свідчать звіти Європейської служби зовнішніх дій (зокрема EUvsDisinfo за 2023-2024 роки), найчастіше походять із РФ, хоча останнім часом дедалі активніше фіксується присутність прокитайських, іранських та інших недружніх інформаційних акторів [37]. Наприклад, упродовж 2023 року аналітики ЄС зафіксували понад 3500 випадків поширення російських дезінформаційних меседжів, спрямованих на формування образу ЄС як «внутрішньо слабкого» та «політично залежного» утворення [38]. Подібні впливи, з одного боку, спрямовані на створення атмосфери недовіри до офіційних інституцій, а з іншого – на посилення внутрішніх конфліктів, які можуть ускладнити процеси ухвалення рішень у питаннях оборони, енергетики чи санкцій. Особливо показовими стають випадки втручання у виборчі процеси, що, своєю чергою, є однією з найбільш чутливих сфер демократичної системи. Напередодні виборів до Європейського парламенту 2024 року ЄС зафіксував активізацію зовнішніх впливів, які спрямовувалися на підтримку крайніх політичних рухів та послаблення центристських сил. Використання ботоферм, створення фальшивих новинних платформ, застосування генеративного ШІ для імітації відео та аудіозаписів кандидатів стало особливо небезпечним, оскільки, фактично, стерло межу між реальністю та цифровою симуляцією [71].

Не менш відчутним для ЄС є кібернетичний вимір гібридних впливів. Попри формальне розділення інформаційної безпеки та кібербезпеки, сучасні загрози дедалі більше поєднують ці сфери [13]. Кібератаки на державні установи, енергетичні компанії, транспортну інфраструктуру та медіаплатформи стають інструментом не лише технічного порушення роботи систем, а й каналом для поширення маніпулятивного контенту. Наприклад, атаки групи Sandworm на енергетичні об’єкти Польщі та Німеччини у 2023 році мали чіткий політичний підтекст, адже відбувалися паралельно з дезінформаційними кампаніями про «енергетичну неефективність»

європейської моделі та «кризу європейської підтримки України» [30]. З огляду на це Європейський Союз активно переглядає стратегічні підходи до забезпечення інформаційної безпеки. Прийняття у 2022-2023 роках «Європейського акту про цифрові послуги» (DSA), «Акту про кіберстійкість» (CRA) та оновлення «Стратегії з протидії іноземному втручанню» значною мірою сформували нову нормативно-правову рамку, що дозволяє регулювати діяльність платформ, підвищувати відповідальність великих онлайн-компаній та посилювати моніторинг зовнішніх інформаційних впливів [66; 69]. DSA, зокрема, впроваджує обов'язковість оцінки ризиків для дуже великих онлайн-платформ (VLOP), що передбачає аналіз дезінформаційних кампаній, маніпулятивної реклами та ризиків, пов'язаних зі штучним інтелектом [3].

Поряд із правовими інструментами ЄС розвиває інституційну інфраструктуру протидії гібридним загрозам. Однією з найбільш ефективних ініціатив сьогодні є діяльність Центру з протидії гібридним загрозам у Гельсінкі (Hybrid CoE), який надає аналітичну та методичну підтримку державам ЄС та НАТО [46]. Крім того, Європейська служба зовнішніх дій суттєво посилила власну систему інформаційного моніторингу, запустивши в 2024 році нові інструменти аналізу впливових операцій, зокрема ті, що використовують штучний інтелект для виявлення координованих маніпулятивних мереж [45]. Зовнішні інформаційні впливи посилюються також через використання соціальних мереж, що давно стали політичним інструментом. У цьому контексті показовою є діяльність TikTok, який, за даними Європейського парламенту, у 2023-2024 роках став одним із найбільших каналів поширення проросійських і прокитайських наративів серед молодіжної аудиторії [37]. Окрему у вагу слід приділити використанню міграційної тематики як інструменту інформаційного тиску. Кризи 2015 року, події на польсько-білоруському кордоні у 2021-2022 роках, а також повторне загострення у 2023 році показали, що міграційний фактор активно експлуатується для створення паніки, посилення ксенофобських настроїв та підриву довіри до європейських гуманітарних політик [48]. Таким чином,

фізична дія доповнювалася інформаційною, створюючи комплексний гібридний вплив [19].

Водночас важливо наголосити, що гібридні загрози, спрямовані проти Європейського Союзу, не існують у вакуумі: вони тісно пов'язані з глобальними трансформаціями міжнародної системи та зміною балансу сил [1]. Адже, як свідчить досвід останнього десятиліття, держави-ревізіоністи дедалі активніше застосовують інформаційні інструменти як невід'ємну частину своєї зовнішньої політики. РФ, Китай, Іран та низка інших акторів прагнуть не лише дестабілізувати політичні процеси в державах ЄС, а й переформатувати інформаційний простір таким чином, щоб він сприяв їхнім стратегічним інтересам у Європі. З огляду на це ЄС вимушений діяти не тільки як об'єкт, що захищається, а й як суб'єкт, який активно формує власну політику інформаційної стійкості. Слід також зазначити, що сучасні зовнішні інформаційні впливи дедалі частіше маскуються під легітимні форми комунікації, що значно ускладнює їх ідентифікацію. Наприклад, у 2023-02024 роках у країнах Балтії та Центральної Європи спостерігалося поширення мережі псевдоаналітичних сайтів, що видавали себе за незалежні медіа, але фактично поширювали фабриковані матеріали про «економічну втому від підтримки України» чи «зниження ефективності санкцій проти РФ» [37]. Характерно, що такі сайти нерідно використовували локальну мову, регіональний контент і навіть посилалися на вигаданих експертів, що створювало ілюзію достовірності. Цей формат інформаційної інфільтрації демонструє, наскільки стратегічно важливим для ЄС стає розвиток власних аналітичних та верифікаційних інструментів, зокрема платформ типу EDMO (European Digital Media Observatory), що поєднують журналістів, науковців та фактчекерів у спільному моніторинговому просторі [4].

Разом з тим технологічні зміни, зокрема поширення генеративного штучного інтелекту, надають зовнішнім акторам нові можливості для маніпулювання аудиторіями. У 2024 році ЄС вперше зафіксував масове використання deepfake-відео, спрямованих проти окремих кандидатів на

виборах, включно зі створенням відео-симуляцій, у яких політики нібито робили дискримінаційні або антиміграційні заяви [38]. Цей феномен став настільки поширеним, що Єврокомісія була змушена розробити окремі рекомендації щодо маркування ШІ-контенту та ведення кампаній у цифровому середовищі. Проблема ускладнюється тим, що не всі платформи рівною мірою реагують на загрози: наприклад, X (Twitter) після зміни політики модерації у 2023 році знизила рівень видалення маніпулятивних матеріалів на 30 %, що створило додаткові ризики для інформаційної безпеки ЄС [37]. Важливо врахувати і той факт, що зовнішні інформаційні впливи часто мають горизонтальний характер, охоплюючи не лише політичну сферу, а й енергетичну, економічну та соціальну системи ЄС. Яскравим прикладом є інформаційні кампанії, спрямовані проти європейської «зеленої» політики. Упродовж 2022-2024 років РФ та пов’язані з нею мережі активно просували наративи про «неефективність» зеленої трансформації, «високу залежність ЄС від імпорту енергії» та «зростання тарифів через підтримку України» [36]. Мета цих кампаній – підірвати довіру до європейської енергетичної стратегії та стимулювати політичні сили, які виступають проти санкцій або за відновлення співпраці з РФ. Таким чином, дезінформація перетворюється на інструмент впливу на стратегічні сфери європейської політики.

Крім того, гібридні загрози проявляються через економічний тиск. У 2023-2024 роках у низці держав-членів були зафіксовані цілеспрямовані спроби іноземних акторів проникнути в критично важливі галузі, від телекомунікацій до логістики, під прикриттям інвестиційної діяльності [61]. Європейська комісія неодноразово попереджала про ризики, пов’язані з придбанням стратегічних підприємств компаніями, які фактично контролюються урядами третіх країн. Зокрема, у 2023 році ЄС заблокував угоду щодо придбання німецького виробника напівпровідників однією з китайських корпорацій, посилаючись на загрозу безпеці ланцюгів постачання. Важливо те, що подібні дії супроводжуються паралельними інформаційними кампаніями, що мають на меті показати ЄС як «неконкурентоспроможний» або

«надмірно бюрократизований» ринок. Це поєднання економічного й інформаційного тиску є типовим елементом сучасних гібридних стратегій [19].

Суттєвим викликом для ЄС залишається питання інформаційної стійкості суспільств, адже навіть найбільш розвинені механізми регулювання та моніторингу не можуть бути повністю ефективними без активної участі громадян. У цьому контексті особливого значення набувають освітні програми з медіаграмотності, які ЄС намагається послідовно впроваджувати починаючи з 2018 року [35]. За даними Єврокомісії, у 2024 році понад 40 % держав-членів інтегрували елементи медіаграмотності у шкільні програми, а також створили національні центри цифрової освіти. Проте рівень стійкості суспільств залишається нерівномірним: наприклад, згідно з дослідженням Eurobarometer 2024 року, понад 30 % громадян ЄС не можуть відрізнити правдиву новину від маніпулятивної, що робить їх вразливими до зовнішніх впливів. Саме тому у 2024 році ЄС запустив нову ініціативу «Пакет демократичної стійкості» (Democracy Resilience Package), спрямовану на посилення незалежності медіа, прозорість політичної реклами та захист виборчих процесів [38]. Вона включає комплекс заходів: від підвищення стандартів безпеки для журналістів до створення механізмів захисту від іноземного фінансування партій та громадських організацій. Інакше кажучи, ЄС намагається будувати системну модель протидії гібридним впливам, що охоплює як нормативно-правові інструменти, так і суспільно-освітні механізми [48].

Загалом ситуація, що склалася, демонструє, що інформаційна безпека Європейського Союзу перетворюється на стратегічний вимір загальної безпекової політики Союзу. У сучасних умовах гібридні загрози діють комплексно, поєднуючи інструменти впливу на політичні процеси, суспільні настрої, економічну та енергетичну стійкість [15]. Тому для ЄС критично важливо розбудовувати сучасну систему багаторівневої інформаційної стійкості, здатну не лише реагувати на загрози, а й передбачати їх. У цьому сенсі нинішня стратегія ЄС спрямована на формування збалансованого підходу, який поєднує нормативні акти, інституційні механізми, технологічні

інновації, кібербезпекові рішення та розвиток критичного мислення серед громадян.

У підсумку, гібридні загрози та зовнішні інформаційні впливи на Європейський Союз формують складне середовище, у якому ключовими елементами є стратегія стійкості, інтеграція інституційних механізмів, технологічні інновації та нормативно-правові заходи. Інформаційна безпека ЄС у сучасних умовах уже не може спиратися на традиційні підходи, адже загрози стають дедалі комплекснішими, швидшими і технологічно оснащенішими. Тому ЄС, фактично, формує нову парадигму інформаційної безпеки – парадигму, в якій запорукою ефективності є не лише захист, а й здатність адаптуватися, передбачати та нейтралізувати загрози ще до того, як вони набудуть політичної або безпекової критичності.

Висновки до розділу 1

Висновки до розглянутих аспектів дають змогу узагальнити ключові положення. Насамперед слід підкреслити, що поняття та структура інформаційної безпеки в системі міжнародних відносин формуються під впливом зростаючої цифровізації, еволюції засобів комунікації та появи нових форм зовнішнього втручання. Інформаційна безпека, у сучасному розумінні, є не лише сукупністю інструментів захисту інформаційного простору, а й комплексною політичною, нормативно-правовою та технологічною системою, що забезпечує стійкість держав і міжнародних організацій до інформаційних загроз. Водночас структура цього феномена постійно ускладнюється, адже, як відомо, взаємозалежність глобальної інфраструктури породжує нові вразливості, а отже, й нові виклики.

Зазначимо, що Європейський Союз, у свою чергу, виступає одним з ключових акторів у сфері глобальної та регіональної безпеки, що, власне, зумовлено його інституційною потужністю, економічною вагою та нормативним впливом. ЄС поступово формує власну модель забезпечення інформаційної безпеки, поєднуючи інструменти кіберзахисту, стратегічних

комунікацій і регуляторних механізмів. Більш того, саме Євросоюз став одним із перших міжнародних об’єднань, яке, реагуючи на сучасні трансформації, інтегрувало питання інформаційної безпеки до широкого спектра зовнішньополітичних і безпекових стратегій. У цьому контексті важливо зазначити, що його роль зміцнюється завдяки розвитку партнерств із державами-членами та третіми країнами, а також активізації взаємодії з НАТО.

Разом із тим гібридні загрози та зовнішні інформаційні впливи залишаються одними з найнебезпечніших чинників, що значною мірою визначають вразливість інформаційного середовища ЄС. Зрештою, гібридні атаки, дезінформаційні кампанії й маніпулятивні технології дедалі інтенсивніше застосовуються як інструменти геополітичного тиску. З огляду на це Європейський Союз вимушений посилювати координацію у сфері стратегічних комунікацій, розширювати можливості моніторингу інформаційних потоків та вдосконалювати нормативно-правові механізми протидії. Сукупно це дозволяє зробити висновок, що ефективна інформаційна безпека ЄС можлива лише за умови системного підходу, який поєднує інституційну спроможність, інноваційні технології та політичну єдність.

РОЗДІЛ 2. ІНСТРУМЕНТИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

2.1. Нормативно-правове регулювання інформаційної безпеки ЄС

Нормативно-правове регулювання інформаційної безпеки ЄС сформувалося як багаторівнева система, що поєднує норми первинного права, акти вторинного законодавства, м'яке право та повноваження спеціалізованих агентств. У широкому розумінні інформаційна безпека в ЄС включає як захист мереж і інформаційних систем від кібератак, так і охорону персональних даних, цілісність демократичних процесів, протидію дезінформації та регулювання цифрових платформ. На рівні установчих договорів ключовими є положення про захист фундаментальних прав і свобод: Хартія основних прав ЄС гарантує право на повагу до приватного життя і захист персональних даних (статті 7 і 8) та свободу вираження поглядів і отримання інформації (стаття 11). Саме напружена рівновага між цими цінностями й безпековими інтересами Союзу визначає логіку подальшого галузевого нормотворення, зокрема в кібербезпеці, цифрових послугах та регулюванні штучного інтелекту [13]. Важливим історичним етапом стала поява Директиви NIS 2016 року, однак російська агресія проти України, зростання кількості кібератак на критичну інфраструктуру показали, що початкові рамки є недостатніми [51]. У відповідь у грудні 2022 року була ухвалена Директива (ЄС) 2022/2555, відома як NIS2, яка з 27 грудня 2022 року замінила попередню Директиву 2016/1148 і запровадила більш жорсткі вимоги до кібербезпеки в 18 секторах – від енергетики й транспорту до систем охорони здоров'я та цифрової інфраструктури [27]. Зокрема, NIS2 поширює коло «суттєвих» та «важливих» суб'єктів, встановлює мінімальні стандарти управління ризиками, детальні правила звітування про інциденти та гармонізує санкційні режими, що є принциповим кроком до створення справжнього «цифрового внутрішнього ринку безпеки» [3]. Передбачено, що держави-члени завершать транспозицію та почнуть повномасштабне застосування цих норм у період 2024–2025 років,

а це означає істотну модернізацію національних стратегій інформаційної безпеки та міждержавної координації.

Паралельно ЄС розбудовує інституційну основу кібербезпеки. Регламент (ЄС) 2019/881, відомий як Cybersecurity Act, надав Європейському агентству з кібербезпеки (ENISA) постійний мандат, посилив його роль як центру експертизи та координації реагування, а також запровадив рамкову систему добровільної сертифікації кібербезпеки ІКТ-продуктів, послуг і процесів на рівні Союзу [13]. У перспективі ця система стає дедалі більш пов'язаної з обов'язковими вимогами NIS2, що поступово переводить сертифікацію з площини рекомендацій у площину фактичної регуляторної необхідності, особливо для операторів критичної інфраструктури.

Не менш важливим елементом правового регулювання інформаційної безпеки є сфера онлайн-платформ і посередницьких послуг. У серпні 2023 року та протягом 2024 року поетапно набули чинності положення Регламенту про цифрові послуги (Digital Services Act, DSA), який заклав нові зобов'язання для онлайн-посередників, хостинг-провайдерів та особливо «дуже великих онлайн-платформ» і пошукових систем з аудиторією понад 45 млн користувачів у ЄС [66]. DSA спрямований на створення безпечнішого цифрового середовища, уточнення відповідальності платформ за незаконний і шкідливий контент, запровадження прозорих механізмів скарг, заборону певних форм таргетованої реклами, зокрема щодо дітей, та вимог до оцінки системних ризиків, пов'язаних із дезінформацією, поляризацією чи загрозами громадському порядку. Важливим доповненням до DSA у сфері захисту інформаційного простору від маніпуляцій є підсилений Кодекс практики щодо дезінформації. Початковий Кодекс 2018 року мав характер добровільної саморегуляції платформ, але вже в червні 2022 року, у відповідь на зростання загроз, пов'язаних із пандемією, повномасштабною агресією РФ проти України та масштабними кампаніями впливу, був ухвалений посилений варіант Документа з 44 зобов'язаннями та 128 конкретними заходами [80]. Після

набуття чинності DSA частина положень Кодексу де-факто інтегрується в правову площину [4].

Новий вимір нормативно-правового регулювання інформаційної безпеки ЄС пов'язаний зі стрімким розвитком штучного інтелекту та його впливом на інформаційне середовище. У 2024 році ЄС ухвалив Регламент (ЄС) 2024/1689 про штучний інтелект (AI Act) – перший у світі комплексний акт, що встановлює ризик-орієнтовану систему регулювання AI. Уже 2 лютого 2025 року почали діяти перші заборони щодо «неприйнятних» практик. Хоча AI Act формально не є актом суто «кібербезпекової» політики, він безпосередньо впливає на інформаційну безпеку, встановлюючи вимоги до прозорості, управління даними, кіберстійкості – ілюстративно для систем загального призначення, які можуть використовуватися і для дезінформаційних кампаній, і для захисту від них [60]. Крім того, сучасна система правового забезпечення інформаційної безпеки ЄС тісно пов'язана з уже усталеними інструментами захисту персональних даних та електронних комунікацій. Загальний регламент про захист даних (GDPR) встановлює високі стандарти безпе ки обробки даних, обов'язок повідомляти про витоки та принципи «privacy by design», які згодом були інтегровані й у кібербезпекові документи [18]. Важливою тенденцією останніх років є те, що ЄС поступово відходить від фрагментарного підходу до більш комплексної та взаємопов'язаної системи, де NIS2, Cybersecurity Act, DSA, посилений Кодекс проти дезінформації, AI Act та пов'язані інструменти працюють як взаємодоповнювальні елементи [59].

У цьому контексті дедалі важливішою стає також зовнішньополітична складова нормативно-правового забезпечення інформаційної безпеки ЄС, адже сучасні загрози, як свідчить практика останніх років, здебільшого мають транскордонний характер. Від масштабних кібератак на енергетичні мережі й урядові установи до скоординованих кампаній дезінформації, що супроводжують виборчі процеси або міжнародні кризи, інформаційні виклики виходять далеко за межі національних кордонів і вимагають узгоджених дій держав-членів та партнерів. Саме тому, починаючи з 2017 року, ЄС активно

розвиває «дипломатичний інструментарій кібербезпеки» – рамки спільної дипломатичної відповіді на зловмисну кібердіяльність (EU Cyber Diplomacy Toolbox) [58]. Цей інструмент передбачає можливість застосування колективних дипломатичних, економічних і санкційних заходів проти суб'єктів, відповідальних за масштабні або системні кіберінциденти. Так, у 2020 році Союз уперше скористався цим механізмом, запровадивши санкції проти російських, китайських і північнокорейських хакерських груп, причетних до атак NotPetya, Cloud Hopper та WannaCry [51]. Ці рішення, як відзначають європейські аналітичні центри, стали важливим прецедентом інтернаціоналізації стандартів кіберповедінки, які ЄС прагне поширити на глобальному рівні.

Крім того, нормативно-правова система ЄС у сфері інформаційної безпеки не обмежується регулюванням кіберпростору як такого, а стосується також захисту демократичних процесів, що є однією з ключових складових інформаційного суверенітету. Після масштабних втручань РФ у вибори різних країн Заходу в період 2016-2020 років та під час російсько-української війни, Євросоюз значно посилив правові механізми запобігання зовнішнім впливам [37]. У 2023-2024 роках ЄС ухвалив низку рішень, спрямованих на обмеження дезінформаційної діяльності іноземних акторів та прозорість фінансування політичної реклами [4]. Водночас розробляються нові правила, які передбачають обов'язкове маркування політичних оголошень, розкриття джерел фінансування кампаній та перевірку відповідності контенту під час виборів стандартам достовірності та прозорості. Особливої актуальності ці ініціативи набули напередодні виборів до Європейського парламенту 2024 року, коли Єврокомісія та Європарламент неодноразово наголошували на загрозі іноземного втручання, включно з використанням deepfake-технологій та автоматизованих мереж ботів [71].

Суттєвим елементом нормативно-правової архітектури ЄС є також акти, спрямовані на зміцнення стійкості критичної інфраструктури. Регламент (ЄС) 2022/2557 про стійкість критично важливих суб'єктів (CER Regulation), який

діє паралельно з NIS2, встановлює вимоги не лише до кіберзахисту, а й до забезпечення фізичної безпеки об’єктів енергетики, транспорту, водопостачання, цифрової інфраструктури та інших секторів [19]. Ці два документи разом формують комплексну модель, у якій інформаційна та фізична безпека розглядаються як взаємопов’язані елементи єдиної системи.

Окремої уваги заслуговує співпраця ЄС із третіми країнами у сфері інформаційної безпеки, яка базується як на міжнародних угодах, так і на секторальних програмах підтримки. У 2022-2025 роках Євросоюз активно розширює партнерські програми зі США, Канадою, Японією, Південною Кореєю та Австралією, що охоплюють питання кіберстійкості, обміну інформацією про загрози, врегулювання інцидентів та стандартизації вимог до критичної інфраструктури [40]. Особливе місце посідає співпраця з Україною, яка, як справедливо визнається в документах Єврокомісії, перебуває на «передньому краї» гібридної війни та є цінним партнером у питаннях виявлення і протидії російським операціям впливу [10]. Після підписання Угоди про цифрову безпеку між Україною та ЄС у 2022 році відбувається систематичне зближення українського законодавства з європейськими нормами, включно з імплемента цією стандартів NIS2, DSA та кіберсертифікації. Не можна оминути й того, що ЄС поступово формує цілісну стратегічну рамку розвитку інформаційної безпеки. Стратегія кібербезпеки ЄС 2020 року, яка продовжує реалізовуватися до 2030 року, передбачає створення єдиного європейського кіберпростору з високим рівнем стійкості, зміцнення оборонного потенціалу, розвиток спільних центрів аналізу загроз і підвищення готовності до масштабних інцидентів [34]. Серед інституційних новацій варто виділити створення Європейського центру компетенцій з кібербезпеки (ECCC), який із 2023 року координує науково-дослідні та інноваційні проєкти у сфері кіберзахисту, а також розподіляє фінансування в рамках програм Digital Europe та Horizon Europe [65].

Водночас, попри значний прогрес, нормативно-правова система інформаційної безпеки ЄС залишається сферою дискусій та викликів. З одного

боку, гармонізація правил підвищує прозорість, безпеку та довіру користувачів до цифрових послуг, створює умови для стійкості критичної інфраструктури й стримує діяльність недобросовісних або ворожих акторів. З іншого, високий рівень регуляторних вимог викликає побоювання щодо надмірного адміністративного навантаження на бізнес, особливо серед малих і середніх підприємств [52]. Низка технологічних компаній також критикує EU-centric модель регулювання, вважаючи її занадто жорсткою та потенційно обмежувальною для інновацій.

У результаті зазначимо, що нормативно-правове регулювання інформаційної безпеки ЄС сьогодні перебуває в стані динамічної еволюції, що зумовлена одночасно зростанням кіберзагроз, геополітичними викликами, цифровою трансформацією економіки та суспільства, а також амбіціями Союзу задавати глобальні стандарти цифрового врядування. Від NIS2 і Cybersecurity Act, які формують «жорстке ядро» кібербезпеки, до DSA й посиленого Кодексу практики з протидії дезінформації, що регулюють інформаційний простір платформ, і до AI Act, який установлює правила для технологій, що дедалі більше визначають структуру цифрової публічної сфери, ми бачимо поступове оформлення цілісної, хоча й складної, правової екосистеми. Вона покликана не лише реагувати на конкретні інциденти чи кризи, а й превентивно зменшувати вразливості, підвищувати стійкість держав, бізнесу й громадян до інформаційних загроз, одночасно зберігаючи високі стандарти прав людини та демократичних процедур. Саме баланс безпеки, свободи та інновацій, який закладається в сучасних актах ЄС, визначатиме, наскільки ефективною й легітимною буде система інформаційної безпеки Союзу в найближче десятиліття.

2.2. Роль інституцій ЄС у забезпеченні інформаційної стійкості

Роль інституцій Європейського Союзу у забезпеченні інформаційної стійкості є однією з ключових складових сучасної архітектури європейської безпеки, адже саме вони формують стратегічні підходи, координують держави-

члени та забезпечують ефективну відповідь на дедалі складніші інформаційні загрози [15]. У XXI столітті, коли інформаційний простір став головним полем конкуренції держав, транснаціональних акторів і навіть приватних технологічних корпорацій, ЄС поступово формує власну модель багаторівневого реагування з чітким розподілом повноважень між інституціями. З одного боку, це дозволяє уникати дублювання функцій, а з іншого – забезпечує синергію зусиль у критично важливих сферах, зокрема у протидії дезінформації, гібридним операціям, кібератакам та зовнішньому маніпулюванню громадською думкою [19]. Передусім варто підкреслити, що Європейська комісія виступає центральним координатором політики інформаційної стійкості (Таблиця 1.). Саме вона ініціює стратегічні документи, розробляє нормативно-правові рамки та здійснює нагляд за їх виконанням. Показовим є ухвалення у 2022 році Європейського плану дій з протидії дезінформації, який, зокрема, офіційно визнав дезінформацію інструментом зовнішньополітичного впливу та загрозою демократичним процесам [4]. Комісія, до того ж, працює з такими технологічними платформами як Meta, Google чи TikTok, вимагаючи прозорості алгоритмів та запроваджуючи жорсткіші стандарти модерації. Від 2023 року, після набуття чинності Закону про цифрові послуги (DSA), платформи з понад 45 млн користувачів у ЄС зобов'язані проводити оцінку системних ризиків, серед яких: поширення дезінформації, маніпулятивна реклама, вплив іноземних акторів [66]. Ця норма, власне, посилила роль Єврокомісії як регулятора цифрового середовища.

Таблиця 2.1.

Роль інституцій ЄС у забезпеченні інформаційної безпеки

Інституція ЄС	Основна роль у забезпеченні інформаційної безпеки	Ключові інструменти та механізми
Європейська Рада	Визначає стратегічні пріоритети та політичні напрями розвитку	Стратегічний порядок денний; висновки щодо кібербезпеки; ініціювання створення

	кібер- та інформаційної безпеки ЄС.	нових політик та директив.
Європейська Комісія	Розробляє законодавчі ініціативи та координує політику цифрової й інформаційної безпеки на рівні ЄС.	Стратегії кібербезпеки (2020), Digital Services Act, Digital Markets Act, NIS2, програми фінансування Digital Europe.
Європейський Парламент	Законодавча підтримка політик та контроль за їх імплементацією; захист цифрових прав громадян.	Прийняття законів у сфері кібербезпеки; резолюції щодо дезінформації; Комітет LIBE.
ENISA (Агентство ЄС з кібербезпеки)	Провідний технічний орган, що забезпечує експертизу, стандарти та рекомендації щодо кіберзахисту й стійкості мереж.	Європейська сертифікація кібербезпеки, NIS2, звіти про загрози (Threat Landscape).
EEAS / StratCom East	Моніторинг, викриття та протидія дезінформації, особливо з боку РФ; стратегічні комунікації.	EUvsDisinfo, кампанії з медіаграмотності, аналітика інформаційних операцій.
Europol / EC3	Бореться з кіберзлочинністю, включно з атаками на критичну інформаційну інфраструктуру.	Європейський центр кіберзлочинності, спільні операції, обмін даними.
Європейська служба інтелектуальної власності (EUIPO)	Протидія онлайн-піратству, маніпуляціям та фейкам у сфері брендів та товарів.	Observatory on Infringements of IPR; системи моніторингу онлайн-контенту.
CERT-EU	Захищає інформаційні системи інституцій ЄС від кібератак.	Реагування на інциденти, управління кіберризиками, обмін оперативною інформацією.
Європейська прокуратура (EPPO)	Розслідує кіберзлочини, що пов’язані з шахрайством і фінансовими атаками проти бюджету ЄС.	Спільні слідчі групи, цифрова криміналістика.

Європейський суд справедливості (CJEU)	Формує правові стандарти захисту даних, конфіденційності та цифрових прав.	Судові рішення (Schrems I/II), тлумачення GDPR і цифрового законодавства.

Водночас важливу роль відіграє Європейська служба зовнішніх дій (ЄСЗД), яка забезпечує політичну та аналітичну складову інформаційної стійкості. Її спеціальний підрозділ East StratCom Task Force, створений у 2015 році після початку російської агресії проти України, здійснює моніторинг дезінформаційних кампаній, публікує щотижневі огляди неправдивих повідомлень та підтримує відкриту базу даних EUvsDisinfo, що на сьогодні містить понад 18 тисяч задокументованих кейсів [38]. У 2022-2024 рр. робота цієї групи значно посилилася через повномасштабне вторгнення РФ в Україну, різке зростання антизахідних наративів у країнах Східного партнерства та активізацію дезінформаційних кампаній Китаю щодо пандемії та глобального економічного порядку. Таким чином, ЄСЗД фактично стала центром аналітичної протидії зовнішнім інформаційним впливам.

Своєю чергою, Європейський парламент відіграє не менш значущу роль, адже саме він формує політичний порядок денний та впливає на вдосконалення законодавчої бази. Парламентські резолюції 2021–2023 років неодноразово наголошували на необхідності посилення незалежних медіа, підтримки журналістських розслідувань та впровадження стандартів прозорості онлайн-реклами. Крім того, прийняття у 2022 році Акта про свободу медіа (European Media Freedom Act) стало спробою створити єдиний європейський стандарт захисту журналістської діяльності [4].

Крім вищезгаданих інституцій, особливе значення мають Європейська рада та Рада ЄС, які визначають стратегічні пріоритети та ухвалюють рішення щодо санкцій, зокрема у відповідь на інформаційні атаки. Так, у 2022-2023 рр. Рада ЄС вперше застосувала механізм санкцій проти акторів, причетних до дезінформаційної діяльності [55].

Європейське агентство з кібербезпеки (ENISA), зі свого боку, зосереджується на технічному вимірі інформаційної стійкості. Його діяльність особливо активізувалася після ухвалення у 2022 році оновленої Директиви NIS2, яка розширила перелік критичних секторів та підвищила вимоги до кіберзахисту операторів критичної інфраструктури [27]. ENISA регулярно проводить тренінги, симуляційні навчання, здійснює моніторинг кіберінцидентів та готує річні звіти про кіберзагрози [30].

Не можна оминути увагою і Європейський центр передового досвіду з протидії гібридним загрозам у Гельсінкі, який, хоча і не є формальною інституцією ЄС, працює під егідою держав-членів та тісно співпрацює з європейськими структурами [26]. Особливо помітним цей внесок став після 2022 року, коли центр опублікував серію звітів про російські інформаційні операції.

Показовим також є те, що ЄС активно залучає до розбудови інформаційної стійкості країни-партнери, насамперед Україну та держави Східного партнерства [58]. Продовжуючи розгляд ролі інституцій ЄС у забезпеченні інформаційної стійкості, слід наголосити на посиленні міжінституційної координації, яка, фактично, стала фундаментом сучасної європейської моделі безпеки. Після початку повномасштабної агресії РФ проти України у 2022 році ЄС запровадив нову систему кризового реагування – механізм Integrated Political Crisis Response (IPCR) [24]. Завдяки цьому механізму у 2023-2024 рр. ЄС оперативно реагував на масовані дезінформаційні кампанії.

Не менш важливим є внесок Європейського суду справедливості (CJEU), який формує юридичні рамки функціонування цифрового ринку та онлайн-комунікацій. Його рішення у справах щодо захисту персональних даних, правових основ модерації контенту або балансування між свободою слова та безпекою мають безпосередній вплив на політику інформаційної стійкості [35].

Додатково варто звернути увагу на роль Європейського комітету регуляторів електронних комунікацій (BEREC), який забезпечує узгодженість правил для телекомунікаційних операторів, що має ключове значення для підтримання технічної цілісності інформаційного простору [7]. BEREC, зокрема, розробляє рекомендації щодо мережевої безпеки, стежить за виконанням правил мережевого нейтралітету та координує діяльність національних регуляторів у сфері електронних комунікацій. У 2023 році BEREC виступив із роз'ясненнями щодо ризиків використання мережевого обладнання, потенційно пов'язаного з іноземними спецслужбами, що стало важливим елементом політики ЄС щодо зменшення залежності від небезпечних постачальників [13]. Суттєве місце в інституційній архітектурі інформаційної стійкості займає і Європейський фонд оборони (EDF), який, хоч і має військовий характер, фінансує низку проєктів з кіберзахисту та гібридної безпеки [1]. Зокрема, у 2023 році Фонд підтримав розробку нових систем виявлення гібридних атак, що поєднують аналіз кіберінцидентів із моніторингом інформаційних операцій. Це дозволяє ЄС використовувати інноваційні технології для раннього виявлення загроз та прогнозування їх можливого впливу на суспільство. Важливо й те, що EDF сприяє створенню єдиного європейського ринку оборонних технологій, що у перспективі допоможе зменшити залежність від зовнішніх постачальників і, відповідно, знизити ризики зовнішнього втручання [24].

У цьому контексті не можна оминути увагою і роботу Європейського омбудсмана, який забезпечує прозорість діяльності інституцій і контроль за дотриманням принципів відкритості [4]. Адже прозорість управління це один із ключових чинників довіри громадян до інституцій, а відтак і до здатності протистояти дезінформації. Омбудсман неодноразово наголошував, що приховування інформації або бюрократична закритість створюють сприятливе середовище для поширення неправдивих наративів, і тому розширення доступу громадян до офіційних даних є частиною стратегії боротьби з інформаційними загрозами. Крім того, ЄС дедалі активніше використовує

інструменти стратегічних комунікацій. У 2023-2024 рр. ЄСЗД, Єврокомісія та Європарламент запустили кілька спільних інформаційних кампаній, спрямованих на підвищення медіаграмотності та демаскування проросійських і проавторитарних наративів [38]. Наприклад, ініціатива #FactsMatter (2023) охопила понад 20 держав-членів і була спрямована на популяризацію перевірки фактів серед молоді. Такі кампанії, на перший погляд, мають просвітницький характер, але, по суті, є інструментом формування суспільної стійкості, найважливішого елемента загальної інформаційної безпеки [47].

У підсумку можна зазначити, що інституції Європейського Союзу формують багатовимірну систему забезпечення інформаційної стійкості, яка поєднує нормативне регулювання, оперативне реагування, технологічні інновації, стратегічні комунікації та міжнародну кооперацію. Ця система, хоча й залишається у процесі розвитку, вже сьогодні демонструє значну ефективність, особливо у контексті протидії гібридним загрозам, спрямованим проти ЄС та його партнерів. Власне, інформаційна стійкість перетворюється на самостійний вимір європейської безпеки, а роль інституцій перетворюється на ключовий ресурс у зміцненні демократичних цінностей та збереженні політичної стабільності в умовах глобальної конкуренції.

2.3. Співпраця ЄС із державами-членами та міжнародними партнерами у сфері інформаційної безпеки

Співробітництво ЄС у сфері інформаційної безпеки посідає ключове місце в архітектурі сучасної європейської та глобальної безпеки, адже інформаційний простір дедалі частіше стає полем стратегічного протиборства між державами, негласними акторами, транснаціональними корпораціями й мережами кіберзлочинності [1]. Упродовж останніх років, насамперед після подій 2014 року, які продемонстрували вразливість європейських демократій до зовнішнього втручання, ЄС послідовно формує багаторівневу систему взаємодії, що поєднує інституційні механізми, нормативно-правові інструменти та практичні форми співпраці. При цьому, що особливо важливо,

таке співробітництво ґрунтується на принципах солідарності, спільної відповідальності та колективної стійкості, які визначають не лише характер внутрішньої координації, а й формат взаємодії з зовнішніми партнерами, від США та Канади до країн Індо-Тихоокеанського регіону [19]. Насамперед варто зазначити, що координація між державами-членами ЄС у сфері інформаційної безпеки розвивається у межах комплексної системи, сформованої на основі таких документів, як Директива NIS (2016), її оновлена версія NIS2 (2022), Стратегія кібербезпеки ЄС 2020 року, а також рішення Ради ЄС щодо протидії гібридним загрозам [27; 34]. Ці документи, по суті, створили правову основу для гармонізації підходів до захисту критичної інфраструктури, підвищення стійкості державних інституцій та запровадження єдиних стандартів реагування на інциденти. Показовим є те, що NIS2, на відміну від первинної директиви, розширила перелік секторів, що підлягають кіберзахисту, включивши енергетику, транспорт, цифрові послуги, постачання води, виробництво медичних виробів, космічні технології тощо [13]. Це підсилює не лише індивідуальну стійкість окремих держав, а й колективну безпеку всього союзу.

Важливо й те, що інформаційна безпека неможлива без ефективної горизонтальної координації, тобто без взаємодії між державами-членами. У цьому контексті ключову роль відіграє Мережа CSIRTs, створена для обміну даними про кіберінциденти й загрози в режимі, наближеному до реального часу. Зокрема, у 2023-2024 роках, за даними Європейського агентства з кібербезпеки ENISA, обсяг інцидентів, пов’язаних із фішингом, атакою програм-вимагачів та компрометацією ланцюгів постачання, суттєво зріс [30], що вимагало оперативної взаємодії між національними командами швидкого реагування. Як наслідок, ЄС дедалі більше використовує механізми спільних тренувань, симуляцій («кіберполігонів») та колективних аудиторій стійкості, що створює умови для набуття державами-членами порівняного рівня підготовки. Попри це, роль Європейської служби зовнішніх дій, а також Центру передового досвіду з протидії гібридним загрозам у Гельсінкі (Hybrid

CoE), є не менш значущою. Саме ці інституції забезпечують стратегічну координацію дій у сфері протидії дезінформації, маніпулятивним кампаніям і зовнішнім впливам. Відомою є діяльність групи East StratCom Task Force, яка з 2015 року веде системний моніторинг російських інформаційних операцій, зокрема в межах платформи EUvsDisinfo [4]. У 2022–2024 роках значна увага приділялася інформаційним атакам, спрямованим на підрив підтримки України, дискредитацію санкційної політики ЄС, а також на посилення протестних настроїв у окремих країнах-членах [37]. З погляду безпекових підходів, таке системне викриття й документування агресивних інформаційних впливів є важливою частиною формування колективної стійкості.

Не менш важливо розглянути співпрацю ЄС із міжнародними партнерами. Передусім ідеться про трансатлантичний вимір, що традиційно відіграє вирішальну роль у формуванні безпекової політики Європи. Співпраця з НАТО у сфері інформаційної безпеки стала особливо динамічною після 2016 року, коли була ухвалена Декларація про співпрацю між ЄС та НАТО [77]. Зокрема, ідеться про спільні навчання з кіберзахисту, координацію механізмів раннього попередження та обмін розвідданими щодо гібридних загроз. Яскравим прикладом став спільний проєкт з підвищення стійкості критичної інфраструктури енергетичного сектору, який почав діяти у 2023 році у відповідь на атаки на європейські газопроводи та об’єкти електропостачання.

Крім того, ключовим партнером ЄС є США, з якими Євросоюз у 2021 році створив Раду з питань торгівлі та технологій (TTC). Один із напрямів діяльності цієї ради, координація заходів із протидії дезінформації та спільне регулювання великих платформ, включно з Facebook, YouTube, TikTok та X (Twitter) [40]. Варто зазначити, що співпраця у межах TTC значно активізувалася у 2023-2024 рр. через зростання загроз з боку іноземних впливів, особливо напередодні виборів до Європейського парламенту та президентських виборів у США. Окрему роль відіграє співпраця ЄС із партнерами з Індо-Тихоокеанського регіону. Наприклад, угоди з Японією (оновлені у 2022 році) передбачають спільні кроки з кіберзахисту критичних

секторів і розробку етичних стандартів для технологій штучного інтелекту. Пор яд із цим, ЄС активно розвиває програму EU Cyber Diplomacy Toolbox, що дозволяє застосовувати санкції проти держав та індивідів, причетних до значних кіберзагроз [58]. Так, у 2020-2023 рр. Євросоюз запровадив низку санкцій проти хакерських угруповань з Росії, Китаю, Північної Кореї та Ірану, що, власне, стало важливим сигналом щодо готовності ЄС застосовувати не лише політичні, а й юридичні інструменти впливу.

Не можна оминути увагою й східних партнерів ЄС, серед яких особливе місце посідає Україна. Після 2022 року співпраця у сфері інформаційної безпеки стала безпрецедентно глибокою, адже Україна перебуває на передовій боротьби з російською гібридною агресією [51]. ЄС підтримує Україну через такі інструменти, як EU Support Hub for Internal Security and Border Management, механізми захисту критичної інфраструктури, кіберекспертну допомогу та програми з протидії дезінформації. Зокрема, у грудні 2023 року Євросоюз виділив додаткові 25 млн. євро на зміцнення кіберстійкості українських державних інституцій, що є черговим підтвердженням стратегічного значення інформаційного партнерства між сторонами. Загалом Європейський Союз поступово формує багатошарову систему співпраці, де внутрішні та зовнішні виміри взаємно посилюють один одного [13]. З одного боку, ЄС прагне забезпечити рівномірну й ефективну координацію між державами-членами, підвищуючи їхню здатність протидіяти кіберзагрозам та дезінформації. З іншого боку, союз активно розвиває глобальну мережу партнерств, переконаний, що лише через колективні дії можна забезпечити достатній рівень стійкості в умовах постійно змінюваного та ускладненого інформаційного середовища [58].

У ширшому контексті важливо наголосити, що стратегічна синергія, яка формується між Європейським Союзом, його державами-членами та зовнішніми партнерами, сприяє поступовому виробленню глобальних норм та стандартів поведінки в інформаційному просторі. Адже, як свідчать події останнього десятиліття, інформаційні загрози дедалі більше набувають

транскордонного характеру, а тому жодна країна не здатна протистояти їм ізольовано. Власне, саме з цієї причини ЄС наполягає на розвитку міжнародної кібердипломатії та елементів «нормативної сили», що спрямовані на створення прозорих, передбачуваних і водночас юридично обов'язкових рамок регулювання цифрового середовища [38]. Показовим у цьому плані є активна позиція ЄС у перемовинах в межах ООН щодо відповідальної поведінки держав у кіберпросторі, а також його участь у формуванні Глобального цифрового договору (Global Digital Compact), що має бути ухвалений у 2025 р. [32]. Слід окремо підкреслити, що співпраця з міжнародними партнерами сприяє не лише зміцненню інформаційної безпеки, а й забезпеченню технологічного суверенітету ЄС. Наприклад, поглиблення партнерства з Південною Кореєю, яке було активізовано у 2022 р., дозволяє Євросоюзу отримувати доступ до передових рішень у сфері мікроелектроніки та захищених телекомунікацій, що є ключовим чинником у зниженні залежності від нестабільних або політично чутливих постачальників. З тієї ж причини ЄС активізував діалог із Австралією та Новою Зеландією щодо регулювання цифрових платформ і протидії дезінформації, оскільки ці держави, маючи схожі нормативні підходи, стають природними союзниками у формуванні «демократичного цифрового простору» [40].

У практичному вимірі важливо звернути увагу на механізми швидкого реагування, які ЄС розвиває разом із партнерами. Наприклад, у 2024 році в межах співпраці ЄС-США було створено оперативну групу для боротьби з іноземним втручанням у вибори (Election Interference Task Force), до якої увійшли експерти з Європолу, Європейської служби зовнішніх дій та американських структур DHS і CISA [71]. Ця група займається обміном розвідданими щодо інформаційних операцій, спрямованих на маніпулювання електоральними процесами, а також розробкою алгоритмів перевірки достовірності політичного контенту в соціальних мережах. Очевидно, що такі механізми є не лише технічними інструментами, а й важливим політичним сигналом про солідарність демократичних держав перед новими викликами.

У внутрішньоєвропейському контексті варто згадати про розвиток спільних центрів аналізу загроз, які об’єднують фахівців із різних держав-членів. Одним із них є Європейський центр компетенцій у сфері кібербезпеки, що розпочав роботу у 2023 році у Бухаресті [65]. Він покликаний координувати дослідницькі програми, спрямовані на підтримку технологічного розвитку в галузі штучного інтелекту, криптографії, квантових технологій та захисту критичної інфраструктури. У цьому контексті важливо зазначити, що ЄС дедалі активніше інвестує у створення мережі національних центрів компетенцій, які разом утворюють інтегровану систему обміну знаннями та дослідницькими результатами, тим самим забезпечуючи довгострокову стійкість союзу в інформаційній сфері.

Окремим напрямом є співпраця ЄС з приватним сектором, без якого сучасна інформаційна безпека є неможливою. По-перше, значна частина цифрової інфраструктури перебуває у приватній власності, що зумовлює необхідність постійного діалогу з компаніями-операторами цифрових платформ, телекомунікаційними корпораціями та виробниками програмного забезпечення. По-друге, саме приватні компанії володіють передовими технологіями, які можуть бути використані для раннього виявлення загроз. У цьому контексті важливим кроком стало впровадження Акту про цифрові послуги (DSA) та Акту про цифрові ринки (DMA), які набули чинності у 2023 році та встановили для великих онлайн-платформ обов’язок прозорості, відповідальності та співпраці з органами ЄС у сфері протидії дезінформації й шкідливому контенту [66]. Така взаємодія робить цифрове середовище більш безпечним і водночас відкриває нові можливості для регулювання поведінки глобальних технологічних гігантів. Якщо говорити про співпрацю із сусідніми державами, то варто згадати посилення діалогу між ЄС та країнами Західних Балкан. Протягом 2024 р. було реалізовано низку програм, спрямованих на зміцнення кіберстійкості Сербії, Північної Македонії та Чорногорії, зокрема через фінансування модернізації державних кіберцентрів та проведення тренінгів із протидії інформаційним впливам [17]. Це свідчить про те, що ЄС

розглядає своїх сусідів не лише як об’єкти політики розширення, а й як партнерів у створенні спільного простору безпеки.

Можна стверджувати, що співпраця ЄС у сфері інформаційної безпеки набуває комплексного, багатофункціонального й водночас стратегічного характеру. Вона включає не тільки захист від кіберзагроз і дезінформації, а й розбудову інституційної стійкості, розвиток технологічного потенціалу, формування глобальних норм поведінки у цифровому середовищі та інтеграцію партнерських держав у спільний простір стабільності. У сучасних умовах, коли інформаційний простір стає ключовим фактором політичної боротьби, економічної конкуренції та навіть військового протиборства, така співпраця має вирішальне значення для збереження демократичних цінностей, правопорядку та європейської моделі безпеки.

Висновки до розділу 2

У висновку варто підкреслити, що нормативно-правове регулювання інформаційної безпеки Європейського Союзу становить складну та багаторівневу систему, яка, утім, демонструє високу здатність до адаптації в умовах постійно змінюваних загроз. Передусім варто зазначити, що європейська модель регулювання ґрунтується на поєднанні загальноєвропейських актів, таких як Директива NIS2, Регламент про кібербезпеку та GDPR, із національними нормативними системами держав-членів. Саме ця взаємодія створює правове середовище, яке, хоча й залишається неоднорідним, проте забезпечує відносно високий рівень передбачуваності та узгодженості політик. Більше того, нормативна база ЄС виконує не лише регулятивну, а й стратегічну функцію, адже вона формує цілісне бачення пріоритетів Союзу у сфері інформаційної стійкості, включно з розвитком кіберзахисних спроможностей, протидією дезінформації та захистом критичної інфраструктури.

Поряд із цим, роль інституцій ЄС у забезпеченні інформаційної стійкості є ключовою та постійно зростає. Європейська служба зовнішніх дій, Європейська комісія, ENISA та спеціалізовані підрозділи, створені у відповідь на масштабні інформаційні атаки, нині фактично формують архітектуру оперативного реагування та стратегічного планування. Важливо й те, що інституції ЄС поступово переходять від фрагментарних підходів до моделі інтегрованої інформаційної безпеки, у межах якої пріоритет надається оперативності, міжвідомчій взаємодії та постійному моніторингу ризиків.

Нарешті, співпраця ЄС із державами-членами та міжнародними партнерами постає важливим фактором зміцнення інформаційної стійкості на глобальному рівні. З одного боку, тісна координація між країнами ЄС дозволяє оперативно реагувати на інциденти, гармонізувати законодавство та розвивати спільні технічні інструменти. З іншого, партнерства з НАТО, ООН, країнами «Великої сімки» чи демократичними державами Азійсько-Тихоокеанського регіону сприяють формуванню ширших механізмів колективної кібероборони.

РОЗДІЛ 3. СУЧАСНІ ПРОБЛЕМИ ТА НАПРЯМКИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

3.1. Інструменти протидії сучасним гібридним інформаційним загрозам ЄС

Останні десятиліття переконливо довели, що гібридні інформаційні загрози стали чи не найнебезпечнішим викликом для Європейського Союзу, оскільки вони поєднують у собі дезінформаційні кампанії, кібероперації, маніпулятивний вплив у соціальних мережах, зовнішнє втручання у демократичні процеси та навіть використання штучного інтелекту з метою підриву суспільної довіри [1]. Відповідно, ЄС, який традиційно ґрунтує свою діяльність на цінностях верховенства права, прав людини та відкритих демократичних інституцій, змушений був, зокрема після 2014 року і особливо після повномасштабного вторгнення РФ в Україну у 2022 році, сформувати комплексний набір інструментів протидії гібридним інформаційним загрозам [19]. У цьому контексті, як слушно зауважують сучасні дослідники, система реагування ЄС стала багаторівневою, динамічною та здатною до швидкої адаптації [26]. Передусім слід підкреслити, що одним із ключових інструментів ЄС у боротьбі з дезінформацією є створення спеціалізованих інституцій та аналітичних структур. Так, East StratCom Task Force, заснована у 2015 році в межах Європейської служби зовнішніх дій, стала фактично першою структурою, яка почала системно відстежувати та спростовувати дезінформацію, насамперед російського походження [4]. Її проєкт EUvsDisinfo, що регулярно публікує аналітичні огляди інформаційних атак, став важливим інструментом формування інформаційної стійкості як інституцій, так і громадськості. Водночас, починаючи з 2020 року, ЄС суттєво активізував співпрацю із соціальними платформами Facebook, X (Twitter), YouTube у рамках Кодексу практик щодо дезінформації. Цей документ, оновлений у 2022 році, включає розширені вимоги щодо прозорості політичної реклами, маркування бот-мереж та контроль над алгоритмічними рекомендаціями, що,

безумовно, є вагомим кроком у зменшенні впливу маніпулятивного контенту [80].

Однак, що особливо важливо, інструменти протидії гібридним загрозам не обмежуються лише реагуванням на дезінформаційні атаки. ЄС також посилює свої кіберзахисні можливості, адже, як показали численні інциденти 2017–2023 років (наприклад, атаки NotPetya 2017 року чи кібератаки на європейські інфраструктурні об'єкти у 2022–2023 роках), інформаційні та кіберзагрози є взаємопов'язаними [13]. У відповідь на це у 2019 році була ухвалена оновлена Кібербезпекова стратегія ЄС, що передбачає створення Європейського центру компетенцій з кібербезпеки (EU Cybersecurity Competence Centre), а також зміцнення ролі ENISA – Агентства ЄС з кібербезпеки [34]. Ці інституції координують зусилля держав-членів, бізнесу та наукових установ у створенні технологічних інструментів раннього виявлення атак, підвищенні кіберстійкості критичної інфраструктури та розвитку системи спільного реагування.

Важливим інструментом протидії гібридним інформаційним загрозам є й нормативно-правове регулювання. Наприклад, у 2022 році ЄС ухвалив Акт про цифрові послуги (Digital Services Act, DSA), який встановлює найжорсткіші у світі правила щодо модерації контенту, прозорості платформ та алгоритмічного управління [66]. Завдяки цьому документу великі цифрові компанії, зокрема Meta та Google, зобов'язані звітувати про роботу алгоритмів, видаляти виявлений шкідливий контент та боротися з координованою неавтентичною поведінкою. Більше того, у 2023 році Європейська комісія розпочала кілька розслідувань проти платформ за невиконання вимог DSA щодо запобігання поширенню прокремлівської дезінформації про війну в Україні [47].

Окремої уваги заслуговує також інструмент стратегічних комунікацій, що активно застосовується ЄС для формування стійкості не лише інституцій, а й громадян. У цьому напрямі важливою є діяльність трьох спеціалізованих команд StratCom: East, South та Western Balkans, кожна з яких відповідає за

моніторинг інформаційних загроз у своїх регіонах [36]. Наприклад, у 2023 році команда East опублікувала серію аналітичних звітів щодо маніпулятивних наративів про «втому Заходу» від підтримки України, що набули поширення у європейських медіа [38]. Паралельно з цим ЄС активно розвиває інструменти підтримки незалежних медіа та медіаграмотності. Зокрема, у 2021-2024 роках реалізовувалися програми EU Media Literacy Week, які були спрямовані на підвищення критичного мислення молоді та дорослого населення. Крім того, у межах програми Creative Europe фінансуються проєкти з розвитку якісної журналістики, що, безперечно, зміцнює внутрішній інформаційний простір [35]. Варто також згадати запуск European Newsroom у 2022 році, спільної редакційної платформи, яка об’єднує 20 національних інформаційних агентств ЄС і створює спільні стандарти інформування, особливо у кризових ситуаціях.

Дуже показовим є й розвиток санкційних механізмів, що стали важливим інструментом протидії інформаційним атакам. Починаючи з 2022 року, ЄС запровадив санкції проти російських державних та наближених до влади медіа: RT, Sputnik та ін. Заборона на мовлення цих ресурсів у межах Союзу мала на меті не цензуру, а захист інформаційного простору від і нструментів пропаганди, що використовувалися як зброя у гібридній війні [55].

До інструментів протидії гібридним загрозам, безумовно, належить і співпраця ЄС з державами-членами та міжнародними партнерами. У цьому контексті важливо згадати про Hybrid Fusion Cell – спеціальну структуру ЄС, що координує обмін інформацією про інциденти між країнами [24]. Крім того, ЄС активно співпрацює з НАТО, розвиваючи спільні механізми оцінювання гібридних ризиків [25]. Більше того, партнерство з Україною після 2022 року суттєво розширилось: українські спецслужби, відомі своєю ефективністю у протидії російським операціям впливу, активно діляться досвідом із відповідними структурами ЄС [51]. Отже, логіка розвитку інструментів протидії гібридним інформаційним загрозам ЄС засвідчує: система захисту повинна ґрунтуватися не лише на технологічних рішеннях чи нормативних регуляціях, але й на цілісному стратегічному баченні. Власне, ЄС дедалі

більше усвідомлює, що сучасна інформаційна війна – це не стільки про окремі атаки чи фейки, скільки про довготривале формування альтернативної реальності, спрямованої на підрив політичної єдності, демотивацію суспільств та створення атмосфери недовіри [36]. Саме тому у 2023 р. ЄС розпочав роботу над оновленою Європейською стратегією інформаційної стійкості, яка поєднує аналіз вразливостей, оцінку загроз та інструменти швидкого реагування [45]. У цьому документі, що наразі перебуває на стадії імплементації, акцент робиться передусім на необхідності синергії між державами-членами, інституціями Союзу та приватним сектором.

Важливою новацією останніх років стало використання штучного інтелекту для автоматичного виявлення та блокування шкідливих інформаційних впливів. Наприклад, у 2023 році Європейська комісія запустила пілотний проєкт AI4Trust, метою якого стало створення технологічних інструментів для виявлення фейкових відео, «діпфейків», бот-мереж та скоординованих кампаній у соцмережах [37]. Зрештою, ці інструменти вже використовуються під час аналізу інформації, що стосується війни в Україні, міграційних криз та виборів у ЄС, адже, як показує досвід, саме в періоди політичної напруги активізуються зовнішні інформаційні впливи. Європейський парламент у 2024 році ухвалив рекомендації щодо етичного використання ШІ для боротьби з дезінформацією, наголошуючи на необхідності уникати надмірного контролю над контентом та забезпечувати прозорість алгоритмів [38]. Крім того, у ЄС зростає розуміння, що протидія гібридним загрозам вимагає не лише технологічних та політичних заходів, а й формування відповідальної культури споживання інформації. У цьому сенсі розвиваються програми підтримки медіаграмотності для освітніх установ, журналістів, державних службовців та широкої громадськості. Наприклад, у 2024 році розширено мережу European Digital Media Observatory (EDMO), яка координує роботу незалежних фактчекінгових організацій, дослідницьких інститутів та університетів [4]. Ця мережа активно відстежує нові форми інформаційних маніпуляцій, а також надає рекомендації урядам країн ЄС щодо

підвищення стійкості суспільства до дезінформаційних впливів. У рамках EDMO також реалізуються освітні проєкти, спрямовані на підвищення критичної медіаграмотності серед учнів шкіл і студентів, що є надзвичайно важливим, адже саме молодь є найбільш активною у цифровому просторі.

У не менш важливому напрямі, зміцненні дипломатичної протидії, ЄС поступово формує мережу партнерств, які дозволяють обмінюватися даними про інформаційні загрози у реальному часі. У цьому контексті прикметним є створення у 2023 році EU-US Disinformation Working Group, що координує зусилля ЄС та США у протидії ворожим інформаційним впливам, насамперед з боку РФ і КНР [40]. Завдяки цьому механізму стало можливим швидше реагувати на дезінформаційні кампанії, спрямовані проти підтримки України, енергетичної політики або трансатлантичної єдності. До того ж ЄС активно розширює партнерство з країнами Східного партнерства, зокрема Україною, Грузією та Молдовою, проводячи спільні тренінги та обмінюючись методиками виявлення й аналізу інформаційних операцій [58].

Окремий блок інструментів пов’язаний зі зміцненням демократії та стійкості виборчих процесів. Після втручання у вибори в США (2016) та низці інформаційних атак під час виборів у Європі (наприклад, у Франції у 2017 році чи Німеччині у 2021 році) ЄС значно посилив свою нормативну базу. У 2023 році набули чинності нові правила щодо прозорості політичної реклами, які вимагають маркувати будь-який контент, що фінансується політичними акторами або третім іноземним суб’єктом [66]. Це дозволяє не лише ідентифікувати джерело впливу, але й оцінювати масштаби зовнішнього втручання. Паралельно, ЄС запустив Election Shield Mechanism, механізм моніторингу інформаційних ризиків у період виборів Європарламенту 2024 року, який виявляв фейки, спрямовані на дискредитацію кандидатів або створення міждержавних напружень [71].

Дуже важливою складо вою інструментарію ЄС стала й підтримка цифрової стійкості критичної інфраструктури, адже, як свідчать численні випадки 2022-2024 рр., кібератаки часто супроводжуються масованими

інформаційними кампаніями. Наприклад, атаки на енергетичні компанії у Польщі та Нідерландах у 2023 році супроводжувалися поширенням фейків про начебто «провину українських біженців» у цих інцидентах. Це ще раз доводить, що кібер- та інформаційні загрози діють у комплексі, а тому потребують синхронізованої відповіді. З цією метою у 2023 році ЄС ухвалив Network and Information Security Directive 2 (NIS2), яка підвищує вимоги до захисту систем в усіх ключових секторах, від транспорту та енергетики до охорони здоров'я [27].

У ширшій перспективі поглиблення інструментів протидії гібридним інформаційним атакам сприяє зростанню стратегічної автономії ЄС. Адже, як слушно зауважується у численних аналітичних звітах, інформаційна стійкість – це не лише захист від зовнішніх маніпуляцій, а й здатність формувати власний позитивний порядок денний [24]. Саме тому ЄС дедалі більше інвестує у власні комунікаційні можливості, формує глобальні наративи про цінності демократії, солідарності, верховенства права та підтримку України. Показовою у цьому контексті стала інформаційна кампанія «Stand with Ukraine», яку ЄС реалізував у 2023 р. у понад 40 країнах світу, демонструючи важливість міжнародної солідарності.

Підсумовуючи, слід підкреслити, що сучасні інструменти протидії гібридним інформаційним загрозам ЄС багаторівневі, взаємопов'язані та здатні до постійного розвитку. Вони охоплюють правові, інституційні, технологічні, освітні, дипломатичні та санкційні механізми, що разом формують комплексну систему інформаційної безпеки. І хоча загрози еволюціонують дедалі швидше, особливо з появою генеративного ШІ, здатного створювати складні моделі маніпулятивного контенту, ЄС демонструє гнучкість і стратегічну далекоглядність. У результаті інформаційна стійкість стає одним із ключових елементів європейської безпекової архітектури, без якого неможливо забезпечити демократичну стабільність, політичну цілісність та ціннісну єдність Союзу у сучасному глобальному середовищі.

3.2. Проблеми імплементації стратегічних документів ЄС у сфері інформаційної безпеки

Одна з ключових проблем імплементації стратегічних документів Європейського Союзу у сфері інформаційної безпеки полягає в тому, що, попри значний прогрес у нормотворчій діяльності, реальна практична реалізація положень цих документів суттєво відстає від темпів трансформації інформаційного середовища [13]. Спостерігається постійне наростання складності інформаційних загроз, і, відповідно, зростає потреба в більш оперативному та узгодженому впровадженні ухвалених стратегічних підходів. Так, прийняття у 2020 році Стратегії кібербезпеки ЄС створило нормативну основу для комплексного захисту цифрового простору [34], однак, як свідчить практика, деякі держави-члени не можуть повною мірою адаптувати національні законодавства до нових вимог, що, власне, і призводить до асиметрії у рівні інформаційної стійкості. З одного боку, країни з високим рівнем цифровізації, наприклад, Естонія чи Фінляндія, демонструють майже зразкове виконання норм ЄС; з іншого, держави з менш розвиненою цифровою інфраструктурою відчутно відстають, що створює «прогалини безпеки» в межах усього Союзу [39].

До того ж, імплементацію ускладнює фрагментованість національних підходів до формування системи кібер- та інформаційної безпеки. Як наслідок, навіть після ухвалення Директиви NIS2 у 2022 році, яка суттєво підвищила вимоги до стійкості критичної інфраструктури [27], виявилося, що частина держав-членів не має достатніх адміністративних і фінансових ресурсів для повного виконання її положень [52]. Крім того, в окремих країнах простежуються проблеми з інституційною координацією: компетенції між органами державної влади або дублюються, або, навпаки, розподілені надто розпорошено, що ускладнює реагування на інциденти та сповільнює впровадження рішень ЄС на національному рівні. Не менш актуальною залишається проблема кадрового забезпечення. Хоча Європейський Союз регулярно підкреслює важливість розвитку «цифрового суверенітету», а у

2023–2024 роках активно інвестує у програми підготовки фахівців з кібербезпеки, дефіцит кваліфікованих кадрів у багатьох державах-членах продовжує перевищувати попит [20]. Зрештою, брак спеціалістів негативно позначається на швидкості адаптації стратегічних документів ЄС у практичну площину, адже навіть найкраще розроблені нормативні акти потребують експертного супроводу та технічного забезпечення. Особливо це помітно в секторі охорони здоров'я, який після пандемії COVID-19 2020–2021 років став одним із головних об'єктів атак, однак так і не отримав у всіх країнах достатнього рівня кадрової підтримки для повноцінної реалізації вимог NIS2.

Водночас варто зазначити, що бар'єри імплементації пов'язані не лише з технічними або адміністративними чинниками, а й з політичними. У деяких державах-членах існує доволі обережне ставлення до поглиблення інтеграційних механізмів, особливо тих, що стосуються передачі частини національних повноважень у сфері безпеки на наднаціональний рівень [15]. Це, між іншим, ускладнює реалізацію таких стратегічних документів, як Європейський акт про кіберстійкість (Cyber Resilience Act), представлений Єврокомісією у 2022 році [69]. У низці парламентів виникли дискусії щодо того, чи не призведе імплементація Акту до надмірного втручання ЄС у внутрішні регулятивні процеси. Не менш важливою перешкодою є фінансова обмеженість. Хоча ЄС забезпечує значну підтримку в межах таких програм, як Digital Europe Programme чи Horizon Europe, виділених коштів, принаймні на практиці, часто не вистачає для одночасного модернізаційного прориву у всіх державах-членах [32]. У менших країнах, наприклад у Словаччині чи Болгарії, ресурси на розбудову сучасних кіберцентрів, підвищення стійкості мережевої інфраструктури або створення систем раннього виявлення загроз суттєво обмежені, що уповільнює реалізацію стратегічних орієнтирів ЄС.

Своєрідним викликом для імплементації стратегічних документів стала і стрімка поява нових технологій. Зокрема, широке впровадження штучного інтелекту після 2023 року створило нові форми загроз: генеративні системи здатні продукувати масштабовані дезінформаційні кампанії, deepfake-відео та

аудіо, що ускладнює верифікацію інформації та підриває довіру до демократичних процесів [38]. ЄС, безперечно, реагує на ці ризики через оновлення Кодексу практик щодо дезінформації (2022) та ухвалення Закону про штучний інтелект (AI Act) у 2024 році [80], але країни-члени стикаються з труднощами адаптації власного законодавства до цих вимог, особливо в частині регулювання високоризикових систем штучного інтелекту. Окремо слід згадати проблему гармонізації інформаційної взаємодії між інституціями ЄС і державами-членами. Попри створення у 2019 році Європейського центру компетенцій з кібербезпеки, а також мережі національних координаційних центрів [65], інформаційний обмін у сфері кіберінцидентів залишається недостатньо оперативним. Частина держав, керуючись міркуваннями національної безпеки, неохоче передає дані про серйозні порушення або атаки, що знижує ефективність спільного реагування [30]. Додатковою проблемою є відсутність єдиного стандарту оцінювання ефективності впровадження стратегічних документів. Хоча Єврокомісія регулярно проводить моніторинг національних планів імплементації, методи оцінювання відрізняються між державами-членами, що унеможливлює вироблення загальної системної картини [39]. Наприклад, модель централізованого управління кіберінцидентами, розроблена Естонією ще у 2021 році, могла б стати стандартом для всієї Європи, однак досі не інтегрована у загальносоюзний підхід через відмінності в адміністративних системах інших країн.

Продовжуючи аналіз, варто наголосити, що ще однією суттєвою проблемою імплементації стратегічних документів ЄС у сфері інформаційної безпеки є нерівномірність цифрового розвитку різних секторів економіки та суспільства [13]. Хоча стратегічні документи передбачають системний та інтегрований підхід, у реальній практиці захищеність публічного сектору значно перевищує рівень інформаційної безпеки приватних компаній, особливо середнього та малого бізнесу. Наприклад, дослідження Єврокомісії за 2023 рік показало, що понад 60 % малих підприємств ЄС не мають базової системи управління кіберризиками, хоча Директива NIS2 передбачає

поширення вимог на значно ширше коло суб’єктів [27]. Це означає, що нормативні положення не завжди знаходять реальне практичне підґрунтя, особливо коли йдеться про обмежені фінансові можливості бізнесу та його недостатню обізнаність щодо інформаційних загроз.

Крім того, серйозною перешкодою залишається питання управління дезінформацією та шкідливими інформаційними впливами з боку зовнішніх акторів. У стратегічних документах ЄС, зокрема у Плані дій щодо демократії 2020 року, окреслені чіткі механізми боротьби з іноземними інформаційними кампаніями [4]. Проте ефективність їх імплементації залежить, між іншим, від можливості держав-членів гармонізувати підходи до ідентифікації, класифікації та блокування дезінформаційних потоків. Як показали події перед виборами до Європарламенту 2024 року, держави-члени суттєво відрізнялися у здатності виявляти й нейтралізувати зовнішні інформаційні атаки, зокрема з боку РФ і Китаю [71]. В окремих країнах, таких як Чехія, були створені потужні центри протидії фейкам, тоді як інші члени ЄС залишилися майже незахищеними, що підкреслює нерівномірність імплементації загальноєвропейських стандартів [38]. До цього додається й проблема недостатньої стандартизації кіберінцидентів. Попри запуск у 2023 році Європейської платформи обміну даними про кіберінциденти, держави-члени часто користуються власними методологіями оцінки серйозності інцидентів, що ускладнює їх правильне категорування та подальший аналіз [30]. Як наслідок, стратегічні документи, що передбачають уніфікований підхід, стикаються з фрагментацією на практиці, що, зрештою, негативно впливає на швидкість та якість реагування на загрози.

Також варто згадати проблему регуляторного навантаження на бізнес. Ухвалення Закону про цифрові послуги (DSA) та Закону про цифрові ринки (DMA) у 2022 році значно посилило вимоги до інтернет-платформ [66], проте багато компаній, особливо середніх, поскаржилися на те, що вимоги до аудиту, модерації контенту та прозорості алгоритмів стали складними у виконанні без додаткової підтримки [52]. Більш того, великі корпорації: Meta, Google, TikTok,

нерідко мають свої уніфіковані глобальні стандарти, які не завжди точно відповідають регуляціям ЄС, а тому процес узгодження та адаптації може тривати роками. Останніми роками особливо виразною стала проблема так званої «інформаційної інерції», ситуації, коли стратегічні документи оновлюються швидко, але практична імплементація не встигає за появою нових технологій та нових загроз. Наприклад, уже у 2025 році стає очевидним, що документи ЄС, ухвалені у період 2020-2022 рр., недостатньо враховують нові виклики, пов'язані зі штучним інтелектом, квантовими обчисленнями та автоматизованими інформаційними операціями [39]. Відповідно, держави-члени стикаються з необхідністю одночасно впроваджувати старі й адаптуватися до нових стратегічних положень, що створює перевантаження системи.

Крім того, ускладнює імплементацію й різний рівень політичної волі в державах-членах. Деякі уряди розглядають інформаційну безпеку як стратегічний пріоритет, а інші – як другорядний напрям, що має менший політичний резонанс [15]. Це, звісно, створює асиметрії, які у стратегічних документах зовсім не передбачені, проте мають надзвичайно суттєві наслідки для створення єдиного цифрового простору. Варто також зазначити, що певні труднощі виникають на рівні міжінституційної взаємодії всередині самого Європейського Союзу. Попри існування чітко визначених ролей Єврокомісії, Європейського парламенту, Європейської ради та інституцій сектору безпеки, інколи процес ухвалення нових регуляторних актів або оновлення наявних документів затягується через різні бачення щодо рівня втручання ЄС у внутрішні справи держав-членів [54].

Розвиваючи зазначену проблематику далі, необхідно підкреслити, що імплементацію стратегічних документів ЄС у сфері інформаційної безпеки гальмує також відсутність достатньо ефективних механізмів контролю та механізмів відповідальності за невиконання встановлених норм [13]. Формально Європейська Комісія має інструменти моніторингу, однак, як засвідчують щорічні звіти за 2022–2024 роки, вони переважно носять

рекомендаційний характер і не містять дієвих санкцій у випадках, коли держави-члени систематично відстають у виконанні вимог таких ключових документів, як NIS2, DSA чи Стратегія кібербезпеки. Внаслідок цього країни, які не приділяють достатньої уваги модернізації інформаційної інфраструктури або не інвестують у розвиток експертного потенціалу, фактично не стикаються з реальними наслідками, що знижує мотивацію до прискорення імплементаційних процесів. Саме тому у 2025 році дедалі частіше обговорюється питання про необхідність запровадження більш жорстких контрольних механізмів, зокрема утворення спеціального європейського органу з моніторингу виконання норм інформаційної безпеки [52].

Утім, навіть посилення контролю не ліквідує іншу, не менш складну проблему – брак чіткої синхронізації між довгостроковими стратегічними документами та короткостроковими пріоритетами, які виникають у відповідь на нові кризи. Наприклад, після початку повномасштабної агресії РФ проти України у 2022 році ЄС змушений був кардинально переформатувати частину своїх інформаційно-безпекових пріоритетів, приділяючи значно більше уваги протидії пропаганді, захисту критичної інфраструктури й кіберстійкості енергетичного сектору [51]. Це, безумовно, було необхідно, проте одночасно призвело до уповільнення реалізації деяких попередньо визначених стратегічних напрямів, які вже були відображені у документах 2020-2021 рр.. Подібна несинхронізованість стратегічної та тактичної дійсності суттєво ускладнює імплементацію, адже держави-члени змушені постійно «перекроювати» свої плани відповідно до нових викликів.

До цього додається ще одна важлива перешкода – недостатня адаптованість стратегічних документів до регіональних особливостей країн ЄС. Хоча Європейський Союз прагне до гармонізації інформаційної політики, фактичні умови у різних державах-членах суттєво відрізняються. Наприклад, Центральна та Східна Європа має значно вищий рівень загроз з боку російських інформаційних операцій, що потребує більш інтенсивних заходів із

медіаграмотності, моніторингу та протидії дезінформації [38]. Натомість країни Західної Європи часто концентруються на питаннях цифрових прав користувачів, штучного інтелекту та етичних аспектів використання даних. Уніфіковані стратегічні документи не завжди враховують такі регіональні відмінності, через що їх імплементація нерідко стає формальною або ж вимагає суттєвих національних доопрацювань [15]. Окремої уваги заслуговує питання стійкості суспільства до інформаційних впливів, яке відіграє особливо важливу роль у контексті реалізації стратегічних документів ЄС. Без розвиненої культури медіаграмотності навіть найефективніші регуляції не здатні забезпечити повний захист інформаційного простору. Попри те, що у 2022-2024 рр. ЄС інвестував значні кошти у програми з підвищення цифрової грамотності, рівень обізнаності населення різних країн суттєво відрізняється. Наприклад, за результатами дослідження Eurobarometer за 2023 рік, лише 48 % громадян країн ЄС можуть впевнено визначити дезінформацію, тоді як стратегічні документи виходять із припущення про значно вищий рівень цифрової компетентності [35]. Саме ця суперечність між стратегічними очікуваннями та реальними можливостями суспільства створює ще один бар’єр на шляху ефективноїої імплементації.

Ще одним викликом виступає залежність ЄС від технологічних рішень, які переважно розробляються поза межами Європи. Значна частина інструментів, необхідних для забезпечення кібербезпеки, штучного інтелекту, аналізу великих даних чи автоматизованої модерації контенту, належить американським або азійським компаніям. Це ускладнює реалізацію таких положень, як гарантування цифрового суверенітету, передбаченого у Стратегії цифрового десятиліття (2021) [34]. Не слід забувати й про те, що сама швидкість ухвалення нових стратегічних документів інколи створює проблеми. ЄС працює у надзвичайно динамічному інформаційному середовищі, тому документи оновлюються регулярно, інколи навіть частіше, ніж їх встигають імплементувати. Так, у період із 2020 по 2024 рік було ухвалено понад 10 масштабних документів у сфері цифрової політики та

інформаційної безпеки [32]. Внаслідок цього держави-члени відчувають своєрідний «нормативний тиск», адже вони змушені одночасно виконувати старі зобов'язання та адаптуватися до нових вимог.

Вирішення окреслених проблем вимагатиме від Європейського Союзу не лише оновлення нормативно-правової бази, а й формування гнучких механізмів підтримки держав-членів, розбудови власного технологічного потенціалу та зміцнення внутрішньої інтеграції. Зрештою, ефективна імплементація стане можливою лише за умов комплексного підходу, який враховуватиме як загальноєвропейські інтереси, так і національні особливості, а також стрімкий характер сучасного інформаційного середовища.

3.3. Напрями вдосконалення політики інформаційної безпеки ЄС та її значення для України

Політика інформаційної безпеки Європейського Союзу перебуває нині у фазі глибокої трансформації, зумовленої поєднанням зовнішніх гібридних загроз, технологічних зрушень і необхідності захисту демократичних процесів як усередині ЄС, так і в сусідніх державах, передусім в Україні. По-перше, важливим напрямом вдосконалення є посилення нормативно-правової основи кібербезпеки та стійкості цифрової інфраструктури: оновлена Директива NIS2, ухвалена у 2022 р. й розширена у 2023 р., встановлює більш жорсткі вимоги до управління ризиками, звітності про інциденти та безпеки ланцюгів постачання в широкому колі секторів, від енергетики до охорони здоров'я, що має бути повністю імплементовано державами-членами у 2024-2025 рр. [27; 13]. Паралельно діє Регламент про кібербезпеку (Cybersecurity Act 2019), який заклав підвалини європейської системи сертифікації кіберпродуктів і послуг, а також ініціативи на кшталт майбутніх актів про кіберстійкість та кіберсолідарність, спрямованих на створення спільних механізмів реагування на масштабні кібератаки [69].

По-друге, ключовим вектором удосконалення політики стає комплексна протидія дезінформації та ширшому феномену іноземної інформаційної

маніпуляції й втручання (FIMI). ЄС поступово формує цілісну «екосистему» інструментів: Кодекс практики щодо дезінформації, система швидкого оповіщення, Європейська обсерваторія цифрових медіа, спеціальний FIMI-toolbox, гібридний та кібердипломатичний «інструментарій», а також мережа співпраці у сфері виборчої безпеки [4]. У березні 2025 р. ЄС додатково посилив спроможності Служби зовнішніх дій (EEAS) з ідентифікації та аналізу FIMI, що стало відповіддю на довгострокові російські інформаційні операції, які розгорнулися ще з 2015 р. і особливо загострилися після повномасштабного вторгнення РФ в Україну у лютому 2022 р. [38]. Водночас, у 2022-2024 рр. ЄС дедалі активніше застосовує санкційний інструмент саме проти дезінформаційної інфраструктури РФ: до санкційних списків включаються російські державні ЗМІ, проксі-платформи та окремі організатори інформаційних операцій, а з 2025 р. Рада ЄС отримала можливість навіть призупиняти ліцензії на мовлення медіа, що систематично поширюють дезінформацію [47].

Третім, не менш важливим виміром модернізації є посилення регулювання цифрових платформ, насамперед через ухвалення та поетапне запровадження Digital Services Act (DSA), який набув чинності у 2023 р. і запроваджує для дуже великих онлайн-платформ обов’язки з оцінки системних ризиків, пов’язаних із дезінформацією, алгоритмічною рекомендацією контенту та політичною рекламою, а також вимагає від них більшої прозорості й доступу дослідників до даних [66]. За сучасних умов, коли соціальні мережі й месенджери використовуються для координації атак на вибори, підриву довіри до демократичних інституцій та поширення антиукраїнських наративів, саме зв’язка DSA з оновленим Кодексом практики щодо дезінформації формує ядро «співрегуляційної» моделі, яка може стати орієнтиром і для України [80]. Показово, що в листопаді 2025 р. в ЄС обговорюється створення Центру демократичної стійкості (Centre for Democratic Resilience) як елементу ширшого «щита демократії», який має об’єднати експертні спільноти держав-членів і, що важливо, країн-кандидатів,

у тому числі України, для раннього виявлення і спільної реакції на кампанії впливу з боку РФ, Китаю та інших акторів [15].

Окремий комплекс напрямів стосується розвитку інституційної та суспільної стійкості: йдеться про розбудову потенціалу ENISA, StratCom-підрозділів EEAS, створення гібридних груп швидкого реагування та інвестиції у кіберосвіту, медіаграмотність і підтримку незалежних медіа [19]. Саме тут роль України як партнера ЄС є подвійною: з одного боку, Україна отримує підтримку, від спільних проєктів зі стратегічних комунікацій до ініціатив з протидії російській дезінформації в інформаційному просторі ЄС, а з іншого, виступає «лабораторією стійкості», яка пропонує власний практичний досвід реагування на багаторічну інформаційну агресію [8]. Уже у Спільній заяві саміту Україна-ЄС 2020 р. Євросоюз підтвердив готовність допомагати Україні протидіяти гібридним загрозам і дезінформації шляхом зміцнення незалежних медіа, медіаграмотності та стратегічних комунікацій, а у 2023 р. високий представник Ж. Боррель наголосив, що боротьба з дезінформацією є спільним пріоритетом ЄС і України [24]. Важливо й те, що низка програм на кшталт проєктів зі стратегічних комунікацій ЄС для уряду України або платформи «Cyber Gate», створеної за підтримки Представництва ЄС та міжнародних фондів, спрямовані на посилення спроможностей держави й суспільства до виявлення фейків, реагування на кібератаки та масштабування проєктів медіаграмотності [10].

Нарешті, перспективним напрямом вдосконалення є більш системна інтеграція України в європейську архітектуру інформаційної безпеки через гармонізацію законодавства, участь у спеціалізованих платформах та обмін кращими практиками. Дослідження українських науковців наголошують, що національне регулювання інформаційної безпеки ще недостатньо повно відображає підходи ЄС, зокрема у сфері прозорої співрегуляції з цифровими платформами й механізмів контролю за політичною рекламою, а також у частині комплексного охоплення технічних і соціальних аспектів інформаційної безпеки в єдиній рамці [11]. У цьому контексті адаптація

положень NIS2, DSA, future-орієнтованих ініціатив щодо кіберстійкості й боротьби з FIMI не лише сприятиме євроінтеграції України, а й допоможе структурувати національну політику довкола чітких стандартів управління ризиками, відповідальності цифрових посередників і захисту прав громадян у мережі. Важливо, що ЄС уже розглядає Україну як активного учасника загальноєвропейського діалогу: у травні 2025 р. українські регулятори медіасфери приєдналися до пан'європейської дискусії з протидії дезінформації й демократичної стійкості, пропонуючи власні напрацювання щодо регулювання онлайн-контенту й взаємодії з платформами під час війни [18].

Таким чином, напрями вдосконалення політики інформаційної безпеки ЄС, від посилення кіберрегуляції й санкційних механізмів проти гібридних загроз до розвитку інструментів стратегічних комунікацій, співрегуляції з платформами й інституційної стійкості, безпосередньо визначають рамкові умови для модернізації української моделі інформаційної безпеки [15]. Для України це означає, по-перше, необхідність системно гармонізувати законодавство з європейським acquis у сфері кібербезпеки й цифрових послуг; по-друге, долучатися до спільних механізмів FIMI-протидії, використовуючи власний досвід виявлення й нейтралізації російських операцій впливу; по-третє, інвестувати у розвиток стратегічних комунікацій, медіаграмотності та незалежних медіа як ключових елементів суспільної стійкості. У підсумку, розбудова спільного простору інформаційної безпеки «ЄС – Україна» постає не лише техніко-правовим завданням, а й стратегічною складовою гарантування демократичного розвитку, збереження суверенітету та зміцнення спроможності об'єднаної Європи протистояти гібридній агресії у довгостроковій перспективі [10].

Усі зазначені напрями свідчать про те, що інформаційна безпека стає для Європейського Союзу не просто технічним компонентом цифрової політики, а справжнім фундаментом демократичної стійкості, без якої неможливо підтримувати ані цілісність внутрішнього ринку, ані ефективність спільної зовнішньої та безпекової політики [15]. Водночас, розвиток комплексної

політики інформаційної безпеки в ЄС демонструє, що інституції Союзу (Єврокомісія, Європейська служба зовнішніх дій, Європарламент, ENISA) поступово переходять від фрагментарного реагування до системного стратегічного планування [13]. Це проявляється у створенні довгострокових програм цифрової трансформації, запуску багаторічного фінансування в межах Digital Europe Programme, а також у формуванні Європейського центру компетенцій з кібербезпеки, який координує інвестиції в інновації та дослідження [65]. У цьому контексті особливої ваги набуває питання співпраці ЄС із країнами-партнерами, серед яких Україна відіграє унікальну роль. З огляду на те, що Україна протягом багатьох років фактично перебуває на передовій гібридної війни, вона стала для Європи ключовим джерелом досвіду щодо протидії дезінформації, кібератакам і психологічним операціям [1]. Як засвідчили події 202-2025 рр., стійкість України в інформаційній сфері нерідко випереджає спроможності окремих країн-членів ЄС, що робить двосторонню співпрацю взаємовигідною [51]. ЄС отримує практичні кейси, які допомагають удосконалити європейські процедури реагування, а Україна – доступ до нормативних стандартів, інструментів кіберзахисту та фінансових ресурсів.

Перспективи розвитку інформаційної безпеки України в межах європейського інтеграційного курсу напряму пов’язані з адаптацією ключових нормативних документів, таких як NIS2, DSA, DMA та майбутній Акт про кіберстійкість [27, 66, 69]. Проте, імплементація цих документів не може бути формальною. Україні варто врахувати, що ЄС переходить до моделі багаторівневої відповідальності цифрових платформ, у якій особливу роль відіграє принцип прозорості: відкритість алгоритмів, доступ дослідників до даних, чітке маркування політичної реклами, можливість відстеження походження контенту [66]. Такий підхід може стати надзвичайно корисним у період післявоєнної відбудови України, коли питання довіри до медіа, етичних стандартів онлайн-комунікації та протидії маніпуляціям відіграватимуть вирішальну роль у демократичній консолідації суспільства [10].

Окремою складовою майбутньої політики має стати формування стійкої інституційної основи. Україні доцільно розвивати національні центри кібербезпеки та стратегічних комунікацій у синергії з відповідними структурами ЄС, зокрема Європейським центром компетенцій з кібербезпеки, Hybrid Fusion Cell та East StratCom Task Force [36, 37]. Створення спільних груп швидкого реагування, регулярні навчання, обмін даними та методологіями аналізу FIMI дадуть змогу Україні не лише укріпити власну захищеність, а й зробити свій внесок у загальноєвропейську інформаційну екосистему. Крім того, необхідно враховувати, що інформаційна безпека у XXI столітті невід'ємно пов'язана з економічною та технологічною безпекою. Саме тому Україні потрібна участь у програмах ЄС, спрямованих на розвиток штучного інтелекту, квантових технологій, захищених мереж зв'язку та аналізу великих даних. Адже сучасні інформаційні операції дедалі більше опираються на машинне навчання, синтетичні медіа, генеративний штучний інтелект та автоматизовані мережі ботів [38]. Вбудованість України в європейський техно-економічний простір дозволить не лише захищатися, а й створювати інноваційні рішення для протидії новим гібридним загрозам.

Зрештою, значення вдосконалення політики інформаційної безпеки ЄС для України є стратегічним. Воно полягає не тільки в можливості підвищити рівень національної безпеки, а й у шансі стати повноцінним учасником формування нової європейської моделі інформаційної стійкості. Участь України у проєктах кіберзахисту, стратегічних комунікацій, регулювання онлайн-платформ і дослідження цифрових ризиків сприятиме гармонізації українського законодавства з європейським acquis і підвищенню довіри між Україною та державами-членами [11]. Більше того, це зміцнює позиції України як активного, а не пасивного учасника європейської безпеки, що підсилює її вплив у процесах прийняття рішень і відкриває нові можливості д ля політичної інтеграції.

Висновки до розділу 3

Зазначимо, що сучасна система протидії гібридним інформаційним загрозам Європейського Союзу поступово трансформується відповідно до масштабів і динаміки викликів, які, до речі, набули особливої інтенсивності після 2014 року та, безумовно, після повномасштабного вторгнення Росії в Україну у 2022 році. Інструменти протидії, що їх використовує ЄС, вирізняються комплексністю та багаторівневістю: від зміцнення кіберзахисту і моніторингу дезінформації до розвитку стратегічних комунікацій та посилення міжінституційної взаємодії. При цьому, важливо підкреслити, що саме нормативно-правові та організаційні механізми, закладені у діяльність таких структур, як East StratCom Task Force, EU Hybrid Fusion Cell чи Європейське агентство з кібербезпеки (ENISA), створюють фундамент для ефективної протидії координаційним інформаційним атакам, зокрема тим, що застосовуються державами-ревізіоністами.

Разом із тим, імплементація стратегічних документів ЄС у сфері інформаційної безпеки, як показує практика, стикається з низкою системних проблем. З одного боку, держави-члени нерівномірно сприймають загрози, а отже, й різняться рівні політичної волі та інституційної спроможності щодо впровадження відповідних норм. З іншого боку, навіть найважливіші документи, зокрема Європейська стратегія кібербезпеки 2020 року, оновлена Стратегія безпеки Союзу чи План дій проти дезінформації, виявляються складними для уніфікованого застосування через різноманітність національних правових систем та різний рівень цифровізації суспільств. До цього додаються фінансові обмеження, недостатня узгодженість між інституціями ЄС, а також, що цілком очевидно, швидка еволюція технологій, яка створює прогалини між теорією та практикою.

У світлі зазначеного напрями вдосконалення політики інформаційної безпеки ЄС мають включати, по-перше, зміцнення наднаціональних механізмів координації, по-друге, оновлення стратегічних підходів до боротьби з дезінформацією, зокрема із застосуванням ШІ-технологій, і, по-третє, інвестування у стійкість громадянського суспільства та

медіаграмотність. Для України, яка, фактично, перебуває на передньому краї протидії гібридним впливам, досвід ЄС є надзвичайно важливим: він дає змогу адаптувати найкращі практики, забезпечити подальше наближення законодавства до acquis ЄС та посилити власну спроможність у сфері інформаційної безпеки. Зрештою, саме синергія європейського та українського підходів може стати основою для формування ефективної системи захисту в умовах довготривалих гібридних загроз.

ВИСНОВКИ

У результаті дослідження інформаційної безпеки Європейського Союзу в сучасних умовах, зроблено наступні висновки:

1. Визначивши поняття та структуру інформаційної безпеки в системі міжнародних відносин, слід підкреслити, що охоплює політичний, правовий, технологічний, соціокультурний та безпековий виміри. Інформаційна безпека, таким чином, розглядається не лише як захист інформаційного простору, але і як цілеспрямована діяльність держав і міжнародних організацій щодо забезпечення цілісності, доступності та достовірності інформації, а також підтримання стійкості суспільств до дезінформації та зовнішніх впливів. У цьому контексті концептуально важливою є структуризація інформаційної безпеки, що включає інституційний рівень (міжнародні організації, державні органи, спеціалізовані служби), нормативно-правовий рівень (стратегії, регламенти, директиви), технологічний рівень (цифрова інфраструктура, кіберзахист, системи моніторингу), а також когнітивний рівень, який визначає здатність суспільства розпізнавати маніпуляції, протистояти інформаційним впливам і формувати критичне мислення..

2. З’ясувавши роль Європейського Союзу у сфері глобальної та регіональної безпеки, варто наголосити, що ЄС трансформувався з економічного союзу в одного з провідних акторів у сфері інформаційної безпеки та стратегічної комунікації. ЄС, будучи унікальним інтеграційним утворенням, активно розробляє і впроваджує комплексну політику інформаційної безпеки, поєднуючи інструменти «м’якої сили», цифрового регулювання та координації між державами-членами. Як наслідок, ЄС виступає не лише об’єктом інформаційного впливу, але й суб’єктом формування глобальних безпекових норм. У цьому контексті важливо зазначити, що інформаційна безпека ЄС безпосередньо пов’язана з його здатністю забезпечувати демократичні процеси, стійкість інституцій,

стабільність суспільств та довіру громадян до державних і наддержавних механізмів управління.

3. Проведене дослідження дало змогу виявити широкий спектр гібридних загроз, зокрема дезінформаційні кампанії, кібератаки, маніпулятивний вплив через соціальні мережі, атаки на критичну інфраструктуру та втручання у виборчі процеси. Зазначимо, що характер цих загроз постійно змінюється, що, у свою чергу, вимагає адаптивних механізмів протидії. Встановлено, що збройна агресія РФ проти України після 2014 року, а особливо після 2022 року, стала каталізатором посилення інформаційної безпеки ЄС. Саме тоді ЄС зіткнувся з масштабними операціями впливу, спрямованими на підрив громадської довіри, дезорієнтацію суспільств, розкол між державами-членами та дискредитацію рішень ЄС щодо санкційної політики й військово-політичної підтримки України. До того ж, гібридні виклики дедалі частіше пов’язані не лише з державними акторами, але й із приватними компаніями, транснаціональними платформами та мережею недержавних груп, що ускладнює ідентифікацію джерела та мети інформаційного впливу.

4. Визначивши роль інституцій ЄС у забезпеченні інформаційної стійкості та нормативно-правове регулювання, маємо підстави стверджувати, що саме інституційний вимір є ключовим у формуванні комплексної системи реагування на гібридні загрози. Оперативна робоча група зі стратегічних комунікацій системно виявляє та спростовує дезінформаційні кампанії, Європейська агенція з кібербезпеки (ENISA), яка координує діяльність щодо кіберзахисту та розвитку спільних стандартів, групи швидкого реагування на дезінформацію, а також численні директиви й регламенти, зокрема Акт про цифрові послуги і Друга Директива про безпеку мережевих та інформаційних систем, створюють правову та інституційну основу для координації зусиль держав-членів. Власне, інституції формують цілісну рамку, що поєднує превенцію, реагування та відновлення після інформаційних інцидентів, тим самим сприяючи зміцненню стійкості ЄС.

5. Встановлено, що ефективність інформаційної безпеки Євросоюзу значною мірою залежить від співпраці з державами-членами. Оскільки компетенції у сфері безпеки залишаються поділеними між національним та наднаціональним рівнями, критично важливо забезпечити координацію стратегій, обмін інформацією, узгодження стандартів кіберзахисту та підвищення готовності до кризових ситуацій. У цьому контексті значущими є спільні навчання, проєкти з побудови цифрової інфраструктури, а також механізми раннього попередження. Крім того, співпраця з міжнародними партнерами, передусім НАТО, США, країнами G7 та східноєвропейськими партнерами, суттєво підсилює можливості ЄС щодо протидії кібератакам, інформаційним операціям і втручанню у політичні процеси. Це, з одного боку, розширює інструментарій реагування, а з іншого – формує спільну глобальну політику інформаційної безпеки.

6. Дослідження дало змогу виявити низку проблем, пов’язаних з імплементацією стратегічних документів ЄС у сфері інформаційної безпеки. Серед найважливіших: нерівномірний рівень цифрової готовності держав-членів, різна спроможність систем кіберзахисту, відсутність єдиних підходів до регулювання медіапростору, а також складність адаптації наднаціональних норм до національних правових систем. Крім того, деякі директиви ЄС реалізуються повільно через недостатній рівень фінансування, кадрові обмеження або політичні суперечності. Водночас постає питання перегляду окремих нормативних актів, оскільки технологічний розвиток відбувається значно швидше, ніж оновлення правової бази. Зазначимо, що попри зазначені проблеми, Європейський Союз продовжує формувати прогресивну модель інформаційної безпеки, здатну адаптуватися до швидкоплинних глобальних змін. Для України, яка, по суті, перебуває на передовій інформаційного протиборства, досвід ЄС має не лише теоретичне, а й практичне значення. По-перше, імплементація європейських стандартів кіберзахисту здатна підвищити стійкість українських інституцій до атак з боку РФ. По-друге, адаптація інструментів ЄС у сфері протидії дезінформації сприятиме зміцненню

національної системи стратегічних комунікацій. По-третє, участь України у спільних проєктах ЄС у сфері інформаційної та кібербезпеки дозволить інтегруватися в єдину європейську архітектуру безпеки. Зрештою, використання європейських практик створює підґрунтя для формування цілісної, ефективної та стійкої політики інформаційної безпеки, що є критично важливим у контексті російсько-української війни та майбутньої інтеграції до ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Голуб'як Н., Голуб'як І. Гібридні загрози як виклики безпековій політиці ЄС. *Вісник Прикарпатського університету. Серія: Політологія*. 2023. Т. 1. №15. С. 53-59. DOI: https://doi.org/10.32782/2312-1815/2024-1-7

2. Гончаров М.В. Дослідження поняття «інформаційна безпека». *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 82. Ч. 1. С. 34-37. DOI: https://doi.org/10.24144/2307-3322.2024.82.1.4

3. Дрига Д. Аналіз правових механізмів забезпечення інформаційної безпеки інформаційної інфраструктури Європейського Союзу. *Herald of Khmelnytskyi National University. Eco№mic Sciences*. 2024. № 334(5). С. 46–51. DOI: https://doi.org/10.31891/2307-5740-2024-334-7

4. Звоздецька О. Інституційні механізми протидії дезінформації в ЄС: проблеми та здобутки. *Медіафорум: аналітика, прогнози, інформаційний менеджмент.* 2022. № 10. С. 107–122. DOI: 10.31861/mediaforum.2022.10.107-122. URL: https://doi.org/10.31861/mediaforum.2022.10.107-122 (дата звернення: 23.11.2025).

5. Звоздецька О. Протидія дезінформації в Європейському Союзі: правовий аспект. *Медіафорум: аналітика, прогнози, інформаційний менеджмент.* 2021. № 9. С. 245–262. DOI: 10.31861/mediaforum.2021.9.245-262. URL: https://doi.org/10.31861/mediaforum.2021.9.245-262 (дата звернення: 23.11.2025).

6. Інформаційна безпека та гібридні загрози: навчальний посібник. Укл. Мухін В.Є., Завгородній В.В., Завгородня Г.А. Київ: ТОВ «ТРОПЕА», 2024. 104 с. DOI: https://doi.org/10.32703/978-617-8268-36-7

7. Кавин С.Я. Правові засади забезпечення кібербезпеки в державах – членах Європейського Союзу. *Актуальні проблеми держави і права*. 2020. Вип. 51. С. 51-58. DOI: https://doi.org/10.32837/apdp.v0i87.2797

8. Карпенко О. Європейський досвід протидії гібридним загрозам для відновлення економіки України. *International Economic Policy*. 2024. Вип.

41. URL: https://iepjournal.com/journals/41/2024_41_12_Karpenko.pdf (дата звернення: 23.11.2025).

9. Карпенко О. Європейський досвід протидії гібридним загрозам для економічного відродження України. *Міжнародна економічна політика*. 2024. № 2 (41). С. 177–186. DOI: 10.33111/iep.eng.2024.41.12. URL: https://doi.org/10.33111/iep.eng.2024.41.12 (дата звернення: 23.11.2025).

10. Мазепа С. Міжнародний досвід захисту інформаційної безпеки: імплементація європейських правових норм в законодавство України // *Вісник юридичного факультету УжНУ*. 2025. Вип. 44. С. 47–53. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/44-2.pdf (дата звернення: 20.10.2025).

11. Мазепа С. Міжнародний досвід захисту інформаційної безпеки: імплементація європейських правових норм в законодавство України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 3(90). С. 289–296. DOI: 10.24144/2307-3322.2025.90.3.42.

12. Милосердна І.М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. *Політичні проблеми міжнародних систем та глобального розвитку*. 2024. №4. С. 179–185. DOI: https://doi.org/10.24195/2414-9616.2024-4.26

13. Мужанова Т. М., Легомінова С. В., Щавінський Ю. В., Якименко Ю. М., Нестеренко Г. П. Основні підходи й напрями розвитку політики кібербезпеки Європейського Союзу. Кібербезпека: освіта, наука, техніка. 2024. Т. 4. № 24. С. 133–149. DOI: 10.28925/2663-4023.2024.24.133149.

14. Новіцький В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. № 1(40). DOI: https://doi.org/10.37750/2616-6798.2022.1(40).254349

15. Прудникова О. В. Інформаційна безпека Європейського Союзу: виклики та тенденції. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія.*

2025. № 3(66). С. 45–56. URL: https://doi.org/10.21564/2663-5704.66.337888 (дата звернення: 20.10.2025).

16. Пугачов О. І. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. №13. https://doi.org/10.54929/2786-5746-2024-13-02-07 (дата звернення: 20.10.2025).

17. Федонюк С. Політика ЄС в аспекті основних глобальних концепцій інформаційної (кібер) безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2021. № 3(11). С. 144-168. URL: https://doi.org/10.29038/2524-2679-2021-03-144-168 (дата звернення: 20.10.2025).

18. Фурсай О. Політика інформаційної безпеки Європейського Союзу. *Літопис Волині*. 2023. №29. С. 165–170. https://doi.org/10.32782/2305-9389/2023.29.27 (дата звернення: 20.10.2025).

19. Хмель А. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). *Acta de Historia & Politica: Saeculum XXI*. 2022. № 3. С. 91–101. DOI: 10.26693/ahpsxxi2021-2022.03.091. URL: https://ahpsxxi.org/index.php/journal/article/view/52 (дата звернення: 23.11.2025).

20. Almeida F. Comparative Analysis of EU-Based Cybersecurity Skills Frameworks. *Computers & Security*. 2025. Т. 151. № 5. № 104329. DOI: 10.1016/j.cose.2025.104329.

21. Bendiek A., Portela C. Revisiting the EU Cybersecurity Strategy: a call for EU leadership in cybersecurity. *SWP Comment*. 2021. № 43. 8 p.

22. Buttigieg C. P., Grech J., Zarb A. The Digital Operational Resilience Act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. *ERA Forum.* 2024. Vol. 25. URL: https://link.springer.com/article/10.1007/s12027-024-00793-w (Last accessed: 20.10.2025).

23. Chiara P. G. Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*. 2024. Vol. 51. Art. 105832. URL: https://www.sciencedirect.com/science/article/pii/S0267364924000281 (Last accessed: 20.10.2025).

24. Council of the European Union. A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security. Brussels, 21.03.2022. ST 7371/22. 46 p. URL: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en (Last accessed: 20.10.2025).

25. Council of the European Union; EEAS. A Strategic Compass for Security and Defence. 2022. URL: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en (Last accessed: 20.10.2025).

26. Cullen P., Juola C., Karagiannis G. et al. The Landscape of Hybrid Threats: A Conceptual Model (Public Version) Luxembourg : Publications Office of the European Union, 2021. (EUR 30585 EN). DOI: 10.2760/44985. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305 (Last accessed: 20.10.2025).

27. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directives (EU) 2018/1972 and (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152.

28. Eckhardt P., Kotovskaia A. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*. 2023. Vol. 4. № 2. P. 147–164. DOI: https://link.springer.com/article/10.1365/s43439-023-00084-z

29. ENISA Threat Landscape 2022: July 2021 to July 2022. *European Union Agency for Cybersecurity*. Athens, 2022. 146 p.

30. ENISA Threat Landscape 2023: July 2022 to June 2023. *European Union Agency for Cybersecurity*. Athens, 2023. 160 p.

31. EU cyber-resilience act – European Parliament Briefing. *European Parliament.* 2022. 12 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI%282022%29739259_EN.pdf (Last accessed: 20.10.2025).

32. EU cybersecurity policies. Shaping Europe's digital future. *Digital-strategy.ec.europa.eu* 2025. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (Last accessed: 20.10.2025).

33. EU Policy on Cyber Defence: Joint communication to the European Parliament and the Council JOIN(2022) 49 final. Brussels, 10.11.2022. 19 p.

34. European Commission; High Representative of the Union for Foreign Affairs and Security Policy. The EU's Cybersecurity Strategy for the Digital Decade: Joint Communication JOIN(2020) 18 final. Brussels, 16.12.2020. 23 p.

35. European Court of Auditors. Disinformation Affecting the EU: Tackled but Not Tamed: Special Report 09/2021. Luxembourg : Publications Office of the European Union, 2021. 56 p. URL: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf (Last accessed: 20.10.2025).

36. European External Action Service. 1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. *European External Action Service.* Brussels, 2023. URL: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en (Last accessed: 20.10.2025).

37. European External Action Service. 2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. *European External Action Service.* Brussels, 2024. URL: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en ((Last accessed: 20.10.2025).

38. European External Action Service. 3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. *European External*

Action Service. Brussels, 2025. URL: https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en (Last accessed: 20.10.2025).

39. European Union Agency for Cybersecurity (ENISA). The EU Cybersecurity Index 2024. Athens, 2025. URL: https://www.enisa.europa.eu/publications/the-eu-cybersecurity-index-2024 Енися

40. Fahey E. The evolution of EU-US cybersecurity law and policy. *Journal of Common Market Studies*. 2024. Vol. 62. № 1. P. 245-271. DOI:10.1080/07036337.2024.2411240. DOI: https://doi.org/10.1080/07036337.2024.2411240

41. Giris V. A. Legal status of European Union bodies and institutions in the field of cybersecurity. *International Law and International Organizations*. 2023. № 1. P. 1–21. DOI: 10.7256/2454-0633.2023.1.39986.

42. Haryati V. W., Sihwiyati S. I., Talitasyadiah A. M. Development of cybersecurity governance in the EU region. *JLAST: Journal of Law and Social Transformation.* 2025. Vol. 3. № 1. P. 13–24.

43. Hroza D. V. Some aspects of EU information security. *Juridical Scientific and Electronic Journal*. 2023. № 12. С. 484–490. DOI: 10.32782/2524-0374/2023-12/120.

44. Hybrid CoE Research Report 15. Countering Disinformation in the Euro-Atlantic. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2025. 48 p. URL: https://www.hybridcoe.fi/wp-content/uploads/2025/10/Hybrid_CoE_Research_Report_15_Countering_disinformation_Euro_Atlantic.pdf (Last accessed: 20.10.2025).

45. Information integrity and countering Foreign Information Manipulation and Interference (FIMI). *European External Action Service (EEAS).* 2025. URL: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en (Last accessed: 20.10.2025).

46. Jungwirth R., Smith H., Willkomm E. Hybrid Threats: A Comprehensive Resilience Ecosystem. *Executive Summary*. Luxembourg:

Publications Office of the European Union, 2023. (JRC129019). DOI: 10.2760/113791. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf (Last accessed: 20.10.2025).

47. Kachelmann M., Reiners W. The European Union's governance approach to tackling disinformation – protection of democracy, foreign influence, and the quest for digital sovereignty. *L'Europe en Formation*. 2023. № 396(1). P. 11–36. DOI: 10.3917/eufor.396.0011. URL: https://shs.cairn.info/revue-l-europe-en-formation-2023-1-page-11 (Last accessed: 20.10.2025).

48. Kalniete S., Pildegovics T. Strengthening the EU's resilience to hybrid threats. European View. 2021. Vol. 20. № 1. P. 23–33. DOI: 10.1177/17816858211004648. URL: https://journals.sagepub.com/doi/10.1177/17816858211004648 (Last accessed: 20.10.2025).

49. Kambourakis G., Neisse R., Nai-Foviⅈ I. Information security in the age of EU-institutions digitalisation: a landscape analysis. Luxembourg : Publications Office of the European Union, 2021. 78 p. (JRC Technical Report, JRC125214).

50. Karpiuk M. The legal status of digital service providers in the sphere of cybersecurity. *Studia Iuridica Lublinensia*. 2023. Vol. 32. № 2. P. 189–201. DOI: 10.17951/sil.2023.32.2.189-201.

51. Kelemen R. The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations. *Connections: The Quarterly Journal*. 2024. T. 22. № 2. P. 75–90. DOI: 10.11610/Connections.22.2.55.

52. Kianpour M., Schomakers E., Kasneci E. Digital sovereignty in practice: analyzing the EU's NIS2 directive. *International Journal of Information Security.* 2025. Vol. 24. № 4. URL: https://link.springer.com/article/10.1007/s10207-025-01090-4 (Last accessed: 20.10.2025).

53. Krykavska I. Regulatory and institutional support of digitalization and cybersecurity of the public administration system in the EU. *Вісник Національного*

університету «Львівська політехніка». Серія: Юридичні науки. 2023. № 1(37). С. 148-158. URL: http://doi.org/10.23939/law2023.37.148

54. Liebetrau T. Problematising EU Cybersecurity: Exploring How the EU has rendered digitisation as a security concern and cybersecurity emerged as an object of EU governance. *Journal of Common Market Studies*. 2024. DOI:10.1111/jcms.13523. URL: https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.13523

55. Lonardo L. EU Law Against Hybrid Threats: A First Assessment. *European Papers: A Journal on Law and Integration*. 2021. Vol. 6. № 2. – P. 1075–1096. DOI: 10.15166/2499-8249/514. URL: https://www.europeanpapers.eu/e-journal/eu-law-against-hybrid-threats-first-assessment (Last accessed: 20.10.2025).

56. Ludvigsen K.R., Nagaraja S. The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act. *arXiv:2205.13196*. 2022. URL: https://arxiv.org/abs/2205.13196 (Last accessed: 20.10.2025).

57. Mafart J. Hybrid threats: the new horizons for a «Europe of internal security»? *Fondation Robert Schuman. European Issue*. 2025. № 787. URL: https://www.robert-schuman.eu/en/european-issues/787-hybrid-threats-the-new-horizons-for-a-europe-of-internal-security (Last accessed: 20.10.2025).

58. Miadzvetskaya D., Wessel R.A.. The externalisation of the EU's cybersecurity regime: towards cyber diplomacy? *European Papers*. 2022. Vol. 7. №. 1. P. 439–472. URL: https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2022_1_2_Articles_Yuliya_Miadzvetskaya_Ramses_Wessel_00570.pdf (Last accessed: 20.10.2025).

59. Navigating the EU Cybersecurity Policy Ecosystem. *Interface Europe*. 2024. URL: https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem (Last accessed: 20.10.2025).

60. Nolte H., Rateike M., Finck M. Robustness and Cybersecurity in the EU Artificial Intelligence Act. *ACM Conference on Fairness, Accountability, and Transparency*. *arXiv:2502.16184*. 2025. DOI: 10.48550/arXiv.2502.16184.

61. Olech A. Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses. *Terroryzm – studia, analizy, prewencja*. 2025. Special Issue. P. 133–158. DOI: 10.4467/27204383TER.25.017.21520. URL: https://ejournals.eu/en/journal/terroryzm/article/hybrid-threats-to-critical-infrastructure-in-the-european-union-selected-hybrid-coe-analyses (Last accessed: 20.10.2025).

62. Ositashvili M. *The key role of the most recent EU regulation – the "Digital Operational Resilience Act" in the legal system, contemporary challenges, and Georgian perspectives* // *European Scientific Journal, ESJ*. 2024. T. 32. P. 586. URL: https://eujournal.org/index.php/esj/article/view/18478 (Last accessed: 20.10.2025).

63. Pingen A. Legislation to strengthen cybersecurity across the Union: NIS 2 Directive. *Eucrim – The European Criminal Law Associations' Forum.* 2023. № 1. P. 60–64.

64. Proto L., Bouza García L., Oleart A. The EU's FIMI Turn: How the European Union External Action Service reframed (dis)information governance. *Media and Communication.* 2025. Vol. 13. № 3. URL: https://www.cogitatiopress.com/mediaandcommunication/article/view/9474 (Last accessed: 20.10.2025).

65. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Tech№logy and Research Competence Centre and the Network of National Coordination Centres. *Official Journal of the European Union*. 2021. L 2021/887.

66. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union.* 2022. L 277.

67. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). *Official Journal of the European Union*. 14.12.2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng (Last accessed: 20.10.2025).

68. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). *Official Journal of the European Union*. 2023. L 2023/2854. URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (Last accessed: 20.10.2025).

69. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) № 168/2013 and (EU) № 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union.* 2024. L 2024/2847. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (Last accessed: 20.10.2025).

70. Renda A. The development of EU cybersecurity policy: from a coordinating actor to a cyber power? *Ankara Review of European Studies*. 2021. № 2. P. 467–495.

71. Saeva E., Tasheva I. The 2024 EU Elections and Cybersecurity: A Retrospective and Lessons Learned. *European View*. 2024. Vol. 23. № 2. DOI: 10.1177/17816858241288.

72. Schmitz-Berndt S., Cole M. D. *Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act*. ACIG. *2022.* T. 1. № 1. DOI: 10.5604/01.3001.0016.1323.

73. Shestak V. A., Savenkova P. G. Genesis of the №tion «cybersecurity» in the fuel and energy sector of the European Union: legal analysis. *Vestnik of Saint Petersburg University. Law.* 2024. Vol. 15. № 3.

74. Singh C. EU cybersecurity law in 2023: A review of the advances in the Network and Information Security 2 Directive (2022/2555). 2023. URL: https://westminsterresearch.westminster.ac.uk/item/w2369/european-cybersecurity-law-in-2023-a-review-of-the-advances-in-the-network-and-information-security-2-directive-2022-2555 (Last accessed: 20.10.2025).

75. Singh C. European Cybersecurity Law in 2023: A Review of the Advances in the Network and Information Security 2 Directive (2022/2555). 2023. URL: https://westminsterresearch.westminster.ac.uk/item/w2369/european-cybersecurity-law-in-2023-a-review-of-the-advances-in-the-network-and-information-security-2-directive-2022-2555 (Last accessed: 20.10.2025).

76. Somogyi T., Nagy R. The impact of the war in Ukraine on the information security of the European Union's banking industry – a case study of Hungary and Slovakia. *Contemporary Military Challenges.* 2023. Vol. 25. № 3–4. P. 23–32. DOI: 10.33179/bsv.99.svi.11.cmc.25.3-4.2.

77. Strucl D. The EU-NATO partnership and ensuring information security and cybersecurity: theory and practice. Sodobni vojaški izzivi. *Contemporary Military Challenges.* 2021. Vol. 23. № 2. P. 29–47. DOI: 10.33179/bsv.99.svi.11.cmc.23.2.2.

78. Szpor G.M.. The evolution of cybersecurity regulation in the European Union law and its implementation in Poland. *Review of European and Comparative Law.* 2021. Vol. 46. №. 3. P. 219–235. DOI:10.31743/recl.12645. URL: https://czasopisma.kul.pl/index.php/recl/article/view/12645 (Last accessed: 20.10.2025).

79. Teichmann F. The EU Cyber Resilience Act: Hybrid governance and compliance theory. *Computer Law & Security Review*. 2025. Vol. 56. Art. 106308. URL: https://www.sciencedirect.com/science/article/abs/pii/S2212473X25000811 (Last accessed: 20.10.2025).

80. The 2022 Strengthened Code of Practice on Disinformation. *European Commission.* 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (Last accessed: 20.10.2025).

81. The EU's Strategic Compass – marching in the right direction? *CEPS Policy Insights.* Brussels : Centre for European Policy Studies, 2022. (Policy Insight 2022-14).

82. Vandezande N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*. 2024. Vol. 52. Art.

105890. URL: https://www.sciencedirect.com/science/article/abs/pii/S0267364923001000 (Last accessed: 20.10.2025).

83. Villani S. Defending the security of the EU constitutional order against malicious cyber activity: reflections on the cyber-targeted sanctions regime. *Questions of International Law.* 2025. Vol. 110. P. 71–93.

84. Vivchar O., Muravska Y. NATO-Ukraine Cooperation as an Important Mechanism for Counteracting Hybrid Warfare. *National Security in Modern World. Legal, Tech№logical and Social Communication Aspects*. 2021. URL: https://orcid.org/0000-0001-9246-2226 (Last accessed: 20.10.2025).

85. Wigell M., Mikkola H., Juntunen T. Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats. – Brussels : European Parliament, 2021. 50 p. DOI: 10.2861/379. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf (Last accessed: 20.10.2025).

АНОТАЦІЯ

Ільченко Л.О. Інформаційна безпека Європейського Союзу в сучасних умовах (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 85 с. (рукопис).

Кваліфікаційна робота магістра присвячена визначенню інструментів забезпечення інформаційної безпеки Європейського Союзу в сучасних умовах. У кваліфікаційній роботі визначено поняття та структуру інформаційної безпеки в системі міжнародних відносин; розкрито роль Європейського Союзу у сфері глобальної та регіональної безпеки; виявлено гібридні загрози та зовнішні інформаційні впливи на ЄС.

У кваліфікаційній роботі визначено роль інституцій ЄС у забезпеченні інформаційної стійкості та нормативно-правове регулювання інформаційної безпеки ЄС; з'ясовано особливості співпраці ЄС із державами-членами та міжнародними партнерами у сфері інформаційної безпеки та інструменти протидії сучасним гібридним інформаційним загрозам ЄС; виокремлено проблеми імплементації стратегічних документів ЄС у сфері інформаційної безпеки та напрями вдосконалення політики інформаційної безпеки ЄС та її значення для України.

Ключові слова: інформаційна безпека, дезінформація, Європейський Союз, кібератаки, глобальна безпека, регіональна безпека.

ANNOTATION

Ilchenko L.O. Information Security of the European Union in Modern Conditions (master's work). Kharkiv: V.N. Karazin Kharkiv National University, 2025. 85 p. (manuscript).

The master's qualification work is devoted to determining the instruments for ensuring the information security of the European Union in modern conditions. The qualification work defines the concept and structure of information security in the system of international relations; reveals the role of the European Union in the sphere of global and regional security; identifies hybrid threats and external information influences on the EU.

The qualification work defines the role of EU institutions in ensuring information stability and regulatory regulation of EU information security; clarifies the features of EU cooperation with member states and international partners in the sphere of information security and tools for countering modern hybrid information threats to the EU; identifies problems of implementing EU strategic documents in the sphere of information security and directions for improving EU information security policy and its significance for Ukraine.

Keywords: information security, disinformation, European Union, cyberattacks, global security, regional security.

ВІДГУК

наукового керівника на кваліфікаційну роботу магістра
студента 2-го року навчання, другого (магістерського) рівня вищої освіти,
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», ОПП «Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних відносин»
Харківського національного університету імені В.Н. Каразіна
Ільченко Лілії Олександрівни
на тему:
«Інформаційна безпека Європейського Союзу в сучасних умовах»

Кваліфікаційна робота магістрантки Ільченко Лілії Олександрівни присвячена ґрунтовному аналізу сучасної політики інформаційної безпеки Європейського Союзу, дослідженню механізмів реагування на гібридні загрози та зовнішні інформаційні впливи, а також визначенню перспектив і значення європейського досвіду для України. Тема роботи є надзвичайно актуальною, оскільки інформаційна стійкість ЄС сьогодні безпосередньо пов'язана з безпекою демократичних процесів, стабільністю держав-членів та ефективністю зовнішньополітичної позиції Союзу, особливо в умовах російської агресії проти України.

Авторка продемонструвала високий рівень теоретичної підготовки та сформовані навички самостійного наукового пошуку. У роботі використано значний масив вітчизняних і зарубіжних джерел, офіційні документи ЄС, стратегічні матеріали Європейської комісії, ЄСЗД, ENISA, аналітичні звіти й сучасні дослідження з інформаційної безпеки. Структура роботи логічна, послідовна й повністю відповідає вимогам до магістерських досліджень.

Позитивним є поєднання у роботі теоретичного аналізу інформаційної безпеки, розгляду інституційної архітектури ЄС, аналізу нормативно-правових механізмів та оцінки практичних інструментів протидії гібридним загрозам. Авторка виявила глибоке розуміння сутності дезінформаційних операцій, кібератак, зовнішніх впливів на виборчі процеси, що становлять основу сучасних ризиків для Європейського Союзу. Чітко сформульовані висновки й практичні рекомендації підкреслюють уміння авторки узагальнювати результати дослідження та робити обґрунтовані аналітичні висновки.

Серед сильних сторін роботи варто виокремити логічно вибудувану структуру та комплексний аналіз інституцій Європейського Союзу разом із їхнім функціональним наповненням у сфері інформаційної безпеки. Авторка продемонструвала здатність поєднувати різні методологічні підходи, що підсилює аналітичну глибину дослідження. Важливою перевагою є також увага до сучасних викликів, зокрема пов'язаних із впливом штучного інтелекту та новими формами інформаційних операцій. Окремо слід підкреслити чітко сформульовані рекомендації щодо можливостей адаптації європейського досвіду в Україні, що надає роботі вагомого практичного значення.

У процесі підготовки роботи були виявлені й окремі аспекти, які можна вдосконалити. Зокрема, було б розширити порівняльні візуалізаційні матеріали (таблиці, схеми), що відобразили б різницю між підходами інституцій ЄС, а також детально опрацювати окремі практичні кейси реагування на інформаційні загрози. Проте ці зауваження мають рекомендаційний характер і не знижують загалом високої якості роботи.

У цілому кваліфікаційна робота магістрантки Ільченко Лілії Олександрівни є самостійним, змістовним і якісно виконаним дослідженням. Робота відповідає вимогам, встановленим до магістерських кваліфікаційних робіт за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», та заслуговує на високу оцінку (95 А). Робота може бути рекомендована до захисту перед екзаменаційною комісією.

Науковий керівник:
Кандидат політичних наук, доцент
Професор кафедри міжнародних відносин **Ольга ВИГОВСЬКА**

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студентки 2-го року навчання, другого (магістерського) рівня вищої освіти,
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», ОПП «Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних відносин»
Харківського національного університету імені В.Н. Каразіна
Ільченко Лілії Олександрівни
на тему:
«Інформаційна безпека Європейського Союзу в сучасних умовах»

Кваліфікаційна робота присвячена комплексному дослідженню теоретичних, нормативних, інституційних та практичних аспектів забезпечення інформаційної безпеки Європейського Союзу в умовах динамічного розвитку цифрових технологій та посилення гібридних загроз. Актуальність теми безсумнівна з огляду на зростання масштабів кібератак, дезінформаційних кампаній, зовнішніх впливів на демократичні процеси, а також необхідність зміцнення стійкості ЄС у контексті сучасних конфліктів, насамперед російсько-української війни. Авторка переконливо обґрунтовує значення інформаційної безпеки як ключового елементу європейської політики безпеки та підкреслює її важливість для України в умовах євроінтеграційного курсу.

Структура роботи логічно вибудувана й відповідає вимогам до магістерських досліджень. У трьох розділах послідовно розкрито теоретичні засади інформаційної безпеки, інституційно-правові й політичні інструменти Європейського Союзу, а також сучасні виклики та напрями подальшого розвитку інформаційної стратегії ЄС. Кожен розділ завершується змістовними висновками, що засвідчує вміння здобувачки узагальнювати матеріал і формувати цілісне бачення досліджуваної проблематики.

Наукова новизна роботи полягає у комплексному аналізі політики інформаційної безпеки ЄС через поєднання трьох ракурсів: теоретичного (структура та концепції інформаційної безпеки), інституційного (ролі Європейської комісії, ЄСЗД, ENISA, держав-членів) та практичного (інструменти реагування на гібридні загрози, механізми імплементації норм). Особливої уваги заслуговує аналіз сучасних викликів, включно з використанням штучного інтелекту у дезінформаційних операціях, впливом зовнішніх акторів та проблемами реалізації стратегічних документів ЄС.

Практична значущість роботи визначається можливістю застосування її результатів при формуванні рекомендацій щодо адаптації української політики інформаційної безпеки до стандартів ЄС, удосконаленні національних стратегічних документів та наближенні законодавства України до вимог цифрової та кібербезпекової політики Євросоюзу. Крім того, напрацювання авторки можуть бути використані у навчальному процесі з дисциплін з міжнародної безпеки, кіберполітики та сучасних інформаційних технологій у міжнародних відносинах.

Авторка продемонструвала ґрунтовну обізнаність із науковими джерелами та офіційними документами ЄС, використала широкий спектр літератури, аналітичних доповідей, нормативних актів, що сприяє академічній повноті роботи. Літературний огляд є змістовним і охоплює як українські, так і зарубіжні дослідження.

Разом з тим, окремі елементи могли б бути подані більш наочно, зокрема: включення порівняльних таблиць політик інформаційної безпеки різних інституцій ЄС або структурованих схем механізмів реагування на гібридні загрози. Аналіз впливу ШІ на інформаційну безпеку міг би бути розширений з огляду на стрімкий розвиток цієї тематики. Однак зазначені зауваження є рекомендаційними та не зменшують загальної позитивної оцінки дослідження.

Кваліфікаційна робота Ільченко Лілії Олександрівни є зрілим, логічно структурованим, науково виваженим та практично значущим дослідженням, яке повністю відповідає вимогам, встановленим до магістерських робіт за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Робота заслуговує на високу оцінку та може бути рекомендована до захисту з результатом А (95 балів).

Рецензент:
кандидат політичних наук,
завідувачка кафедри міжнародної інформації
Навчально-наукового інституту міжнародних відносин
Київського національного університету
імені Тараса Шевченка **Наталія БЄЛОУСОВА**