МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
ФАКУЛЬТЕТ ПРАВА ТА МІЖНАРОДНИХ ВІДНОСИН

Кафедра міжнародних відносин

Спеціальність 291 “Міжнародні відносини, суспільні комунікації та регіональні студії”
Освітня програма 291.00.01 “Суспільні комунікації”

БАКАЛАВРСЬКА РОБОТА
на тему:
ІНФОРМАЦІЙНА БЕЗПЕКА ЄВРОПЕЙСЬКОГО СОЮЗУ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Студентки 4 курсу
денної форми навчання
Моначиної Анастасії Олегівни

Науковий керівник:
кандидат наук з державного управління,
доцент кафедри міжнародних відносин
Пістракевич О.В

Київ - 2025

ЗМІСТ

ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ

ЄС – Європейський Союз

CER Directive – Директива про стійкість критичних об'єктів

CSIRT – Комп'ютерна група реагування на надзвичайні ситуації

DSA – Закон про цифрові послуги

EC3 – Європейський центр з боротьби з кіберзлочинністю

EEAS (ЄСЗС) – Європейська служба зовнішніх справ

ENISA – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки

GDPR – Загальний регламент про захист даних

Hybrid CoE – Європейський центр з протидії гібридним загрозам

NIS Directive 1, 2 – Директива про безпеку мереж та інформаційних систем 1,2

RAS – Система швидкого сповіщення про дезінформацію

SIAC – Єдина система розвідки

ВСТУП

Актуальність проблеми. Інформація у сучасному світі стала не просто важливим ресурсом, а стратегічним активом, що впливає на безпеку, розвиток економіки, політичні процеси та соціальні трансформації. У цифрову епоху інформація стає важливим чинником у формуванні державної політики, у забезпеченні національної та міжнародної безпеки, а також у підтримці соціальних та економічних систем. За останні роки, і особливо після початку повномасштабної війни між Російською Федерацією та Україною у 2022 році, інформаційна безпека стала центральним елементом європейської політики. Зі збільшенням інтенсивності кібератак, дезінформаційних кампаній і пропагандистських заходів, що мають на меті дестабілізацію політичних процесів, питання захисту інформаційного простору стало не лише проблемою технічного характеру, а й важливою складовою національної та колективної безпеки.

У світлі розвитку сучасних технологій та збільшення кількості гібридних загроз, інформаційна безпека стала однією з ключових складових національної та міжнародної безпеки. Російсько-українська війна, яка продовжує мати серйозні наслідки для Європейського Союзу, підкреслює критичну важливість ефективних механізмів захисту від інформаційних атак. Зокрема, в контексті цієї війни, боротьба за контроль над інформаційними потоками, дезінформація, вплив на громадську думку та політичні рішення стають одними з найбільших викликів для ЄС. Поява нових стратегій у галузі інформаційної безпеки, необхідність адаптації правових і політичних інструментів в умовах війни — усе це робить тему дослідження актуальною і значущою як для теоретичного, так і для практичного вивчення.

Гібридні загрози, до яких можна віднести не тільки військові дії, а й інформаційні операції, стали невід'ємною частиною міжнародних відносин

і безпеки. Це вимагає нових підходів до розуміння безпеки, коли інформаційні технології та комунікаційні мережі здатні змінювати хід військових конфліктів і навіть формувати нові політичні реалії. У таких умовах значення інформаційної безпеки виходить за межі традиційного розуміння її як захисту інформації тільки в рамках окремих держав. Вона стає важливою складовою інфраструктурної, економічної та політичної безпеки на рівні всього Європейського Союзу, що визначає необхідність нових підходів до її дослідження та вдосконалення її забезпечення.

Загалом, концепція інформаційної безпеки ЄС в умовах війни з Росією є багатогранною та включає в себе не тільки кібербезпеку, а й захист від політичних маніпуляцій, стратегічну комунікацію, захист інфраструктури, боротьбу з дезінформацією та багато інших аспектів. Одним із головних завдань цього дослідження є розкриття не тільки теоретичних основ цієї концепції, а й аналіз механізмів, які використовуються для її забезпечення на практиці.

Зважаючи на вищезазначене, дослідження інституційних та правових механізмів інформаційної безпеки ЄС допоможе сформувати більш чітке розуміння того, які виклики та загрози стоять перед Євросоюзом у цих умовах, а також визначити можливості для підвищення ефективності існуючих механізмів захисту. Тема також є важливою для визначення майбутніх стратегічних напрямків розвитку інформаційної безпеки ЄС у часи кризи та війни.

Об'єктом дослідження — забезпечення інформаційної безпеки Європейського Союзу.

Предметом дослідження виступають політичні, нормативно-правові, інституційні та стратегічні механізми забезпечення інформаційної безпеки ЄС в умовах російсько-української війни.

Мета дослідження — проаналізувати сучасний стан, виклики та перспективи розвитку інформаційної безпеки Європейського Союзу в умовах війни Росії проти України.

Завдання дослідження:

- дослідити стан наукової розробки проблеми та джерельну базу дослідження;
- проаналізувати понятійно-категоріальний апарат та методи дослідження;
- визначити політико-правові засади та інституційні механізми, що регламентують інформаційну безпеку ЄС;
- охарактеризувати основні стратегії та інструменти, які використовуються ЄС для забезпечення інформаційної безпеки;
- визначити ключові виклики та загрози інформаційній безпеці ЄС в умовах російсько-української війни, а також реакцію ЄС на ці загрози;
- висвітлити стратегічні перспективи забезпечення інформаційної безпеки ЄС.

Хронологічні межі дослідження охоплюють період з 2014 року — початку агресії Росії проти України — і до 2025 року. **Територіальні межі** охоплюють Росію, Україну, країни-члени ЄС та інституції Європейського Союзу.

Практичне значення дослідження полягає у можливості використання результатів роботи для розробки ефективних стратегій і механізмів захисту критичних інфраструктур, удосконалення освітніх програм у галузі європейських студій, міжнародних відносин та кібербезпеки, а також для підвищення рівня підготовки фахівців у зазначених сферах.

Теоретичне значення дослідження полягає в поглибленні наукового розуміння інформаційної безпеки як складової сучасної безпекової політики Європейського Союзу. Розроблені теоретичні підходи та

концептуальні моделі дозволяють глибше осмислити роль інформаційної безпеки в умовах сучасних гібридних загроз, а також окреслити нові напрями для подальших досліджень у сфері інтеграції інформаційної безпеки в загальну стратегію європейської безпеки.

Апробація роботи. Матеріали дослідження було представлено 15 травня 2025 року на 3 Міжнародній науково-практичній конференції «Research in Science, Technology and Economics» у секції «Міжнародні відносини» у рамках теми «Інформаційна безпека ЄС: відповіді на російську агресію та партнерство з Україною» та опубліковано в однойменному збірнику.

А також 4 червня 2025 року на 1 Міжнародній науково-практичній конференції «Modern Perspectives on Science and Economic Progress» у секції «Міжнародні відносини» у рамках теми «Інституційні механізми забезпечення інформаційної безпеки Європейського Союзу в умовах російсько-української війни» після чого теж опубліковано в однойменному збірнику.

Структура роботи. Бакалаврська робота складається зі вступу, трьох розділів, які розбиті на вісім підрозділів, висновків, списку використаних джерел та літератури у кількості 54 найменувань. Загальний обсяг роботи становить 60 сторінок.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ

1.1 Стан наукової розробки проблеми та джерельна база дослідження

У даному підрозділі проводиться огляд наукових досліджень та експертних публікацій, що стосуються проблеми інформаційної безпеки Європейського Союзу в умовах російсько-української війни. Огляд охоплює різні джерела, що дають змогу проаналізувати сучасний стан наукової розробки цієї проблеми, а також розглядає джерела, на яких побудоване дослідження, проведене в рамках підготовки цієї бакалаврської роботи.

Наукова література, що стосується теми інформаційної безпеки Європейського Союзу в умовах російсько-української війни, є досить різноманітною і включає монографії, статті в наукових журналах, а також дослідження, виконані в рамках міжнародних програм. Однак більшість робіт зосереджена на кібербезпеці, де інформаційна безпека розглядається переважно в технічному аспекті, з акцентом на захист комп'ютерних мереж, систем та даних.

Значна частина наукових досліджень стосовно інформаційної безпеки ЄС пов'язана із вдосконаленням нормативно-правових механізмів для боротьби з інформаційними загрозами. Ф. Хоффман, який у своїй праці "Гібридні загрози: переосмислення еволюційного характеру сучасного конфлікту" вказує, що інформаційні атаки, які поєднуються з кіберзагрозами, ставлять під загрозу демократичні процеси в ЄС. Важливим аспектом дослідження є аналіз регулювання на рівні ЄС щодо інформаційної безпеки, зокрема оновленої Директиви NIS2, яка була

спрямована на забезпечення більш ефективного захисту критичної інфраструктури від цифрових та інформаційних атак[1].

Крім того, дослідники з інформаційної безпеки, як-от А. Місюра та В. Паливода, активно розглядають проблеми боротьби з інформаційними загрозами у ЄС. Вони підкреслюють, що для ефективної боротьби з цим необхідна координація між державами-членами та європейськими інституціями, що дозволяє підвищити обізнаність про загрози та впроваджувати заходи для їх нейтралізації[2].

О. Фурсай вивчає аспекти інформаційної політики ЄС, акцентуючи увагу на розвитку правових норм, які забезпечують боротьбу з дезінформацією. Вона відзначає, що в умовах глобальних інформаційних загроз, особливо з боку Росії, ЄС активно вдосконалює законодавчу базу, що дозволяє регулювати поширення неправдивої інформації. Зокрема, Фурсай звертає увагу на стратегічні комунікації, які допомагають ЄС справлятися з дезінформаційними кампаніями, що стають важливим елементом гібридних загроз. Її дослідження підкреслюють значущість співпраці з міжнародними партнерами, такими як НАТО, у протидії інформаційним атакам, а також важливість активної ролі громадянського суспільства в контролі за інформаційною сферою[3].

У роботі Трояна Сергія "Інформаційно-безпекова політика Європейського Союзу" досліджується стратегія ЄС щодо забезпечення інформаційної безпеки в умовах сучасних загроз. Автор розглядає питання захисту інформаційних мереж та систем від зовнішніх впливів, зокрема

---

[1] Hoffman, Frank, "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict" (2009). *Strategic Forums*. URL: https://digitalcommons.ndu.edu/strategic-forums/40 (date of access: 02.02.2025).

[2] А.О Місюра, В.О Паливода. Концептуальні підходи НАТО та ЄС до забезпечення стійкості держави і суспільства у сфері національної безпеки. *Національний інститут стратегічних досліджень*. URL: https://niss.gov.ua/sites/default/files/2018-04/NATO-ES-stiykist-59383.pdf (date of access: 02.02.2025).

[3] Фурсай, О. (2023). ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ. *Літопис Волині*, (29), 165-170. https://doi.org/10.32782/2305-9389/2023.29.27

кіберзлочинності, а також створення умов для безпечного функціонування громадян, суспільства та держави в інформаційному просторі. Троян акцентує увагу на важливості правових засад і програм, спрямованих на протидію кіберзлочинності, а також на необхідності розробки й впровадження технічних засобів для підтримки національних та європейських систем безпеки. Крім того, він підкреслює значення інформаційної безпеки для забезпечення стабільності внутрішньої ситуації в ЄС, а також для боротьби з гібридними загрозами. Важливим аспектом є розвиток співпраці між країнами ЄС, приватним сектором і міжнародними партнерами для протидії кіберзлочинності та створення спільних систем реагування на загрози[4].

Паралельно з українськими дослідженнями, у наукових працях західних вчених, наприклад, Родерік Паркес, акцентує увагу на важливості інформаційної безпеки як одного з основних компонентів стратегічної безпеки ЄС. Вони розглядають роль ЄС у формуванні спільної стратегії з боротьби з гібридними загрозами, в тому числі й через механізми моніторингу та протидії дезінформації. Дослідники вважають, що Європейський Союз повинен активніше використовувати інструменти стратегічних комунікацій і залучати всі можливі ресурси для протидії зовнішнім інформаційним атакам. Вони також підкреслюють необхідність розширення законодавчої бази для забезпечення більш ефективного захисту інформаційного простору ЄС[5].

Водночас є дослідження, які більше фокусуються на аналітичних інструментах для боротьби з дезінформацією, зокрема матеріали від

---

[4] Троян С. Інформаційно-безпекова політика Європейського Союзу. *erNAU - Electronic Institutional Repository of the National Aviation University of Ukraine.* URL: https://er.nau.edu.ua/items/a0ff4b35-e55a-421a-8771-dad5dd77f1b9 (дата звернення: 11.02.2025).

[5] Daniel Fiott, Roderick Parkes. PROTECTING EUROPE: The EU's response to hybrid threats. *European Union Institute for Security Studies (EUISS)*. URL: https://www.jstor.org/stable/resrep21143.4 (date of access: 03.02.2025).

Європейської служби зовнішніх справ (EEAS), які вивчають ефективність платформ для виявлення та протидії дезінформації, як EUvsDisinfo. Це важливі дослідження для розуміння контексту і типів загроз, які стоять перед ЄС у межах російсько-української війни.

Важливу роль у дослідженні відіграють публікації міжнародних організацій. Європейський Союз активно працює над удосконаленням механізмів інформаційної безпеки, і однією з головних ініціатив є Стратегічний компас для безпеки та оборони ЄС, який є не лише політичним, а й правовим документом, що регламентує стратегії боротьби з гібридними загрозами. Зокрема, документ "2024 Progress Report on the Implementation of the Strategic Compass for Security and Defence" детально описує прогрес у реалізації стратегічних ініціатив[6].

Експертні публікації часто аналізують реакцію ЄС на зовнішні впливи, зокрема з боку Росії, і описують механізми реагування на дезінформацію. Hybrid CoE (Європейський центр з протидії гібридним загрозам) активно досліджує тактики Росії щодо поширення дезінформації та маніпуляцій у країнах Балтії та інших країнах ЄС. Одним із таких експертних звітів є Hybrid CoE Working Paper 32[7], що розкриває тактики Росії в Балтійському регіоні.

Офіційні документи та законодавчі акти, прийняті Європейським Союзом, є основою для розуміння правових і політичних засад у сфері інформаційної безпеки. Важливу роль відіграє Директива NIS2, яка встановлює загальні вимоги до забезпечення кібербезпеки та

[6] 2024 Progress Report on the Implementation of the Strategic Compass for Security and Defence. *EEAS*. URL: https://www.eeas.europa.eu/eeas/2024-progress-report-implementation-strategic-compass-security-and-defence-0_en (date of access: 14.03.2025).

[7] Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage - *The European Centre of Excellence for Countering Hybrid Threats*. URL: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/ (date of access: 14.03.2025).

інформаційної безпеки в країнах ЄС. Одним із ключових документів є також Закон про цифрові послуги (Digital Services Act, DSA), який визначає правила для великих цифрових платформ, що оперують на території ЄС.

Для аналізу стану інформаційної безпеки в Європейському Союзі важливе значення мають публікації в міжнародних новинних виданнях, оскільки вони дають можливість оцінити поточну ситуацію з різних точок зору. Одним із таких авторитетних джерел є Financial Times, яке регулярно публікує статті про кібербезпеку, вплив інформаційних атак на політичні процеси та економіку. Це видання дає короткий аналіз загроз та виявляє уразливі точки в інформаційній інфраструктурі ЄС, що дозволяє зрозуміти масштаби проблеми. Читачі можуть дізнатися про методи інформаційних війн, які використовуються державами, зокрема Росією, та їх вплив на демократичні процеси в Європі.

Інші відомі видання, такі як The New York Times та The Guardian, також зосереджуються на питанні інформаційної безпеки, надаючи важливі дослідження та коментарі експертів. Вони не лише висвітлюють конкретні інциденти, як-от кібератаки на урядові установи, а й аналізують стратегії захисту, що використовуються Європейським Союзом для боротьби з дезінформацією та шкідливими кібердіями.

Серед новинних видань, які активно висвітлюють теми інформаційної безпеки в ЄС, також варто відзначити Reuters та BBC News. Ці медіа пропонують новини, що стосуються міжнародних відносин, кібератак, а також розслідувань щодо втручання в вибори та зловживання інформацією для маніпулювання громадською думкою. Інколи ці видання публікують доповіді з різних європейських країн про поточний стан політики в галузі кібербезпеки, підкреслюючи важливість співпраці між державами для забезпечення стійкості до зовнішніх загроз.

З огляду на надані джерела, можна зробити висновок, що тема інформаційної безпеки Європейського Союзу є активно досліджуваною як в наукових, так і в експертних колах. Особливо важливими є роботи, що аналізують механізми боротьби з інформаційними атаками в умовах гібридних загроз. Однак, попри великий обсяг робіт, важливим є подальше вдосконалення стратегій ЄС у контексті цифрової безпеки та інформаційної стійкості, особливо в умовах зростання кількості дезінформаційних кампаній і не тільки.

Таким чином, наукова база з інформаційної безпеки ЄС в умовах російсько-української війни є достатньо розвинутою, але теми, пов’язані з новими механізмами захисту та адаптацією правових актів ЄС до нових викликів, потребують подальших досліджень. Більшість сучасних робіт фокусується на політичних та нормативних аспектах, що надають юридичний фундамент для практичних кроків щодо інформаційної безпеки.

1.2 Понятійно-категоріальний апарат та методи дослідження

Для дослідження інформаційної безпеки Європейського Союзу в умовах російсько-української війни важливо чітко визначити ключові терміни та методи, що використовуються у дипломній роботі. Вони є основою для аналізу складних взаємозв'язків між різними аспектами міжнародної безпеки, зокрема в контексті інформаційних загроз. Крім того, вивчення впливу зовнішніх факторів на безпеку інформаційного середовища ЄС потребує застосування спеціальних методів дослідження, що дозволяють ефективно оцінити ці виклики та стратегії захисту.

У рамках цієї роботи розглядаються ключові поняття, що мають важливе значення для розуміння теми.

Інформаційна безпека — це стан захищеності інформаційного середовища від загроз, які можуть впливати на конфіденційність,

цілісність, доступність та достовірність інформації. Інформаційна безпека є важливою складовою національної та міжнародної безпеки, оскільки забезпечує стабільність політичних, економічних і соціальних структур. За визначенням Європейського Союзу, інформаційна безпека включає захист інформації та інформаційних систем від несанкціонованого доступу, зміни, знищення або будь-якої іншої несанкціонованої дії. Важливим аспектом є також захист від загроз, що можуть виникати внаслідок кіберзагроз або гібридних атак[8].

Згідно з Директивою (ЄС) 2016/1148, кібербезпека визначається як здатність захищених мережевих і інформаційних систем протистояти загрозам, які можуть поставити під сумнів доступність, автентичність, цілісність або конфіденційність даних, що обробляються чи зберігаються цими системами, а також послуг, які вони надають[9].

Інформаційна війна — це сукупність стратегій і заходів, спрямованих на використання інформації як інструмента політичного та військового впливу. Це включає дезінформацію, маніпулювання громадською думкою, пропаганду з метою досягнення конкретних цілей. Інформаційна війна є особливо актуальною в умовах сучасних гібридних загроз, коли інформаційний простір стає важливим елементом національної та міжнародної безпеки[10].

---

[8] Information security. *European Data Protection Supervisor*. URL: https://www.edps.europa.eu/data-protection/data-protection/reference-library/information-security_en (date of access: 05.02.2025).

[9] Directive (EU) 2016/1148 of Cybersecurity of network and information systems *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX:32016L1148#:~:text=KEY%20TERMS%20*%20Cybersecurity:%20the%20ability%20of,for%20example%20water%20supply,%20electricity%20services,%20etc. (date of access: 05.02.2025).

[10] Joint Framework on countering hybrid threats a European Union response. *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018 (date of access: 05.02.2025).

Дезінформація — це свідомо неправдива або оманлива інформація, яка поширюється з метою обману, часто для досягнення політичних або економічних вигод, і може завдати шкоди громадськості[11].

Для вивчення проблеми інформаційної безпеки ЄС використовуються різні методи. Емпіричні методи включають спостереження, яке дозволяє фіксувати факти й події, що відбуваються в реальному часі у сфері інформаційної безпеки ЄС. Наприклад, спостереження за реакцією ЄС на інформаційні атаки з боку Росії допомагає оцінити ефективність політичних і правових заходів. Порівняння використовується для аналізу різних підходів до забезпечення інформаційної безпеки в країнах ЄС, а також для порівняння практик управління кіберзагрозами в різних політичних та правових системах.

Аналіз і синтез — аналізуються різні аспекти інформаційної безпеки, починаючи від теоретичних концепцій до конкретних механізмів їх реалізації в ЄС. Наприклад, синтезуються стратегії безпеки, розроблені у відповідь на конкретні загрози. Індукція та дедукція: ці методи використовуються для виведення загальних висновків з конкретних фактів та застосування загальних принципів до окремих випадків, що дозволяє сформулювати рекомендації для посилення безпеки.

Узагальнюючі методи використовується для формулювання загальних теоретичних висновків на основі спостережень та аналізу, що дозволяє вивести основні принципи та стратегії в контексті забезпечення інформаційної безпеки ЄС.

Методи прогнозування використовуються для визначення потенційних загроз для інформаційної безпеки ЄС у майбутньому, враховуючи сучасні тенденції в міжнародних відносинах.

---

[11] Tackling online disinformation. *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation (date of access: 04.02.2025).

Застосування саме цих різноманітних методів дозволяє глибше зрозуміти механізми інформаційної безпеки ЄС та їх взаємозв'язок з поточними міжнародними кризами. Використання емпіричних, теоретичних і спеціалізованих методів дозволяє не тільки дослідити теоретичні основи, але й зробити конкретні висновки про ефективність заходів, що вживаються для забезпечення безпеки в умовах геополітичної нестабільності. Вибір методів для даного дослідження обґрунтований необхідністю не тільки оцінити поточний стан, але й спрогнозувати майбутні виклики для ЄС у сфері інформаційної безпеки.

Отже, огляд наукової розробки проблеми показав, що тема є надзвичайно актуальною та активно вивчається. Як українські, так і західні дослідники, експерти та офіційні інституції ЄС приділяють значну увагу питанням інформаційної безпеки, вдосконаленню нормативно-правової бази для протидії інформаційним загрозам, зокрема в контексті гібридних атак та дезінформації. Було підкреслено важливість координації між державами-членами ЄС, роль стратегічних комунікацій та співпраці з міжнародними партнерами. Незважаючи на значний обсяг проведених досліджень, виявлено потребу в подальшому вивченні нових механізмів захисту та адаптації законодавства ЄС до динамічних викликів, зумовлених зростанням кількості дезінформаційних кампаній.

Для забезпечення глибини та систематичності дослідження, було чітко визначено понятійно-категоріальний апарат, що включає ключові терміни: інформаційна безпека, кібербезпека, інформаційна війна та дезінформація. Ці дефініції стали основою для подальшого аналізу. Методологічна база дослідження поєднала емпіричні (спостереження, порівняння) та теоретичні (аналіз і синтез, індукція та дедукція, узагальнюючі) методи. Такий багатогранний підхід дозволяє не тільки оцінити поточний стан інформаційної безпеки ЄС, але й встановити взаємозв'язки між різними аспектами міжнародної безпеки в умовах інформаційних загроз. Це є

критично важливим для розуміння механізмів захисту та їх ефективності в умовах поточної геополітичної нестабільності, зокрема в контексті російсько-української війни.

РОЗДІЛ 2

КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄС

2.1 Політична та нормативно-правова основа інформаційної безпеки ЄС

Інформаційна безпека стала однією з ключових сфер діяльності Європейського Союзу в умовах нових викликів, які виникають через активізацію гібридних воєн та посилення інформаційних загроз. Російсько-українська війна, яка розпочалася у 2014 році й перейшла у фазу повномасштабного вторгнення у 2022 році, висвітлила вразливості інформаційного простору не лише України, але й усіх держав-членів ЄС. У цих умовах Європейський Союз активно адаптує свої політичні ініціативи та нормативно-правову базу для забезпечення інформаційної стійкості, захисту критичної інфраструктури, а також боротьби з дезінформацією.

Політична складова інформаційної безпеки ЄС включає розробку довгострокових стратегій, що спрямовані на консолідацію зусиль усіх країн-членів для спільного реагування на виклики в інформаційному просторі. Першою спробою Європейського Союзу встановити єдині правила кібербезпеки стала Директива про безпеку мереж та інформаційних систем (NIS Directive), ухвалена у 2016 році. Це була перша загальноєвропейська нормативна база, спрямована на зміцнення кібербезпеки держав-членів та покращення їхньої здатності реагувати на кібератаки. Директива вимагала від країн розробки національних стратегій кібербезпеки, створення спеціалізованих органів – груп реагування на інциденти у сфері комп’ютерної безпеки (CSIRT), а також запровадження механізмів контролю та співпраці між державами. Вона була орієнтована насамперед на операторів критичної інфраструктури, зокрема енергетичного, транспортного, фінансового, медичного секторів та

цифрових послуг, зобов'язуючи їх підвищувати рівень безпеки та звітувати про значні інциденти.

Попри значний внесок у формування єдиної безпекової політики ЄС, директива NIS мала низку недоліків, зокрема недостатню деталізацію вимог, слабкі механізми моніторингу та відсутність чітких санкцій за порушення. Крім того, стрімкий розвиток цифрових технологій, зростання кількості та складності кібератак, а також гібридні загрози, які посилилися внаслідок пандемії COVID-19 та війни Росії проти України, виявили потребу в суттєвому оновленні законодавства. У відповідь на ці виклики 16 грудня 2020 року Європейська комісія запропонувала оновлену Директиву NIS2, яка передбачала значне посилення вимог до кіберзахисту, розширення переліку секторів, що підпадають під регулювання, а також запровадження суворішої відповідальності для підприємств та національних органів.

Робота над новим документом тривала понад рік, і в травні 2022 року Рада ЄС та Європейський парламент досягли політичної згоди щодо тексту директиви. 16 січня 2023 року NIS2 офіційно набула чинності, а держави-члени отримали два роки для імплементації її положень у національне законодавство. Основні нововведення NIS2 включають: обов'язкове проведення регулярних аудитів кібербезпеки, посилення вимог до управління ризиками, впровадження нових механізмів контролю та звітності, а також розширення переліку суб'єктів, на які поширюються правила директиви[12]. Важливим аспектом стало створення Європейської мережі органів з кіберкризового управління (EU-CyCLONe), яка координує дії у разі масштабних кібератак.

Одночасно з ухваленням NIS2 Європейський Союз приділив увагу зміцненню фізичної безпеки критичних об'єктів, що є невід'ємною

[12] NIS2 Directive: new rules on cybersecurity of network and information systems. *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (date of access: 05.02.2025).

складовою кіберзахисту. Директива про стійкість критичних об'єктів (CER Directive), ухвалена разом із NIS2 та чинна з 16 січня 2023 року, спрямована на посилення безпеки ключових інфраструктурних об’єктів, включаючи енергетику, транспорт та охорону здоров’я. Вона встановлює нові вимоги до оцінки ризиків, забезпечення захисту від фізичних загроз, таких як теракти, природні катастрофи чи диверсії, а також передбачає співпрацю між країнами-членами для протидії транскордонним загрозам.

Всі ці заходи є частиною ширшої Стратегії кібербезпеки для цифрового десятиліття, яку Європейська комісія представила 16 грудня 2020 року та яка набула чинності у січні 2023 року. Ця стратегія визначає основні напрямки розвитку цифрової безпеки ЄС до 2030 року, зокрема зміцнення захисту критичних секторів, розвиток кіберстійкості держав та бізнесу, підвищення рівня міжнародного співробітництва у сфері кібербезпеки[13].

Важливим доповненням до цієї стратегії стало ухвалення Європейським Союзом Акта про кібербезпеку, який запроваджує систему сертифікації для цифрових продуктів і послуг. Це дозволяє підвищити довіру користувачів і бізнесу, забезпечуючи відповідність сертифікованих продуктів високим стандартам безпеки. Окрім того, акт встановлює обов’язкові вимоги до виробників і розробників програмного забезпечення, що є особливо актуальним на тлі зростання кібератак, зокрема з використанням вразливостей у ПЗ. Це питання набуло ще більшої значущості в контексті російсько-української війни, яка продемонструвала необхідність посилення контролю та захисту цифрового простору ЄС[14].

---

[13] The EU’s Cybersecurity Strategy for the Digital Decade. *Shaping Europe’s digital future*. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (date of access: 06.03.2025).

[14] The EU Cybersecurity Act. *Shaping Europe’s digital future*. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (date of access: 08.02.2025).

Загальний регламент захисту даних (GDPR) також є одним із найжорсткіших законів щодо конфіденційності та безпеки даних у світі. Хоча він був розроблений і прийнятий Європейським Союзом, його вимоги поширюються на організації по всьому світу, якщо вони обробляють дані осіб, які перебувають у ЄС, або пропонують товари чи послуги для таких осіб. Регламент набрав чинності 25 травня 2018 року, і з того часу компанії, що не дотримуються вимог, можуть бути оштрафовані на великі суми, що досягають десятків мільйонів євро.

GDPR визначає основні принципи захисту даних, які повинні бути дотримані під час обробки персональних даних. Це включає правомірність, добросовісність і прозорість обробки, обмеження цілей, мінімізацію даних, точність, обмеження зберігання, цілісність і конфіденційність. Важливою частиною є також відповідальність: організації повинні бути здатні продемонструвати свою відповідність вимогам регламенту.

Регламент також надає нові права для осіб, чиї дані обробляються, зокрема право на доступ, виправлення, видалення, обмеження обробки, переносимість даних та право на заперечення. Всі ці зміни покликані дати громадянам більше контролю над своїми персональними даними, що особливо важливо в епоху цифрових технологій[15].

Таким чином, ЄС невпинно зміцнює свою політику інформаційної безпеки, реагуючи на сучасні виклики: кібератаки, гібридні загрози та дезінформаційні кампанії. Російсько-українська війна стала каталізатором масштабних змін, що сприяли прийняттю директив NIS2 і CER, а також посиленню кібербезпекових стандартів для критично важливої інфраструктури. Крім того, GDPR встановлює суворі вимоги до захисту

[15] What is GDPR, the EU’s new data protection law? - *GDPR.eu*. URL: https://gdpr.eu/what-is-gdpr/ (date of access: 14.02.2025).

даних і цифрових технологій, що підвищує стійкість європейського цифрового простору.

Однак загрози залишаються динамічними, і ЄС продовжує адаптувати свої механізми захисту. Важливим аспектом залишаються стратегії боротьби з дезінформацією, зокрема через запровадження нових регуляторних ініціатив. ЄС також активно продовжує працювати над зміцненням кіберстійкості, розвитку аналітичних спроможностей та посилення міжнародної співпраці для протидії новим цифровим загрозам.

2.2 Інституційні механізми забезпечення інформаційної безпеки ЄС

Інформаційна безпека Європейського Союзу в умовах російсько-української війни є критично важливою для захисту суспільної довіри, демократичних процесів і єдності країн-членів. Російські дезінформаційні кампанії, пропаганда та гібридні загрози, спрямовані на маніпуляцію інформаційним простором, створюють серйозні виклики для ЄС. Для протидії цим загрозам ЄС створив комплексну систему інституційних механізмів, що включає спеціалізовані агентства, координаційні платформи та національні органи. Ці структури забезпечують моніторинг інформаційних загроз, протидію дезінформації та координацію зусиль між країнами-членами.

Європейська служба зовнішніх справ (EEAS) є центральною інституцією ЄС, відповідальною за реалізацію спільної зовнішньої та безпекової політики. В контексті інформаційної безпеки EEAS виконує критичну функцію протидії зовнішнім дезінформаційним впливам, насамперед з боку Росії, Китаю та інших авторитарних держав. У межах EEAS створено спеціальну Гібридну клітинку (Hybrid Fusion Cell), яка аналізує загрози гібридного характеру, зокрема інформаційні кампанії,

дезінформацію, вплив через соціальні медіа, а також координує міжвідомчу відповідь на такі загрози на рівні всього ЄС[16].

У оновленому Стратегічному компасі ЄС (Strategic Compass 2024) наголошується на провідній ролі EEAS у підвищенні інформаційної стійкості країн-членів та партнерів. Зокрема, значна увага боротьбі з дезінформацією, яка стала потужним інструментом у війні. З 2015 року функціонує East StratCom Task Force — спеціальна група в межах Європейської служби зовнішньої діяльності. Вона працює у трьох основних напрямках: стратегічна комунікація, підтримка незалежних медіа та викриття дезінформації[17].

Вона аналізує та спростовує фейки через платформу EUvsDisinfo, яка містить тисячі задокументованих випадків прокремлівської пропаганди. Крім того, група координує комунікаційні кампанії, що пояснюють політику ЄС, особливо у країнах Східного партнерства, таких як Україна, Сакартвело та Молдова[18].

Окрему увагу приділяють підвищенню обізнаності про методи інформаційних маніпуляцій. East StratCom Task Force розробляє звіти та аналітику для урядів і громадянського суспільства, що дозволяє краще розуміти загрози та реагувати на них. Також вони підтримують незалежні медіа та журналістів, які працюють у регіонах, де інформаційний простір піддається найбільшій загрозі з боку дезінформаційних кампаній.

Завдяки цій роботі вдалося викрити та нейтралізувати сотні маніпулятивних наративів, спрямованих на дискредитацію ЄС, НАТО та демократичних цінностей. Група продовжує адаптувати свої методи,

---

[16] A Europe that protects: good progress on tackling hybrid threats. *European Commission*. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2788 (date of access: 13.03.2025).

[17] 2024 Progress Report on the Implementation of the Strategic Compass for Security and Defence. *EEAS*. URL: https://www.eeas.europa.eu/eeas/2024-progress-report-implementation-strategic-compass-security-and-defence-0_en (date of access: 14.03.2025).

[18] About. *EUvsDisinfo*. URL: https://euvsdisinfo.eu/about/ (date of access: 20.02.2025).

використовуючи новітні технології для аналізу даних, співпрацюючи з партнерами та розширюючи свою діяльність у відповідь на нові виклики в інформаційному просторі[19].

Крім того, EEAS координує політичну та інституційну взаємодію у рамках ініціативи Східного партнерства у посиленні їхньої інформаційної безпеки. EEAS надає експертну підтримку у розробці стратегій боротьби з інформаційними атаками, впровадженні стандартів стратегічної комунікації та розвитку національних систем інформаційної стійкості[20]. Ці зусилля є частиною ширшої політики ЄС щодо захисту демократичних інститутів, вільних виборів і прав людини в умовах гібридних викликів.

Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) було створене в 2004 році відповідно до Регламенту ЄС № 460/2004[21] як відповідь на потребу у зміцненні кібер- та інформаційної безпеки в Європейському Союзі. Після декількох змін у мандаті та статусі, у 2019 році ENISA отримала постійний статус та розширений мандат на підставі Cybersecurity Act[22].

Основне завдання ENISA полягає у підтримці держав-членів та інституцій ЄС у впровадженні сучасних політик інформаційної безпеки, підвищенні кіберстійкості, розвитку стандартів та сертифікаційних схем у сфері ІКТ[23].

---

[19] Questions and Answers about the East StratCom Task Force. *EEAS*. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11234 (date of access: 24.02.2025).
[20] Eastern Partnership. *EEAS*. URL: https://www.eeas.europa.eu/eeas/eastern-partnership_en (date of access: 18.03.2025).
[21] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). *EUR-Lex*. (date of access: 16.03.2025).
[22] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *EUR-Lex*. 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng (date of access: 15.03.2025).
[23] The EU Cybersecurity Act. *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (date of access: 14.03.2025).

ENISA не лише розробляє рекомендації щодо захисту інформації, а й координує міждержавні навчання з реагування на інциденти, організовує загальноєвропейські кібернавчання (наприклад, Cyber Europe), аналізує тенденції та ризики в інформаційному просторі, а також консультує інституції ЄС щодо стратегічних питань безпеки. Особливу увагу ENISA приділяє роботі з дезінформацією, захистом критичної інформаційної інфраструктури та інформаційним аспектам гібридних загроз — особливо в контексті російсько-української війни[24].

Крім технічних і політичних функцій, ENISA активно працює в освітньому напрямку — створює аналітичні звіти, навчальні матеріали, глосарії термінів і платформи для обміну досвідом. Наприклад, агентство запровадило систему сертифікації, яка допомагає користувачам і компаніям розуміти, які продукти відповідають стандартам безпеки. Також ENISA координує співпрацю між національними CSIRT (командами реагування на комп'ютерні інциденти), забезпечуючи синергію у випадку масштабних атак на інформаційний простір ЄС[25].

Європейський центр із протидії гібридним загрозам (Hybrid CoE), розташований у Гельсінкі, є міжурядовим аналітичним центром, створеним у 2017 році за ініціативи ЄС і НАТО для підтримки держав-членів у виявленні, аналізі та протидії гібридним загрозам. Його діяльність зосереджена на дослідженні таких аспектів, як інформаційні операції, кіберактивність, впливові кампанії, економічний тиск, а також правові та воєнні інструменти гібридного впливу. Центр об'єднує понад 30

---

[24] What we do | ENISA. *Home.* URL: https://www.enisa.europa.eu/about-enisa/what-we-do (date of access: 19.03.2025).

[25] 2023 CONSOLIDATED ANNUAL ACTIVITY REPORT. 2024. 178 p. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/2023%20Consolidated%20Annual%20Activity%20Report_1.pdf (date of access: 19.03.2025).

країн-партнерів та відіграє провідну роль у формуванні спільної європейської політики протидії гібридним викликам[26].

У 2024 році Hybrid CoE опублікував спеціальний звіт, присвячений російським інформаційним кампаніям, спрямованим на дестабілізацію політичних процесів у країнах Балтії. Аналіз у звіті вказує на широке використання фейкових новин, ботоферм, деструктивних наративів у соціальних мережах, а також маніпуляцію емоційно чутливими темами (напр., етнічні питання, мова, історія). Центр наводить конкретні приклади використання платформ TikTok, VK та Telegram для поширення дезінформації, зокрема щодо присутності НАТО в регіоні та підтримки України[27].

Важливою частиною роботи Hybrid CoE є організація тренінгів, симуляційних навчань і семінарів для аналітиків, державних службовців та журналістів. У межах партнерства з Україною, Центр сприяє обміну досвідом у сфері ідентифікації й деконструкції пропагандистських наративів, а також допомагає розробляти національні стратегії інформаційної стійкості. Окрім того, Hybrid CoE активно взаємодіє з НАТО та Європейською службою зовнішніх справ (EEAS), забезпечуючи координацію стратегічної комунікації на рівні ЄС і посилення інституційного реагування на гібридні інформаційні загрози[28].

---

[26] About us - Hybrid CoE. *The European Centre of Excellence for Countering Hybrid Threats*. URL: https://www.hybridcoe.fi/about-us/ (date of access: 20.03.2025).

[27] *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage - The European Centre of Excellence for Countering Hybrid Threats. URL: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/* (date of access: 14.03.2025).

[28] Hybrid CoE continues to work to support European security and Ukraine. *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats*. URL: https://www.hybridcoe.fi/news/hybrid-coe-continues-to-work-to-support-european-security-and-ukraine/ (date of access: 30.03.2025).

Система швидкого оповіщення (Rapid Alert System) була створена у 2019 році Європейською Комісією як ключовий елемент механізму захисту демократичних процесів в ЄС. Вона дозволяє державам-членам, інституціям ЄС та зовнішнім партнерам оперативно обмінюватися інформацією про загрози, пов'язані з дезінформацією, особливо в контексті виборів, пандемій чи конфліктів. Система функціонує як внутрішня платформа обміну попередженнями, прикладами наративів та індикаторами координації інформаційних атак[29].

Європейський центр боротьби з кіберзлочинністю (EC3), як структурний підрозділ Європолу, було засновано у 2013 році для координації зусиль проти тяжких форм кіберзлочинності, включаючи кіберзлочини, що супроводжують інформаційні атаки. Центр спеціалізується на боротьбі з хактивізмом, фішингом, зломом медіаінфраструктури, незаконним поширенням контенту та фінансовими схемами, які можуть бути частиною гібридних операцій. Особливо після початку повномасштабної агресії Росії проти України, EC3 розширив увагу до злочинів, які підтримують дезінформацію і втручання в інформаційний простір ЄС[30].

Таким чином, Європейський Союз сформував багаторівневу систему інституційного захисту інформаційного простору, яка охоплює стратегічні, аналітичні, оперативні та правоохоронні виміри. EEAS, ENISA, Hybrid CoE, Rapid Alert System та EC3 працюють у взаємодії, забезпечуючи не лише виявлення та нейтралізацію інформаційних загроз, але й формування стійкості демократичних суспільств до зовнішніх впливів. Кожна з цих структур виконує унікальну функцію — від стратегічної комунікації до

---

[29] Factsheet: Rapid Alert System. *EEAS*. URL: https://www.eeas.europa.eu/node/59644_en (date of access: 02.04.2025).

[30] European Cybercrime Centre - EC3 | Europol. *Europol*. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (date of access: 29.03.2025).

кримінального переслідування, що дозволяє ЄС діяти скоординовано та ефективно в умовах гібридної війни.

Особливої ваги ці інституційні механізми набули після початку повномасштабної агресії Росії проти України, коли інформаційна безпека стала питанням не лише цифрового, а й геополітичного виживання. Синергія між державами-членами, підтримка партнерських країн (зокрема України), а також гнучкість і адаптивність у реагуванні на нові загрози є визначальними чинниками стійкості ЄС у сучасному інформаційному середовищі.

2.3 Стратегії інформаційної безпеки ЄС

Стратегії інформаційної безпеки Європейського Союзу формуються як відповідь на цілеспрямовані зовнішні інформаційні впливи, зокрема дезінформацію, маніпуляцію громадською думкою та пропаганду, які використовуються з метою підриву демократичних процесів. У відповідь на зростання зовнішнього впливу на громадську думку, втручання у виборчі процеси та поширення цілеспрямованої дезінформації, ЄС формує багаторівневі підходи до захисту свого інформаційного простору. Ці підходи поєднують політичні, нормативні та оперативні механізми, спрямовані на запобігання маніпулятивним кампаніям, зміцнення суспільної стійкості та забезпечення демократичного контролю над інформаційними потоками. Стратегії розвиваються у постійній динаміці — з урахуванням нових викликів, змін технологічного середовища та посилення загроз з боку авторитарних режимів.

«Стратегічний компас» Європейського Союзу, представлений у 2022 році, є ключовим стратегічним документом у сфері безпеки й оборони, який окреслює амбітну програму зміцнення європейської спроможності діяти в умовах багатовекторних загроз. У цьому документі інформаційна безпека розглядається як критично важливий компонент колективної

стійкості країн-членів. Зокрема, підкреслюється, що інформаційні операції, зокрема дезінформація, маніпуляція фактами, вплив через соціальні мережі та інші цифрові засоби, є складовою гібридної війни, яка ставить під загрозу стабільність демократичних суспільств ЄС.

У розділі, присвяченому гібридним загрозам, "Стратегічний компас" чітко зазначає, що Росія, а також інші авторитарні режими, систематично використовують інформаційні впливи як інструмент політичного тиску та дестабілізації. Особлива увага приділяється інформаційним атакам під час виборчих кампаній, впливу на громадську думку щодо санкційної політики, а також поширенню антиєвропейських і антиукраїнських наративів. У відповідь на це ЄС зобов'язався розвивати спільну ситуаційну обізнаність, посилювати стратегічну комунікацію, а також розширювати аналітичні спроможності в межах EEAS та інших відповідних інституцій.

Також у документі зазначається необхідність координації зусиль у межах так званого «інформаційного захисту демократії» — комплексної політики, спрямованої на виявлення та протидію спробам маніпулювати інформацією ззовні. Таким чином, Strategic Compass встановлює принципову рамку, в якій інформаційна безпека є не лише технічним або кібернетичним, а передусім політичним і стратегічним пріоритетом ЄС[31].

У рамках реалізації стратегічного курсу з інформаційної безпеки Європейська служба зовнішніх справ (EEAS) відіграє провідну роль у координації заходів з виявлення, аналізу та протидії зовнішнім дезінформаційним впливам. Сторінка EEAS, присвячена гібридним загрозам, акцентує увагу на тому, що поширення неправдивої або маніпулятивної інформації стало одним із найнебезпечніших інструментів зовнішнього впливу на європейські демократії. Особливо це стосується кампаній, пов'язаних з Росією, які систематично намагаються

[31] Strategic Compass - A Strategic Compass for Security and Defence. *EEAS,* 2022. URL: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf, P. 17–21 (date of access: 01.04.2025).

дестабілізувати політичну ситуацію в державах-членах, а також дискредитувати політику ЄС щодо України.

У відповідь на ці виклики EEAS впроваджує механізми стратегічної комунікації, аналітичного моніторингу та партнерської взаємодії. Центральну роль у цьому процесі відіграє група East StratCom Task Force, створена у 2015 році, яка щоденно аналізує інформаційні потоки, ідентифікує дезінформаційні наративи, веде базу даних EUvsDisinfo і підтримує країни Східного партнерства у посиленні власної інформаційної стійкості.

Водночас EEAS визнає, що боротьба з дезінформацією — це не лише питання безпеки, а й захисту прав людини, свободи слова та цифрової етики. Тому основою її підходу є не цензура, а прозорість, викриття джерел дезінформації, просування фактів та підвищення довіри до незалежних медіа[32].

У межах стратегії інформаційної безпеки ЄС важливу роль відіграє ініціатива Digital Decade, яка закладає основи для формування цифрового та стійкого європейського суспільства до 2030 року. Вона визначає чотири ключові напрями: розвиток цифрових навичок, цифровізацію бізнесу, інфраструктури та публічних послуг. З точки зору інформаційної безпеки, особливе значення мають цілі, пов’язані з цифровою грамотністю населення, подоланням диспропорцій у доступі до цифрових ресурсів та формуванням кадрового резерву з достатнім рівнем спеціалізованих знань у сфері цифрових технологій.

За даними Звіту про стан цифрового десятиліття за 2024 рік, лише 55,6% громадян ЄС мають базові цифрові навички, хоча стратегічна мета передбачає досягнення рівня у 80% до 2030 року. Такий рівень обізнаності є критично важливим для інформаційної безпеки, оскільки низький рівень

[32] Action Plan against Disinformation. *EUR-Lex*. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0036 (date of access: 02.04.2025).

цифрової грамотності значно підвищує вразливість суспільства до дезінформаційних впливів, онлайн-маніпуляцій і пропаганди. Програма також передбачає інтенсивну підготовку кадрів — до 2030 року кількість кваліфікованих фахівців у сфері ІКТ має зрости до 20 мільйонів осіб, з акцентом на подолання гендерного дисбалансу в секторі. Це безпосередньо стосується формування інституційної спроможності країн-членів забезпечувати захист інформаційного простору.

Крім того, у рамках "шляху до цифрового десятиліття" запроваджено нову модель управління, яка передбачає щорічну координацію між Єврокомісією та державами-членами. Вона має на меті не лише контроль за досягненням цифрових цілей, а й створення умов для масштабних міждержавних проектів, спрямованих на підвищення стійкості цифрової екосистеми ЄС. Таким чином, Digital Decade слугує стратегічною платформою не тільки для цифрової трансформації, а й для розбудови інформаційного імунітету суспільства, що є основою ефективної інформаційної безпеки[33].

Презентована Європейською Комісією у 2025 році стратегія ProtectEU відображає оновлений підхід ЄС до внутрішньої безпеки в умовах поглиблення гібридних загроз, включно з інформаційними атаками з боку недружніх держав і підконтрольних їм акторів. Ця стратегія, розроблена як відповідь на зміну геополітичного ландшафту та повернення великомасштабної війни на європейський континент, передбачає комплекс заходів із підвищення стійкості суспільства до маніпуляцій, дезінформації та атак на критичну інфраструктуру, в тому числі — інформаційну.

ProtectEU формує політику інформаційної безпеки через запровадження системного підходу до боротьби з гібридними впливами. Серед ключових ініціатив — посилення захисту цифрових платформ,

[33] Digital Decade. *Digital Skills and Jobs Platform*. URL: https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/digital-decade (date of access: 03.04.2025).

телекомунікаційних і хмарних сервісів, а також створення умов для зниження залежності від постачальників, що потенційно становлять ризик безпеці. Особливу увагу приділено імплементації директив CER і NIS2 у державах-членах, що дозволить побудувати цілісну систему захисту критичних інформаційних потоків. У цьому ж контексті ЄС також працює над посиленням технологічного суверенітету, зокрема шляхом перегляду правил державних закупівель та забезпечення кіберстійкості транспортних хабів.

Важливою складовою стратегії є оновлений механізм оцінки внутрішніх загроз, що дозволяє в режимі реального часу виявляти спроби втручання в інформаційний простір та координувати відповідь на рівні всієї Спілки. Для цього зміцнюється аналітична спроможність ЄС через Єдину систему розвідки (SIAC) та регулярні звіти про загрози. У межах співпраці з іншими інституціями ЄС — насамперед EEAS і Europol — ProtectEU спрямовує зусилля на посилення інформаційної інтеграції, обмін даними та формування єдиної політики реагування на інформаційні інциденти.

Таким чином, хоча ProtectEU є документом із ширшим безпековим охопленням, інформаційна безпека в ньому виступає як структурна складова сучасної моделі безпеки: не як ізольована сфера, а як центральний вектор боротьби з гібридними викликами, що поєднує технологічні, нормативні та соціальні аспекти[34].

Європейський Союз сформував цілісну стратегічну рамку інформаційної безпеки як відповідь на зростання гібридних загроз, зокрема дезінформаційних атак з боку Росії. Стратегічний компас, ініціативи EEAS, Digital Decade та стратегія ProtectEU демонструють, що інформаційна безпека розглядається як політичний і безпековий пріоритет.

---

[34] Commission unveils ProtectEU – a new European Internal Security Strategy. *European Commission*. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920 (date of access: 08.04.2025).

Вона охоплює розвиток цифрових навичок, захист критичної інфраструктури, прозорість інформаційного простору та підтримку демократичної стійкості. ЄС поєднує аналітику, регулювання й освіту для послідовної протидії зовнішнім інформаційним впливам.

РОЗДІЛ 3

ВПЛИВ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ЄС

3.1 Виклики та загрози інформаційній безпеці ЄС

На тлі повномасштабної агресії Росії проти України інформаційна безпека ЄС зазнала цілеспрямованих атак. На відміну від кібербезпеки, яка здебільшого охоплює технічний захист комп’ютерних мереж, систем та даних, інформаційна безпека зосереджується на збереженні достовірності, цілісності та суспільної довіри до інформації, що циркулює в публічному просторі. У цьому контексті ключовими викликами та загрозами стали дезінформаційні кампанії, маніпуляції громадською думкою, пропаганда, зловживання медіа та спотворення історичних наративів.

Росія, використовуючи інструменти інформаційної війни, цілеспрямовано впливає на демократичні процеси в країнах ЄС, підриваючи довіру до урядів, послаблюючи єдність політичних рішень та маніпулюючи емоційним фоном у суспільстві. Особливу небезпеку становить використання цифрових платформ і соціальних мереж для масового розповсюдження фейкових наративів, які часто маскуються під достовірні джерела або поширюються через підставні акаунти, інфлюенсерів чи бот-мережі.

Найбільш поширеними є дезінформаційні кампанії та інформаційні операції для впливу на громадську думку в державах-членах ЄС. Одним із наймасштабніших прикладів є функціонування мережі вебпорталів під умовною назвою "Portal Kombat" — це інфраструктурно пов’язана система з щонайменше 193 сайтів, які з початку повномасштабної агресії проти України у 2022 році почали системно транслювати про-кремлівські наративи, дискредитацію України та критику західних демократій.

Ці сайти не створюють власного контенту, натомість масово ретранслюють публікації з акаунтів російських або проросійських акторів, державних агентств (наприклад, Інформаційне агентство Росії «ТАРС») або регіональних установ. Їх технічна структура уніфікована: однакова HTML-архітектура, графічне оформлення, хостинг у Росії (IP 178.21.15.85, AS49352), оптимізація під пошукові системи, використання однакових іконок, шаблонів та RSS-каналів.

Сайти pravda-fr[.]com (Франція), pravda-de[.]com (Німеччина), pravda-pl[.]com (Польща), pravda-en[.]com (Велика Британія та США), зареєстровані у червні 2023 року, систематично поширюють інформаційні матеріали, спрямовані на: делегітимацію української влади, створення хибного образу "спеціальної військової операції" як виправданої, розпалювання політичної поляризації в ЄС, зниження підтримки України серед громадян західних країн.

Особливо небезпечним є те, що ці кампанії орієнтовані не лише на широкі аудиторії, а й на локальні спільноти. Наприклад, в екосистемі "-news.ru" було створено десятки сайтів, які імітують новинні ресурси з українських міст — зокрема, Kherson-news[.]ru, Mariupol-news[.]ru, Tiraspol-news[.]ru, — та спрямовані на поширення проросійської пропаганди в окупованих або прикордонних зонах.

Використання штучного інтелекту, автоматизованих ботів і точково адаптованих наративів дозволяє цим платформам не лише поширювати фейки, але й імітувати інформаційну легітимність, створюючи хибне враження достовірного медіа-простору. Це — цілеспрямована стратегія когнітивного впливу, що руйнує здатність громадян критично сприймати інформацію, особливо в умовах інформаційного перевантаження[35].

---

[35] PORTAL KOMBAT. A structured and coordinated pro-Russian propaganda network. *VIGINUM*. 2024. URL: https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf (date of access: 09.04.2025).

Важливою загрозою для інформаційної безпеки Європейського Союзу стало перенесення кібер- та інформаційних атак на країни, які не є прямими учасниками конфлікту, але виступають із чіткою підтримкою України. Згідно з даними CyberPeace Institute, у 2022 році було зафіксовано 464 інциденти проти країн, які не беруть участі у бойових діях, з яких 239 — лише у IV кварталі, що становить зростання на 368,6% порівняно з попереднім періодом.

Найбільш постраждали Польща (70 атак), Латвія (32) та США (22). Основними цілями були державні установи, транспортний сектор, адміністративно-підтримувальні служби, що вказує на системне прагнення дестабілізувати державне управління, логістику та критичні сервіси у країнах-партнерах України. Зокрема, у Польщі було зафіксовано понад 40% атак на державні структури, причому майже половина інцидентів припала на перші два тижні листопада — період, коли спостерігалося загострення політичної риторики з боку РФ щодо Польщі.

Зростання активності хактивістських груп, таких як NoName057(16), KillNet та Anonymous Russia, демонструє переход від ізольованих кіберінцидентів до узгоджених інформаційно-психологічних операцій, часто з елементами фейкових повідомлень, дефейсингу урядових сайтів або паралельного запуску DDoS-атак. За IV квартал 2022 року діяльність Anonymous Russia зросла на 472,7%, а NoName057(16) відповідали за 46,6% атак серед усіх інцидентів поза зоною бойових дій.

Особливу загрозу становить те, що проросійські хактивісти все частіше об’єднуються в коаліції, створюючи централізовані канали координації в Telegram, обмінюючись ресурсами, бот-мережами та навіть пропонуючи "DDoS-as-a-service" для масового доступу до атакувальної інфраструктури[36].

---

[36]Cyber Dimensions of the Armed Conflict in Ukraine. *CyberPeace Institute.* 2022. URL: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf (date of access: 09.04.2025).

Російсько-українська війна істотно трансформувала ландшафт інформаційної безпеки Європейського Союзу, вивівши на передній план загрози, які не обмежуються лише технічними атаками на цифрову інфраструктуру. Найбільшою небезпекою стали скоординовані дезінформаційні кампанії, системне маніпулювання суспільною думкою та інституційна делегітимація через фейкові наративи й штучні платформи.

Ескалація діяльності проросійських акторів, таких як KillNet, NoName057(16) та Anonymous Russia, свідчить про перехід до більш складних і масованих інформаційно-психологічних операцій, спрямованих на послаблення єдності ЄС, розпалювання поляризації та зниження підтримки України. Особливо вразливими виявилися країни Центральної та Східної Європи, що активно підтримують Україну.

3.2. Забезпечення інформаційної безпеки ЄС

На фоні масованих дезінформаційних кампаній, атак на медіаінфраструктуру та організованих інформаційно-психологічних операцій, ЄС почав впроваджувати багаторівневі механізми — як на рівні окремих країн, так і в межах наднаціональної координації.

З початком повномасштабної війни в Україні заходи, раніше закладені в нормативно-стратегічних документах ЄС, пройшли перевірку в реальних кризових умовах. Цей підрозділ спрямований на аналіз конкретних інструментів, форматів взаємодії та прикладів реагування, які були застосовані з боку ЄС для протидії інформаційним загрозам російського походження.

Особливу увагу буде приділено механізмам оперативного реагування, інформаційній стійкості держав-членів, ролі медіа-платформ, а також участі громадянського суспільства та незалежних експертних спільнот у формуванні європейської інформаційної безпеки.

Одним із прикладів системної відповіді на нові виклики стало розширення повноважень та активізація діяльності EEAS, зокрема її підрозділу East StratCom Task Force. Саме ця структура адмініструє платформу EUvsDisinfo, яка з 2015 року фіксує та спростовує приклади проросійської дезінформації. З початку повномасштабної війни в Україні база даних платформи значно зросла: упродовж лише першого року конфлікту було задокументовано кілька тисяч випадків дезінформації, спрямованої на легітимізацію агресії, дискредитацію української влади та делегітимацію рішень ЄС, зокрема санкційної та оборонної політики[37].

Паралельно, на національному рівні окремі країни ЄС, зокрема Франція, створили спеціалізовані органи для виявлення і блокування ворожих інформаційних операцій. Так, у 2021 році при Секретаріаті національної оборони Франції було створено агентство Viginum, яке у 2023 році викрило функціонування координованої мережі фейкових вебсайтів під умовною назвою Portal Kombat, про яке вже згадувалося раніше. Агентство виявило єдину цифрову інфраструктуру та централізовану стратегію просування таких меседжів через пошукову оптимізацію та автоматизовану дистрибуцію[38].

Одним із ключових елементів сучасної політики ЄС у сфері інформаційної безпеки є регуляція діяльності цифрових платформ, які відіграють центральну роль у поширенні як достовірної, так і маніпулятивної інформації. У цьому контексті Європейська Комісія у 2022–2023 роках запровадила нові жорсткі правила в рамках Закону про цифрові послуги (Digital Services Act, DSA), який став чинним у серпні 2023 року для дуже великих онлайн-платформ (VLOP) і пошукових систем (VLOSE) з аудиторією понад 45 мільйонів користувачів у ЄС. Згідно з

---

[37] Ukraine. *EUvsDisinfo*. URL: https://euvsdisinfo.eu/ukraine/ (date of access: 10.04.2025).
[38] French agency uncovers pro-Russian propaganda network. *Euronews*. URL: https://www.euronews.com/next/2024/02/13/french-agency-uncovers-pro-russian-propaganda-network (date of access: 12.04.2025).

новими вимогами, компанії на кшталт Meta, Google, TikTok, X (колишній Twitter), Amazon і YouTube зобов'язані регулярно оцінювати й мінімізувати системні ризики, пов'язані з дезінформацією, політичною маніпуляцією, підривом виборчих процесів, а також — що особливо актуально в контексті війни — з розповсюдженням ворожих наративів, пов'язаних із війною Росії проти України.

Якщо платформи не виконують вимог, вони можуть бути оштрафовані на суму до 6% свого глобального річного обороту, що створює прецедентну систему відповідальності в цифровому середовищі. Крім того, Єврокомісія отримала повноваження проводити зовнішні аудити систем модерації контенту, алгоритмів та рекламних інструментів компаній, що дозволяє виявляти і санкціонувати ті механізми, які сприяють поширенню дезінформації або не забезпечують достатньої прозорості у її протидії[39].

Одним із перших тестів нових правил стала реакція на кризу дезінформації після початку повномасштабного вторгнення РФ в Україну. Комісар ЄС з питань внутрішнього ринку Тьєррі Бретон неодноразово публічно закликав компанії посилити боротьбу з фейковим контентом та вживати "ефективних, а не декларативних заходів" для захисту цифрової публічної сфери ЄС. Наприклад, у жовтні 2023 року Єврокомісія офіційно відкрила розслідування проти X (Twitter) за підозрою у поширенні проросійської пропаганди, фейкових фото і відео та відсутності швидкого реагування на дезінформаційні сплески під час війни в Ізраїлі, які були частково пов'язані з тим самим типом мереж, що діяли в контексті української війни[40].

---

[39] The EU's Digital Services Act. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (date of access: 15.04.2025).

[40] Europe battles 'avalanche of disinformation' from Russia / L. Abboud et al. *Financial Times*. URL: https://www.ft.com/content/2ffe8b64-f9bc-46d4-bf40-eefbbc6fac77 (date of access: 22.04.2025).

Таким чином, Європейський Союз демонструє перехід від м'якого саморегулювання до жорсткого, юридично зобов'язального режиму цифрової відповідальності, що може слугувати зразком для інших демократичних країн у боротьбі з ворожими інформаційними впливами.

В умовах повномасштабної війни Європейський Союз не лише зміцнює власну інформаційну безпеку, а й активно підтримує кіберстійкість України як держави-партнера. У цьому контексті співпраця між ЄС та українськими органами у сфері цифрової безпеки набуває стратегічного значення. У 2023 році Європейське агентство з кібербезпеки (ENISA) підписало меморандум про взаєморозуміння з Україною, який став основою для широкомасштабної співпраці. Йдеться не лише про обмін інформацією про загрози, а й про участь України в навчаннях ЄС з реагування на інциденти, а також про включення українських експертів у програму EU Cybersecurity Atlas — цифрову екосистему обміну досвідом між країнами-членами та партнерами. Така інтеграція має на меті побудову спільного інформаційного простору, що є вкрай важливо в умовах гібридної війни, яка не визнає географічних кордонів[41].

Практичне значення такої співпраці проявляється у кількох вимірах. По-перше, досвід України, яка стала об'єктом сотень масштабних кібератак з 2014 року, є унікальним джерелом навчання для країн-членів ЄС. Українські кейси з протидії фішинговим кампаніям, масовим DDoS-атакам, деструктивним програмам (як-от «NotPetya», «Prestige», «Azov») розглядаються в Європі як основа для моделювання потенційних сценаріїв на власній території. По-друге, в умовах постійних атак на критичну інфраструктуру — зокрема, енергетичні об'єкти, транспортні системи, банківські сервіси — ЄС отримує змогу адаптувати власні нормативно-технічні рішення до реалій масштабної гібридної агресії.

[41] Enhanced EU-Ukraine cooperation in Cybersecurity. *Home | ENISA*. URL: https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity (date of access: 16.04.2025).

Українські кейси розглядаються як "лабораторія стійкості", на основі якої формуються нові рекомендації ENISA, CERT-EU та інституцій цифрової дипломатії ЄС.

Паралельно із розширенням практичної взаємодії з Україною, Європейський Союз у жовтні 2024 року здійснив важливий політичний крок — вперше офіційно запровадив санкції проти фізичних осіб та організацій, причетних до кібератак, інформаційного саботажу та маніпулятивних впливів, які здійснюються в інтересах або за підтримки Росії. Нова правова рамка дозволяє застосовувати замороження активів, заборону на в'їзд до країн-членів ЄС, а також обмеження на фінансові та технологічні транзакції. До списків вже внесено кілька десятків осіб, серед яких — як представники спецслужб РФ, так і цивільні «активісти», які координували атаки на державні сайти Польщі, Латвії та Франції, а також адміністратори проросійських Telegram-каналів, що поширювали фейки про війну в Україні[42].

Ці санкції мають не лише каральний, а й превентивний характер: вони спрямовані на припинення безкарності інформаційних злочинів у цифровому просторі, які раніше залишалися поза межами юрисдикційних повноважень. Їхнє впровадження стало можливим завдяки зусиллям країн Балтії, Польщі та Франції, які активно просували ідею створення єдиної санкційної політики щодо інформаційних атак. Таким чином, Європейський Союз засвідчив готовність перейти від декларацій до дій, розширивши поняття безпеки до цифрового виміру. У комбінації з партнерством з Україною, такі заходи формують єдиний фронт оборони проти ворожих інформаційних операцій, що загрожують демократичному ладу та політичній стабільності на континенті.

---

[42] A new system will allow EU to sanction people waging sabotage on behalf of Russia. *AP News*. URL: https://apnews.com/article/eu-russia-ukraine-sanctions-69b106f14e30653a4a7b5fd15b11d251 (date of access: 15.04.2025).

У відповідь на безпрецедентні виклики, спричинені повномасштабною агресією Росії проти України, Європейський Союз продемонстрував рішучу й багатовимірну відповідь у сфері інформаційної безпеки. На зміну декларативним підходам прийшли практичні дії: регуляція цифрових платформ через Digital Services Act, оперативна протидія дезінформації з боку EEAS та національних структур, таких як французьке агентство Viginum, а також підтримка фактчекерських ініціатив і розвиток стратегічної комунікації. Усі ці заходи спрямовані на підвищення інформаційної стійкості як окремих держав-членів, так і Союзу загалом.

Не менш важливою складовою політики ЄС стало посилення міжнародної співпраці, зокрема з Україною. Участь українських фахівців у спільних кібернавчаннях, інтеграція в європейські програми обміну даними та використання українського досвіду як моделі для адаптації європейських стратегій кіберзахисту є важливими елементами нового безпекового підходу. Доповненням до цього стала санкційна політика ЄС, яка дозволяє притягати до відповідальності фізичних осіб та організації, причетні до інформаційного саботажу.

У сукупності ці кроки формують засади нової європейської парадигми інформаційної безпеки, що поєднує правовий захист, технологічну модернізацію та міжнародну солідарність.

3.3. Стратегічні перспективи забезпечення інформаційної безпеки ЄС

Зростаюча інтенсивність інформаційних загроз, пов’язаних з російсько-українською війною, продемонструвала, що Європейському Союзу необхідно не лише реагувати на інформаційні атаки, а й формувати довгострокову, стійку та адаптивну систему інформаційної безпеки, здатну ефективно функціонувати в умовах війни, криз та невизначеності. Інформаційна безпека вже не розглядається як технічне чи комунікаційне

питання — вона набуває стратегічного статусу поряд із оборонною, енергетичною та економічною безпекою. У цьому контексті перспективи ЄС у галузі інформаційної безпеки передбачають інтеграцію зусиль на рівні політик, технологій, освіти, інституцій та міжнародної співпраці.

Однією з ключових стратегічних ліній Європейського Союзу в контексті забезпечення інформаційної безпеки є посилення аналітичної та розвідувальної спроможності. Зокрема, йдеться про розвиток так званої Single Intelligence Analysis Capacity — структури, яка має стати основою для формування спільної стратегічної культури в галузі безпеки. У 2025 році передбачено проведення загальноєвропейського аналізу загроз, який стане базою для політичних рішень у сфері інформаційної безпеки. Важливість цього процесу підкріплюється інвестиціями в захищену інфраструктуру для аналітичної роботи, що дає змогу ЄС діяти автономно та проактивно в інформаційному середовищі.

Значну роль у цій архітектурі відіграє також EU Satellite Centre (EU SatCen), діяльність якого посилюється відповідно до нових безпекових викликів. Центр отримує розширений доступ до урядових супутникових даних, що дозволяє здійснювати оперативний моніторинг не лише геопросторових, але й інформаційних загроз. У 2023 році під час міністерського засідання Ради ЄС було погоджено створення урядової служби супутникового спостереження (EU Earth-Observation service), що дозволить зміцнити геоаналітичну незалежність Європейського Союзу. Це має вирішальне значення для виявлення дезінформаційних кампаній і гібридних впливів у прикордонних зонах або регіонах підвищеної турбулентності[43].

---

[43] ANNUAL PROGRESS REPORT on the Implementation of the Strategic Compass for Security and Defence. *EEAS.* URL: https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf (date of access: 15.04.2025).

Розвиток Single Intelligence Analysis Capacity також передбачає створення класифікованої платформи інформаційних технологій, яка уможливить обмін розвідданими між державами-членами ЄС у реальному часі. У результаті Європейський Союз планує перейти від фрагментарної оцінки загроз до інтегрованого, багатоступеневого аналізу інформаційної обстановки. Така аналітична основа стане критично важливою не лише для протидії поточним загрозам, а й для стратегічного планування у сфері інформаційної безпеки, особливо в умовах тривалих конфліктів і невизначеності[44].

Гібридні загрози, зокрема іноземні інформаційні маніпуляції та втручання, є одним із найбільш деструктивних інструментів, які використовуються проти Європейського Союзу. З огляду на зростання масштабів і складності таких впливів, ЄС розробив та активно впроваджує EU Hybrid Toolbox — інструментальну рамку для виявлення, аналізу та нейтралізації гібридних атак. Цей набір включає як технічні засоби виявлення, так і методології стратегічного реагування на рівні держав-членів. У 2023 році було оновлено Операційний протокол реагування на гібридні загрози, що дозволило підвищити узгодженість дій на випадок криз[45].

Додатково, у січні 2024 року було завершено оцінку прогалин у 18 критично важливих секторах, що дало змогу конкретизувати базові показники стійкості до гібридного впливу. На основі цього аналізу почалося формування EU Hybrid Rapid Response Teams — спеціалізованих груп швидкого реагування, здатних надавати цільову допомогу окремим

---

[44] Questions and answers: a background for the Strategic Compass. *EEAS*. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-background-strategic-compass-0_en (date of access: 17.04.2025).

[45] A new method to help policymakers defend democracy against hybrid threats. *The Joint Research Centre: EU Science Hub*. URL: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en (date of access: 16.04.2025).

державам-членам, місіям ЄС або партнерам (як у випадку з Молдовою). Їхнє завдання — швидке реагування на гібридні кампанії, включаючи поширення фейків, кібератаки, саботаж або психологічний тиск через медіа[46].

В умовах зростання загроз, пов'язаних із дезінформацією та зовнішнім втручанням у демократичні процеси, ЄС створив багатокомпонентний інструмент під назвою FIMI Toolbox (Foreign Information Manipulation and Interference Toolbox). Цей набір інструментів поєднує чотири ключові елементи: ситуаційну обізнаність, підвищення стійкості, заходи з дезактивації загроз та зовнішньополітичну відповідь. Інструментарій FIMI дозволяє координувати зусилля держав-членів, цифрових платформ, медіа та неурядових організацій у виявленні та нейтралізації інформаційних атак на ранніх етапах.

Центральне місце у FIMI Toolbox займає створений у 2023 році FIMI Information Sharing and Analysis Center — спеціалізована структура, яка забезпечує обмін даними про інформаційні маніпуляції між країнами ЄС, партнерами, експертними організаціями та громадським сектором. Центр пропонує єдину методологію аналізу, стандарти атрибуції загроз, а також рекомендації щодо запровадження обмежувальних заходів проти відповідальних акторів. Крім того, зібрана інформація інтегрується у спільну цифрову платформу — FIMI Data Space, яка дозволяє проводити порівняльний аналіз кампаній дезінформації у різних країнах та контекстах[47].

Інституціоналізація FIMI як окремого виміру безпеки засвідчує зростання ролі інформаційної гігієни в демократичному врядуванні. У

---

[46] Hybrid threats: Council paves the way for deploying Hybrid Rapid Response Teams. *Council of the EU*. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/ (date of access: 17.04.2025).

[47] FIMI-ISAC. *FIMI-ISAC*. URL: https://fimi-isac.org/index.html (date of access: 29.04.2025).

майбутньому цей підхід дозволить ЄС розширити власні можливості не лише щодо реагування, а й щодо стратегічного стримування зовнішніх інформаційних впливів — зокрема через систему санкцій, прозорі стандарти платформ та посилення політичної відповідальності цифрових посередників. Важливо, що ці інструменти функціонують у тісній співпраці з громадянським суспільством, що забезпечує довіру та підзвітність[48].

У відповідь на зростання геополітичної конкуренції у космічній сфері, ЄС у березні 2023 року вперше ухвалив EU Space Strategy for Security and Defence. Документ передбачає зміцнення супутникової інфраструктури ЄС, захист критичних космічних об'єктів та обмін даними з партнерами. Зокрема, у січні 2024 року було опубліковано перший закритий аналіз загроз у космосі, що базується на потужностях Single Intelligence Analysis Capacity. У стратегії підкреслюється важливість космосу як середовища для безпечного управління даними, зв’язку та навігації, а також як зони потенційного конфлікту[49].

У морському вимірі було оновлено Європейську стратегію морської безпеки (EU Maritime Security Strategy) у жовтні 2023 року. Документ передбачає активізацію військово-морської присутності в стратегічних регіонах, включно з Індо-Тихоокеанським простором, та організацію перших міжвідомчих навчань із морської безпеки у 2024 році. Значна увага приділяється співпраці з партнерами — зокрема, проведено спільні місії з Індією та Бразилією в межах програми CRIMARIO, а також підготовлено

---

[48] Strategic foresight. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/strategic-foresight_en (date of access: 30.04.2025).

[49] Defence Industry and Space. *European Commission.* URL: https://defence-industry-space.ec.europa.eu/eu-space-strategy-security-defence_en (date of access: 23.04.2025).

запуск Common Information Sharing Environment — платформи для обміну інформацією між морськими структурами країн ЄС[50].

Інформаційний суверенітет у цьому контексті розглядається як здатність ЄС захищати ключові канали зв'язку — зокрема, підводні кабелі, супутникові з’єднання та авіаційні маршрути. У 2023 році було проведено стратегічне обговорення про забезпечення безпечного доступу до повітряного простору, результатом чого має стати нова Європейська стратегія повітряної безпеки (EU Airspace Strategy for Security and Defence), запланована на 2025 рік. Такий комплексний підхід формує основу для інтегрованої моделі захисту інформаційного середовища як у фізичному, так і в цифровому вимірі[51].

Зростаюча інтенсивність гібридних загроз, пов’язаних з російсько-українською війною, продемонструвала, що Європейському Союзу необхідно не лише реагувати на інформаційні атаки, а й формувати довгострокову, стійку та адаптивну систему інформаційної безпеки, здатну ефективно функціонувати в умовах війни, криз та невизначеності. Інформаційна безпека більше не є лише питанням технологій або комунікацій — вона стала стратегічним компонентом загальноєвропейської безпеки, рівнозначним оборонній, енергетичній чи економічній стабільності.

У відповідь на ці виклики, ЄС вдався до системної модернізації своїх підходів: створено нові аналітичні центри, ініційовано програми стратегічного моніторингу, оновлено протоколи реагування на гібридні

---

[50] Maritime security strategy. *Oceans and fisheries*. URL: https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/maritime-security-strategy_en#:~:text=The%20revised%20strategy%20on%20maritime,the%20Council%20in%20October%202023 (date of access: 29.04.2025).

[51] EUROPEAN UNION SPACE STRATEGY FOR SECURITY AND DEFENCE. *European Union.* 2024. URL: https://defence-industry-space.ec.europa.eu/document/download/5e3dfcd1-2ff2-4fd1-85f7-74d0d9b62b3a_en?filename=Factsheet%20EU%20Space%20Strategy%20for%20Security%20and%20Defence.pdf (date of access: 29.04.2025).

загрози. Важливо, що ЄС не обмежується лише внутрішніми заходами — зростає співпраця з державами-партнерами, зокрема Україною, а також залучення громадянського суспільства до протидії дезінформації. Такий підхід формує багаторівневу екосистему інформаційної безпеки, здатну реагувати як на швидкоплинні виклики, так і на довгострокові стратегічні загрози.

Особливу увагу у стратегіях ЄС приділено не лише запобіганню атакам, а й підвищенню стійкості — як цифрових платформ, так і демократичних інституцій загалом. Впровадження законодавчих ініціатив на кшталт Digital Services Act або Cyber Solidarity Act забезпечує правову рамку для дій як приватного, так і державного секторів. Це свідчить про готовність ЄС перейти від принципу «реактивності» до режиму «проактивної безпеки», що дозволяє передбачати та запобігати інформаційним загрозам на ранніх етапах.

Таким чином, стратегічні перспективи забезпечення інформаційної безпеки ЄС полягають у комплексній інтеграції аналітичних, нормативних, технологічних та дипломатичних інструментів. У довгостроковій перспективі це дозволить Європейському Союзу не лише захищатися, але й бути глобальним актором у сфері цифрової безпеки, який задає стандарти відповідального інформаційного управління в умовах глобальної турбулентності.

ВИСНОВКИ

Дослідження інформаційної безпеки Європейського Союзу в умовах російсько-української війни дозволило всебічно проаналізувати існуючі механізми захисту інформаційного простору ЄС. В умовах агресії Росії проти України інформаційна безпека стала однією з ключових складових національної та міжнародної безпеки, і ЄС був змушений адаптуватися для ефективної протидії новим загрозам.

Огляд наукових досліджень та джерел підтверджує, що тема інформаційної безпеки Європейського Союзу в умовах російсько-української війни є надзвичайно актуальною та активно вивчається. Визначено, що основні роботи зосереджені на аналізі інформаційних і кіберзагроз, дезінформації та гібридних атаках, а також на вдосконаленні нормативно-правових механізмів ЄС для боротьби з інформаційними загрозами. Основними джерелами є наукові монографії, статті, офіційні документи ЄС та публікації міжнародних організацій. Важливою частиною джерельної бази є аналіз регулювання на рівні ЄС, зокрема нормативних актів. Проте, незважаючи на великі обсяги досліджень, залишається потреба в подальшому вдосконаленні стратегій ЄС у боротьбі з новими інформаційними викликами.

У роботі було чітко визначено основні поняття, що стосуються інформаційної безпеки, такі як кібербезпека, інформаційна війна та дезінформація, що дозволяє ефективно аналізувати ідентифіковані загрози. Для дослідження використовувалися різноманітні методи, зокрема такі як: спостереження, порівняння та аналіз, синтез, індукція та дедукція.

Аналіз політико-правових засад та інституційних механізмів інформаційної безпеки ЄС дозволив встановити, що Європейський Союз за останнє десятиліття розробив багаторівневу нормативно-правову систему, спрямовану на захист цифрового та інформаційного простору. Важливу роль у цьому процесі відіграють такі документи, як Директива

NIS та її оновлена версія NIS2, Директива CER, Загальний регламент захисту даних (GDPR), а також Акт про кібербезпеку. Ці нормативні акти закладають правову основу для захисту критичної інфраструктури, даних та цифрових сервісів. Інституційний рівень представлений такими ключовими органами, як Європейська служба зовнішніх справ, ENISA, Європейський центр боротьби з гібридними загрозами (Hybrid CoE), Система швидкого оповіщення (Rapid Alert System) та Європейський центр боротьби з кіберзлочинністю. Їхня взаємодія забезпечує скоординовану відповідь на загрози, що виникають у сфері інформаційної безпеки.

Охарактеризовано основні стратегії та інструменти, які ЄС застосовує для забезпечення інформаційної безпеки. Насамперед це стратегічні документи: «Стратегічний компас» (Strategic Compass), стратегія Digital Decade, ініціатива ProtectEU. У центрі цих документів — визнання інформаційної безпеки як структурної частини загальної безпекової архітектури ЄС. До інструментів забезпечення інформаційної безпеки належать механізми стратегічної комунікації (наприклад, діяльність East StratCom Task Force), розвиток цифрової грамотності населення, підтримка незалежних медіа, сертифікаційні ініціативи у сфері ІКТ, а також новітні регуляторні заходи (наприклад, Digital Services Act), які встановлюють зобов’язання для цифрових платформ у сфері боротьби з дезінформацією.

Визначено ключові виклики та загрози інформаційній безпеці ЄС, пов’язані з російсько-українською війною. З’ясовано, що головними загрозами є масові дезінформаційні кампанії, які мають чітко скоординований характер. Ці кампанії часто поєднують фейки, фішинг, використання штучного інтелекту та мереж ботів. Значною загрозою стали платформи, як-от Portal Kombat, що створюють ілюзію достовірного медіа-простору. Кібертаки на країни-партнери України (Польща, Латвія, Франція) демонструють прагнення до дестабілізації не лише України, а й ЄС загалом. Значна частина атак супроводжується діяльністю

хактивістських груп, таких як NoName057(16), Anonymous Russia, KillNet, які координуються через Telegram та інші платформи.

Проаналізовано реакцію ЄС на вищезгадані загрози**.** У відповідь на масштабні інформаційні атаки ЄС переходить від декларативних стратегій до практичних дій. Серед них — запровадження юридично обов'язкових норм для цифрових платформ (DSA), розширення повноважень EEAS, створення спеціалізованих агенцій (як Viginum у Франції), а також політичні санкції проти осіб, причетних до інформаційних атак. ЄС активно підтримує Україну у сфері цифрової безпеки через обмін досвідом, спільні навчання, залучення українських спеціалістів до європейських платформ.

Висвітлено стратегічні перспективи забезпечення інформаційної безпеки ЄС у тривалих кризових ситуаціях. ЄС посилює власну аналітичну спроможність через створення структури Single Intelligence Analysis Capacity, удосконалення супутникового моніторингу (EU SatCen) та формування груп швидкого реагування (EU Hybrid Rapid Response Teams). Особливу увагу приділено формуванню нормативної бази для FIMI Toolbox — інструменту протидії інформаційним маніпуляціям. У середньостроковій перспективі інформаційна безпека розглядається як один із головних векторів політики ЄС поряд з енергетичною, оборонною та економічною стабільністю. У довгостроковому вимірі ЄС прагне стати глобальним актором у сфері інформаційної безпеки.

Загалом, інформаційна безпека ЄС в умовах російсько-української війни вимагає комплексного підходу, що включає як правові, так і інституційні заходи для захисту інформаційного простору. Стратегії, спрямовані на боротьбу з дезінформацією, кіберзагрозами та іншими викликами, визначають основні напрямки в забезпеченні стабільності ЄС. Особлива увага приділяється розвиткові аналітичних можливостей, координації між державами-членами та вдосконаленню механізмів

оперативного реагування. У майбутньому Європейський Союз має посилювати роль інформаційної безпеки як одного з ключових компонентів загальної стратегії безпеки, орієнтуючись на технологічну незалежність, цифрову стійкість та прозорість інформаційних процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. А.О Місюра, В.О Паливода. Концептуальні підходи НАТО та ЄС до забезпечення стійкості держави і суспільства у сфері національної безпеки. *Національний інститут стратегічних досліджень*. URL: https://niss.gov.ua/sites/default/files/2018-04/NATO-ES-stiykist-59383.pdf (date of access: 02.02.2025).
2. Троян С. Інформаційно-безпекова політика Європейського Союзу. *erNAU - Electronic Institutional Repository of the National Aviation University of Ukraine.* URL: https://er.nau.edu.ua/items/a0ff4b35-e55a-421a-8771-dad5dd77f1b9 (дата звернення: 11.02.2025).
3. Фурсай, О. (2023). ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ. *Літопис Волині,* (29), 165-170. https://doi.org/10.32782/2305-9389/2023.29.27
4. 2023 CONSOLIDATED ANNUAL ACTIVITY REPORT. 2024. 178 p. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/2023%20Consolidated%20Annual%20Activity%20Report_1.pdf (date of access: 19.03.2025).
5. 2024 Progress Report on the Implementation of the Strategic Compass for Security and Defence. EEAS. URL: https://www.eeas.europa.eu/eeas/2024-progress-report-implementation-strategic-compass-security-and-defence-0_en (date of access: 14.03.2025).
6. About. *EUvsDisinfo*. URL: https://euvsdisinfo.eu/about/ (date of access: 20.02.2025).
7. About us - Hybrid CoE. *The European Centre of Excellence for Countering Hybrid Threats.* URL: https://www.hybridcoe.fi/about-us/ (date of access: 20.03.2025).

8. Action Plan against Disinformation. *EUR-Lex*. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0036 (date of access: 02.04.2025).
9. A Europe that protects: good progress on tackling hybrid threats. *European Commission*. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2788 (date of access: 13.03.2025).
10. A new method to help policymakers defend democracy against hybrid threats. *The Joint Research Centre: EU Science Hub*. URL: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en (date of access: 16.04.2025).
11. A new system will allow EU to sanction people waging sabotage on behalf of Russia. *AP News*. URL: https://apnews.com/article/eu-russia-ukraine-sanctions-69b106f14e30653a4a7b5fd15b11d251 (date of access: 15.04.2025).
12. ANNUAL PROGRESS REPORT on the Implementation of the Strategic Compass for Security and Defence. *EEAS*. URL: https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf (date of access: 15.04.2025).
13. CISA says Killnet DDoS attacks on U.S. hospitals had little effect. *Cyber Security News | The Record from Recorded Future News*. URL: https://therecord.media/ddos-hospitals-cisa-killnet-limited-effects (date of access: 22.04.2025).
14. Commission unveils ProtectEU – a new European Internal Security Strategy. *European Commission*. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920 (date of access: 08.04.2025).

15. Cyber Dimensions of the Armed Conflict in Ukraine. *CyberPeace Institute.* 2022. URL: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf (date of access: 09.04.2025).
16. Daniel Fiott, Roderick Parkes. PROTECTING EUROPE: The EU's response to hybrid threats. *European Union Institute for Security Studies (EUISS)*. URL: https://www.jstor.org/stable/resrep21143.4 (date of access: 03.02.2025).
17. Defence Industry and Space. *European Commission.* URL: https://defence-industry-space.ec.europa.eu/eu-space-strategy-security-defence_en (date of access: 23.04.2025).
18. Digital Decade. *Digital Skills and Jobs Platform.* URL: https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/digital-decade (date of access: 03.04.2025).
19. Directive (EU) 2016/1148 of Cybersecurity of network and information systems *EUR-Lex.* URL: https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX:32016L1148#:~:text=KEY%20TERMS%20*%20Cybersecurity:%20the%20ability%20of,for%20example%20water%20supply,%20electricity%20services,%20etc. (date of access: 05.02.2025).
20. Dr Gerald L. Kovacich Dr Andy Jones. 2 - High-Technology Crime Miscreants: Profiles, Motives, and Philosophies. *High-Technology Crime Investigator's Handbook (Second Edition) Establishing and Managing a High-Technology Crime Prevention Program*. 2006. No. 2. P. 23–48.
21. Eastern Partnership. *EEAS.* URL: https://www.eeas.europa.eu/eeas/eastern-partnership_en (date of access: 18.03.2025).
22. Enhanced EU-Ukraine cooperation in Cybersecurity. *Home | ENISA*. URL:

https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity (date of access: 16.04.2025).

23. European Cybercrime Centre - EC3 | Europol. *Europol*. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (date of access: 29.03.2025).
24. EUROPEAN UNION SPACE STRATEGY FOR SECURITY AND DEFENCE. *European Union*. 2024. URL: https://defence-industry-space.ec.europa.eu/document/download/5e3dfcd1-2ff2-4fd1-85f7-74d0d9b62b3a_en?filename=Factsheet%20EU%20Space%20Strategy%20for%20Security%20and%20Defence.pdf (date of access: 29.04.2025).
25. Europe battles ‘avalanche of disinformation’ from Russia / L. Abboud et al. *Financial Times*. URL: https://www.ft.com/content/2ffe8b64-f9bc-46d4-bf40-eefbbc6fac77 (date of access: 22.04.2025).
26. Factsheet: Rapid Alert System. EEAS. URL: https://www.eeas.europa.eu/node/59644_en (date of access: 02.04.2025).
27. FIMI-ISAC. *FIMI-ISAC*. URL: https://fimi-isac.org/index.html (date of access: 29.04.2025).
28. French agency uncovers pro-Russian propaganda network. *Euronews*. URL: https://www.euronews.com/next/2024/02/13/french-agency-uncovers-pro-russian-propaganda-network (date of access: 12.04.2025).
29. Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175.
30. Hoffman, Frank, "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict" (2009). *Strategic Forums*. URL:

https://digitalcommons.ndu.edu/strategic-forums/40 (date of access: 02.02.2025).

31. Hybrid CoE continues to work to support European security and Ukraine. *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats*. URL: https://www.hybridcoe.fi/news/hybrid-coe-continues-to-work-to-support-european-security-and-ukraine/ (date of access: 30.03.2025).
32. Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage - *The European Centre of Excellence for Countering Hybrid Threats*. URL: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/ (date of access: 14.03.2025).
33. Hybrid threats: Council paves the way for deploying Hybrid Rapid Response Teams. *Council of the EU*. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/ (date of access: 17.04.2025).
34. Information security. *European Data Protection Supervisor*. URL: https://www.edps.europa.eu/data-protection/data-protection/reference-library/information-security_en (date of access: 05.02.2025).
35. Joint Framework on countering hybrid threats a European Union response. *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018 (date of access: 05.02.2025).
36. Maritime security strategy. *Oceans and fisheries*. URL: https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/maritime-security-strategy_en#:~:text=The%20revised%20strategy%2

0on%20maritime,the%20Council%20in%20October%202023 (date of access: 29.04.2025).

37. NIS2 Directive: new rules on cybersecurity of network and information systems. *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (date of access: 05.02.2025).
38. PORTAL KOMBAT. A structured and coordinated pro-Russian propaganda network. *VIGINUM*. 2024. URL: https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf (date of access: 09.04.2025).
39. Questions and answers: a background for the Strategic Compass. *EEAS*. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-background-strategic-compass-0_en (date of access: 17.04.2025).
40. Questions and Answers about the East StratCom Task Force. EEAS. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11234 (date of access: 24.02.2025).
41. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). *EUR-Lex*. (date of access: 16.03.2025).
42. REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *EUR-Lex*. 2019.

URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng (date of access: 15.03.2025).

43. Strategic Compass - A Strategic Compass for Security and Defence. *EEAS,* 2022. URL: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf, P. 17–21. (date of access: 01.04.2025).
44. Strategic foresight. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/strategic-foresight_en (date of access: 30.04.2025).
45. Tackling online disinformation. *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation (date of access: 04.02.2025).
46. The Cybersecurity Strategy. *Shaping Europe's digital future.* URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (date of access: 03.03.2025).
47. The EU Cybersecurity Act. *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (date of access: 08.02.2025).
48. The EU's Cybersecurity Strategy for the Digital Decade. *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (date of access: 06.02.2025).
49. The EU's Digital Services Act. *European Commission.* URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (date of access: 15.04.2025).
50. Thomas Rid. Active Measures: The Secret History of Disinformation and Political Warfare. 2020. Volume 64, No. 1. P. 1–2.
51. Ukraine. *EUvsDisinfo.* URL: https://euvsdisinfo.eu/ukraine/ (date of access: 10.04.2025).

52. What is cybersecurity?. *Cisco*. URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html (date of access: 05.02.2025).
53. What is GDPR, the EU's new data protection law? - *GDPR.eu*. URL: https://gdpr.eu/what-is-gdpr/ (date of access: 14.02.2025).
54. What we do | *ENISA*. *Home* URL: https://www.enisa.europa.eu/about-enisa/what-we-do (date of access: 19.03.2025).