РОЗДІЛ ІІІ. РЕГІОНАЛЬНІ СТУДІЇ

УДК 351.862.4:004.9.056(4-6ЄС)

Євгенія Вознюк,
кандидат політичних наук, доцент, доцент кафедри міжнародних комунікацій та політичного налізу,
Волинський національний університет імені Лесі Українки,
Voznyuk.Yevhenija@vnu.edu.ua
ORCID ID: 0000-0002-7828-7430;

Вікторія Андрюхіна,
здобувачка третього (освітньо-наукового) рівня освіти,
ОНП Міжнародні відносини і стратегічні комунікації України та ЄС
спеціальності 292 Міжнародні відносини, суспільні комунікації
та регіональні студії,
Волинський національний університет імені Лесі Українки,
Andriukhina.viktoriia@vnu.edu.ua
ORCID ID: 0000-0002-7332-4765
DOI 10.29038/2524-2679-2025-02-136-154

ПОРІВНЯЛЬНИЙ АНАЛІЗ КІБЕРБЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Кібербезпека набула стратегічного значення як ключовий елемент національної та наднаціональної безпеки. Європейський Союз, об'єднуючи понад два десятки країн із різним рівнем цифрової зрілості, постає перед необхідністю уніфікації підходів до кіберзахисту. У статті здійснено комплексний аналіз кібербезпекової політики ЄС в умовах загострення глобальних гібридних загроз, її інституційної архітектури, правового забезпечення, механізмів реагування на сучасні загрози. Проаналізовано функціонування ключових структур – ENISA, CERT-EU, CSIRT Network, Європейської комісії, EEAS та East StratCom – і їх взаємодію в межах загальноєвропейського підходу до кіберстійкості. Розглянуто еволюцію нормативно-правової бази – від першої Директиви NIS до її оновлення у вигляді NIS2, – а також Закон про цифрові послуги (DSA) і нові ініціативи, як-от Європейський щит кібербезпеки та Cyber Solidarity Act. Особливу увагу приділено ролі публічної дипломатії Союзу, гібридним загрозам,

дезінформаційним кампаніям, утручанню в демократичні процеси, зокрема в контексті російсько-української війни, і цифровому суверенітету як стратегічному пріоритету. Доведено, що інституційна архітектура кібербезпеки об'єднання поєднує нормативні, оперативні, комунікаційні та стратегічні елементи, що дає змогу забезпечувати стійкість цифрового середовища в умовах нових загроз. У статті використано історичний, порівняльний, системний підходи, контент-аналіз і SWOT-аналіз для виявлення сильних та слабких сторін кіберполітики ЄС, а також визначення її можливостей і загроз. Проведено порівняльний аналіз політик США, Китаю, НАТО та України, що дає змогу оцінити унікальність підходу Європейського Союзу до цифрової безпеки, заснованого на захисті прав людини, багаторівневому управлінні й міжнародній кооперації. Підкреслено роль України як важливого партнера в забезпеченні спільної кіберстійкості на східному фланзі Європи.

Ключові слова: кібербезпека, Європейський Союз, NIS2, ENISA, дезінформація, гібридні загрози, цифрова дипломатія.

Yevheniia Vozniuk,
Lesya Ukrainka Volyn National University,
ORCID ID: 0000-0002-7828-7430;

Viktoriia Andriukhina,
Lesya Ukrainka Volyn National University,
ORCID ID: 0000-0002-7332-4765

COMPARATIVE ANALYSIS OF CYBERSECURITY IN THE EUROPEAN UNION

Cybersecurity has acquired strategic importance as a key element of national and supranational security. The European Union, comprising more than two dozen countries with varying levels of digital maturity, faces the need to unify its approaches to cyber defence. The article offers a comprehensive analysis of the EU's cybersecurity policy in the context of the intensification of global hybrid threats, its institutional framework, legal foundations, and mechanisms for addressing contemporary threats. The functioning of key structures – ENISA, CERT-EU, CSIRT Network, the European Commission, EEAS, and East StratCom – and their interaction within the framework of a pan-European approach to cyber resilience are analysed. The evolution of the regulatory framework is considered: from the first NIS Directive to its update in the form of NIS2, as well as the Digital Services Act (DSA) and new initiatives, such as the European Cy-

bersecurity Shield and the Cyber Solidarity Act. Particular attention is paid to the role of the Union's public diplomacy, hybrid threats, disinformation campaigns, interference in democratic processes, in particular in the context of the Russian-Ukrainian war, and digital sovereignty as a strategic priority. It is proven that the institutional architecture of the Union's cybersecurity combines regulatory, operational, communication and strategic elements, which allows ensuring the resilience of the digital environment in the face of new threats. The article uses historical, comparative, systemic approaches, content analysis and SWOT analysis to identify the strengths and weaknesses of the EU's cyber policy, as well as to determine its opportunities and threats. A comparative analysis of the policies of the United States, China, NATO and Ukraine is also conducted, which allows assessing the uniqueness of the European Union's approach to digital security, based on the protection of human rights, multi-level governance and international cooperation. The role of Ukraine as an important partner in ensuring common cyber resilience on the eastern flank of Europe is emphasized.
Key words: cybersecurity, European Union, NIS2, ENISA, disinformation, hybrid threats, digital diplomacy.

1. ВСТУП

Постановка проблеми. У XXI ст. інформаційні технології стали фундаментом соціального, політичного та економічного життя. Водночас зросла й залежність держав від стабільного функціонування кіберпростору, що, своєю чергою, актуалізувало проблему кібербезпеки як стратегічного пріоритету. Особливого значення це питання набуває для Європейського Союзу, який об'єднує понад два десятки країн із власними інформаційними системами, інфраструктурою та рівнем цифрової зрілості. У зв'язку з цим формування ефективної політики кіберзахисту, яка б забезпечувала стійкість цифрової Європи, є необхідною умовою її безпеки, добробуту й глобальної конкурентоспроможності.

Сучасні виклики, пов'язані з гібридними загрозами, кібератаками на критичну інфраструктуру, утручанням у виборчі процеси, дезінформаційними кампаніями, здійсненими третіми державами, потребують системної та уніфікованої відповіді від інституцій ЄС. Кібератака на уряд Естонії (2007 р.), вірус WannaCry (2017 р.), масштабні втручання в медіапростір під час пандемії COVID-19, кампанії дезінформації в контексті російсько-української війни (із 2014 р.) – усе це доводить, що без надійного нормативного й інституційного каркасу забезпечення кібербезпеки жоден політичний або економічний проєкт не може бути сталим.

Аналіз останніх досліджень і публікацій. Досліджуючи питання кібербезпеки Європейського Союзу, звертаємо увагу на систематичний огляд NIS2 від Jukka Ruohonen (2024), який представив «A Systematic Literature Review on the NIS2 Directive», де розглянуто понад 50 академічних джерел, сфокусованих на новій Директиві, що включає збільшення охоплення критичної інфраструктури; виклики взаємодії між CSIRT і приватним сектором; потребу в загальноєвропейських стандартах risk management [1]. В іншій статті «The Incoherency Risk» (2024) J. Ruohonen підкреслює, що швидке багатошарове регулювання (NIS2, DORA, DSA) породжує ризик «дискоординованості» між законами, індустріями й країнами [2]. Аналітика ABB «NIS2 Country Implementation Study» (2024) порівнює імплементацію NIS2 у всіх державах-членах – відзначено різні підходи: централізована (Франція), децентралізована (Німеччина), проблеми з правозастосуванням (Польща) [3].

Аналізуючи формальне оцінювання стану кібербезпеки в ЄС, ENISA в «Report on the State of Cybersecurity in the Union» відзначило нерівномірність реалізації NIS2 серед держав-членів і різний рівень готовності критичних секторів [4].

Kaspar Rosager Ludvigsen (2025) у статті «Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law» виявляє п’ять ключових принципів регулювання кібербезпеки: добровільне співробітництво, адаптивні визначення, державне підсилення, обов’язкові CERT і санкції. Порівняльно аналізує регулятивні механізми ЄС та США [5].

Cîrnu, Răduna, Vasiloiu й ін. (2023) у «Comparative Analysis on Cyber Diplomacy in EU and US» порівнюють інструменти кібердипломатії США та ЄС. Увагу зосереджено на EU Toolbox vs US Cyber Diplomacy Act, підкреслено роль ЄС у формуванні норм міжнародної кібеповедінки [6].

Мета дослідження – комплексний порівняльний аналіз політики Європейського Союзу у сфері кібербезпеки: її становлення, інституційної архітектури, законодавчого забезпечення, практики реагування й перспектив розвитку в умовах сучасних загроз.

Методика дослідження. Для досягнення поставленої мети використано комплекс загальнонаукових і спеціальних методів: історичний метод – для реконструкції етапів розвитку політики кібербезпеки ЄС; порівняльний метод – для аналізу законодавства країн ЄС та інших міжнародних акторів; системний підхід – для виявлення взаємозв’язків між інституціями й механізмами реагування; контент-аналіз – для вивчення публічних заяв, стратегій, звітів і законодавства; SWOT-аналіз – для оцінки сильних та слабких сторін поточної політики.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Питання кібербезпеки почало набирати вагомості в політичному порядку денному Європейського Союзу з початку 2000-х років, однак концептуальні підходи до цієї теми розвивалися ще раніше – у контексті цифрової модернізації та інформаційного суспільства. Перші політичні документи на рівні ЄС у сфері цифрової безпеки з'явилися на тлі розбудови електронного урядування, електронних сервісів, зростання онлайн-комерції та зростаючої ролі даних як стратегічного ресурсу.

Теоретичне осмислення кібербезпеки розвивалося в межах ширших концепцій інформаційної безпеки, цифрового суверенітету, мережевої держави (network state) і безпеки як соціального конструкту. Західна наукова традиція значну увагу приділяє поняттю resilience – стійкості систем до кіберзагроз [2]. Під впливом цього підходу в Союзі стала домінувати не лише ідея оборони, а й адаптації, відновлення та стратегічної комунікації.

Паралельно формувався дискурс цифрового суверенітету, згідно з яким держава або наддержавне утворення (таке як Європейський Союз) повинні мати контроль над своїми цифровими ресурсами, даними й платформами. Це стало особливо актуальним після розкриттів Едварда Сноудена (2013), що продемонстрували глобальну вразливість навіть союзників США перед засобами кібернагляду.

Історично першим значущим кроком до формування політики кібербезпеки в ЄС стало створення у 2004 р. Європейського агентства з мережевої й інформаційної безпеки (ENISA). Після цього відбулися хвилі стратегічних і нормативних ініціатив: перша Стратегія кібербезпеки ЄС (2013 р.), Директива NIS (2016 р.), її оновлення у вигляді NIS2 (2022 р.), запуск проєкту «EU Cyber Shield» (2023 р.).

Отже, історико-теоретичні основи політики кібербезпеки в ЄС формувалися під впливом як практичних викликів (атаки, витоки даних, утручання у вибори), так і еволюції глобальної думки щодо природи загроз, ролі держави в кіберпросторі та необхідності багаторівневої цифрової безпеки.

Кібербезпека в Європейському Союзі забезпечується завдяки взаємодії багатьох інституцій, кожна з яких виконує окремі функції у сфері запобігання, реагування, стратегічного планування й інформаційного обміну. Ця архітектура поступово еволюціонувала під впливом загроз, досвіду попередніх інцидентів та потреби узгодження політик між державами-членами.

Отже, роль інституцій в архітектурі кібербезпеки ЄС не є ізольованою – між ними налагоджено механізми співпраці (табл. 1). Так, ENISA

Таблиця 1

Основні інституції ЄС та їх функції*

Інституція	Функції
ENISA (European Union Agency for Cybersecurity)	Підтримка держав-членів у розробці національних стратегій, аудит кіберготовності, координація CSIRT, участь у навчаннях (Cyber Europe)
CERT-EU (Computer Emergency Response Team for the EU)	Захист IT-систем установ ЄС, реагування на кіберінциденти, обмін інформацією з національними центрами реагування
CSIRT Network	Мережа груп реагування держав-членів, координація між ними через ENISA, технічний обмін інформацією
Європейська Комісія (DG CONNECT, DG HOME)	Розробка та впровадження законодавчих ініціатив, фінансування кіберпроєктів, моніторинг імплементації директив
Європейська служба зовнішньої дії (EEAS)	Реалізація зовнішньої кібердипломатії, протидія дезінформації (East StratCom Task Force)
EUROPOL/EC3	Розслідування кіберзлочинів, обмін інформацією про кіберзагрози, співпраця з INTERPOL
Європейська рада	Координація політики безпеки на стратегічному рівні, затвердження загальних рамок реагування на загрози

**Складено автором.*

підтримує технічну взаємодію між CSIRT, у той час як CERT-EU має тісний зв'язок з інституціями ЄС та повідомляє про загрози. DG CONNECT бере участь у формуванні політики, а EEAS – у зовнішній дипломатичній комунікації на теми дезінформації й кіберзагроз. Усі структури узгоджують свою діяльність із європейськими стратегіями, такими як EU Cybersecurity Strategy (2020 р.) та NIS2 (2022 р.).

Діяльність цих інституцій підтримується через спеціальні платформи, наприклад MeliCERTes (інструмент обміну інформацією між CSIRT), Rapid Alert System для моніторингу виборів, EUCS (сертифікаційна рамка безпеки) [3; 7].

Отже, інституційна архітектура кібербезпеки ЄС поєднує нормативні, оперативні, комунікаційні та стратегічні елементи, що дає змогу забезпечувати стійкість цифрового середовища в умовах нових загроз.

Рис. 1. *Еволюція ключових правових актів ЄС**

**Складено автором.*

Розбудова правових механізмів кіберзахисту в Європейському Союзі відбувається на основі директив, стратегічних документів і регламентів, що визначають обов'язки держав-членів, бізнесу та інституцій ЄС. Основним правовим інструментом стала Директива NIS (2016 р.), яка зобов'язала держави створити національні органи кібербезпеки, мережі CSIRT й узгодити базові вимоги до кіберзахисту критичної інфраструктури.

У 2022 р. ЄС ухвалив оновлену версію – Директиву NIS2, яка значно розширила перелік суб'єктів регулювання, запровадила вимоги до управління ризиками, звітності про інциденти та накладення штрафів. Поряд із цим у 2022 р. набув чинності Digital Services Act (DSA), який регулює прозорість алгоритмів, обмеження шкідливого контенту, реклами та захист персональних даних користувачів [3].

У відповідь на зростання масштабів атак у 2023 р. презентовано ініціативу «Європейський щит кібербезпеки», що передбачає створення

мережі оперативних центрів безпеки (SOC), котрі працюватимуть у режимі реального часу на рівні ЄС. Також запроваджено акт про кіберсолідарність (Cyber Solidarity Act), що передбачає спільні бюджети на стримування кіберзагроз та фінансування інноваційних кіберрішень [8].

На рис. 1 еволюції актів ілюструється поступовий перехід від добровільних механізмів до обов'язкових із фінансовими санкціями й підвищенням рівня відповідальності платформ і держав-членів за інформаційну безпеку. Ці зміни відображають зростання значущості кіберзагроз у системі безпеки ЄС та наближення до моделі цифрового суверенітету, де Союз самостійно регулює правила функціонування кіберпростору.

Політика кібербезпеки Європейського Союзу вирізняється багаторівневою структурованістю, поєднанням нормативного врегулювання, міждержавної координації та зовнішньої дипломатичної активності. SWOT-аналіз (табл. 2) дає змогу комплексно оцінити ключові аспекти цієї політики з урахуванням внутрішніх і зовнішніх факторів впливу.

Отже, сильні сторони кіберполітики ЄС полягають насамперед у наявності уніфікованої нормативно-правової бази, зокрема Директиви NIS2 і Закону про цифрові послуги, які встановлюють загальноєвропейські стандарти для цифрових операторів та критичної інфраструктури [9; 10]. Важливою перевагою є функціонування таких інституцій, як ENISA, мережа CSIRT і CERT-EU, що забезпечують координацію, сертифікацію та реагування на кіберінциденти [11]. Додатково активна публічна дипломатія ЄС, зокрема ініціативи на кшталт East StratCom Task Force і платформи EUvsDisinfo, формує нову якість комунікації з громадянами та захисту від когнітивних загроз [12; 13]. Важливою рисою є акцент на дотриманні прав людини в цифровому середовищі, що вирізняє ЄС серед інших глобальних акторів [7].

Однак слабкі сторони свідчать про наявність дисбалансів між державами-членами: рівень кіберготовності, фінансування та людський капітал суттєво відрізняються, що ускладнює ефективну реалізацію політики на загальноєвропейському рівні [14]. Окремою проблемою є низька цифрова грамотність частини населення, а також громіздкість бюрократичних процедур, що вповільнюють ухвалення рішень і впровадження інновацій.

Серед можливостей виокремимо розширення партнерства з ключовими стратегічними союзниками – НАТО, Україною [15; 16]. Таке співробітництво сприяє обміну досвідом, координації протидії кіберзагрозам та зміцненню кіберстійкості в ширшому геополітичному вимірі. Значним ресур-

Таблиця 2

SWOT-аналіз кіберполітики ЄС*

Компонент	Характеристика
Сильні сторони (Strengths)	Уніфіковане законодавство (NIS2, DSA); наявність спеціалізованих інституцій (ENISA, CSIRT); активна публічна дипломатія (East StratCom); міждержавна координація; підтримка прав людини в цифровому просторі.
Слабкі сторони (Weaknesses)	Різний рівень кіберготовності серед держав-членів; недостатнє фінансування інновацій; бюрократичність у прийнятті рішень; низька цифрова грамотність у частини населення.
Можливості (Opportunities)	Посилення партнерства з НАТО, Україною; розвиток власного технологічного сектору; упровадження єдиного ринку кібербезпеки; поширення стандартів ЄС за межами Союзу (soft power).
Загрози (Threats)	Гібридна агресія третіх країн (рф, КНР); залежність від іноземних ІТ-компаній; кібератаки на критичну інфраструктуру; поширення дезінформації та недовіри до інституцій.

**Складено автором.*

сом розвитку також є внутрішній технологічний сектор ЄС, можливість упровадження єдиного ринку кібербезпеки (Cybersecurity Single Market), що дасть змогу активізувати інновації, стартапи та захист інфраструктури на уніфікованій базі. М'яка сила Європейського Союзу проявляється в поширенні своїх стандартів і моделей кібербезпеки за межами Союзу [7].

Водночас загрози залишаються серйозними та зростаючими. Ідеться насамперед про гібридну агресію з боку недружніх держав, насамперед росії й Китаю, які використовують кібератаки, дезінформацію та когнітивні операції як елементи стратегічного впливу [17]. Вразливість ЄС посилюється через залежність від іноземних ІТ-компаній у сферах хмарних технологій, обчислювальних потужностей і мікроелектроніки.

Кібератаки на критичну інфраструктуру, зокрема енергетичну, транспортну та медичну, демонструють зростаючу складність і потенційну шкоду [15]. Крім того, масштабне поширення дезінформації та зниження довіри до інституцій ускладнюють реалізацію політик цифрової безпеки.

Політика кібербезпеки ЄС має вагомий системний потенціал, однак її успішність значною мірою залежить від подолання внутрішніх дисбалансів й адаптації до мінливих зовнішніх загроз. Поглиблення інтеграції з країнами-партнерами, особливо з Україною, відкриває нові горизонти для посилення загальноєвропейської кіберстійкості.

Кібербезпека Європейського Союзу розвивалася доволі активно під постійним впливом гучних кіберінцидентів, які загрожували як державним системам, так і громадянам. Аналіз кейсів дає змогу виявити типові загрози, слабкі місця в системі реагування, а також механізми, що виявилися ефективними.

За останні п'ять років Європейський Союз постійно стикається з різко зростаючим рівнем практичних кіберзагроз, що стали наслідком активізації інформаційного тероризму державами-агресорами. Так, згідно з ENISA Threat Landscape Report (2023 р.), основними загрозами були (табл. 3, рис. 2) [18].

Спершу WannaCry (2017 р.), який став прикладом глобальної атаки, що охопила понад 150 країн, уключаючи кілька держав-членів ЄС (Іспанію, Францію, Великобританію). Вірус-шантажист заблокував тисячі комп'ютерів через розповсюдження шкідливого ПЗ, що зашифровувало файли користувачів, зокрема в лікарнях, транспортних системах, банках. Він продемонстрував низький рівень готовності до атаки, особливо в державному секторі. Реакція Європейського Союзу полягала в закликах до оновлення систем безпеки, а також посиленні функцій ENISA.

Наступним розглянемо SolarWinds (2020 р.), хоча основним об'єктом атаки була інфраструктура США, ланцюговий вплив на Європу став очевидним – кіберзловмисники отримали доступ до IT-систем органів влади в декількох країнах ЄС. На сьогодні його пов'язують із російською хакерською групою APT29. Цей інцидент актуалізував дискусію про ланцюгові ризики постачання (supply chain cybersecurity) і посилив тиск на прийняття NIS2, а також висвітлив серйозні прогалини у виявленні вторгнень та довірі до оновлень ПЗ.

Ще одним яскравим прикладом є дезінформація під час виборів (2019 р., 2022 р.). Європейський Союз фіксував кампанії дезінформації, зокрема, щодо вакцинації, виборчих процесів у Франції, Німеччині, Італії. У 2022 р. виявлено масштабні наративи, що дискредитують підтримку України.

Таблиця 3

Основні типи кіберзагроз*

Тип загроз	Джерело	Ціль	Приклад
Ransomware	Кіберзлочинці	Бізнес, держустанови	WannaCry, Ryuk
APT (Advanced Persistent)	Спонсоровані держави	Інфраструктура, оборона	APT28, APT29
Supply Chain	Компрометація ПЗ	Критичні оновлення	SolarWinds
Дезінформація	Іноземні структури	Населення, імідж інституцій	COVID-фейки, антиукраїнські меседжі
DDoS-атаки	Активісти, держави	Банки, новинні портали	Killnet атаки 2022–2023

**Складено автором.*

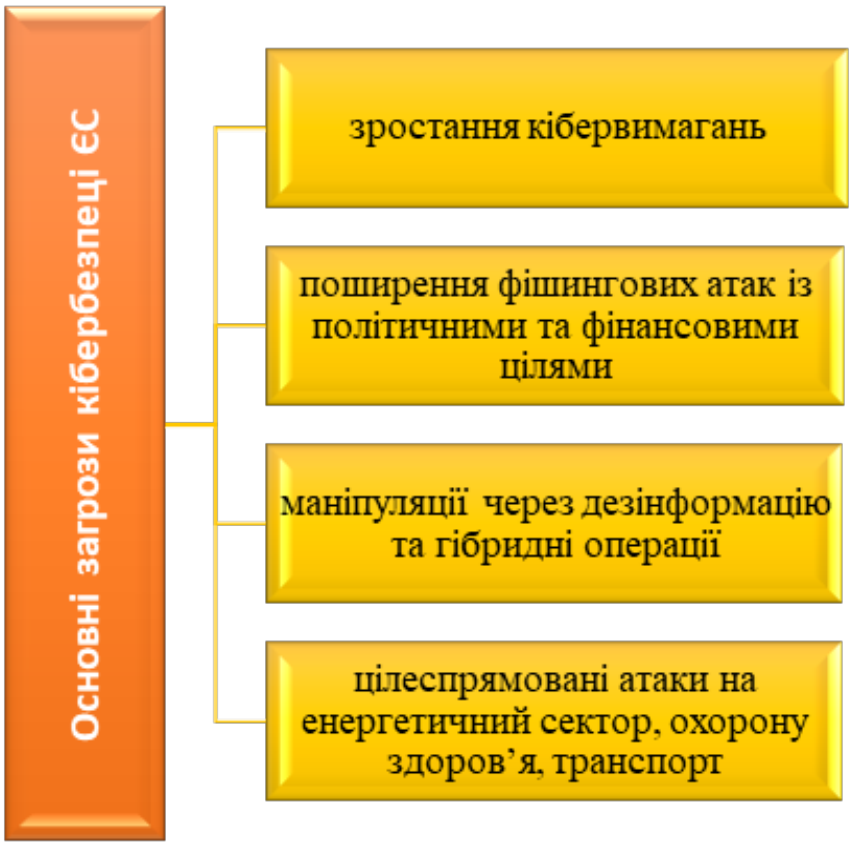

Рис. 2. *Основні загрози кібербезпеці ЄС**

**Складено автором.*

Як відповідь, EEAS через East StratCom Task Force посилила публічні контрнаративи та запускала проєкти цифрової грамотності [12].

Із 2014 р., особливо після повномасштабного вторгнення у 2022 р., Україна стала об'єктом сотень кібератак із боку рф. ЄС запровадив спільні тренування, оперативну допомогу, підтримку CERT-UA, уключення держави в окремі механізми реагування, оскільки значно посилились атаки на системи логістики, урядові портали, інфраструктуру не лише нашої держави, а й Латвії, Литви, Польщі та Фінляндії. Ці дії стали прикладом зовнішньої кіберсолідарності й правильності запровадження загальноєвропейської платформи кіберреагування.

Отже, аналіз кейсів демонструє, що загрози для Європейського Союзу мають комплексний характер – від технічних інцидентів до когнітивної війни через інформаційний простір. Відповіддю має бути не лише технологічний, а й політичний, освітній та дипломатичний підхід.

У відповідь на виклики гібридного впливу, маніпуляцій у медіапросторі й поширення дезінформації ЄС розробив багаторівневу комунікаційну стратегію. Її метою є не лише захист від інформаційних атак, а й активне просування демократичних цінностей, формування стійких до маніпуляцій суспільств.

East StratCom Task Force – підрозділ, створений у 2015 р. при Європейській службі зовнішньої дії (EEAS), є основним інструментом боротьби з дезінформацією, зокрема з боку російської федерації [12]. Його діяльність охоплює моніторинг фейків, публікацію викриттів на платформі EUvsDisinfo.eu, вироблення контрнаративів, аналітику інформаційних кампаній. Із 2022 р. активність підрозділу значно зросла – проаналізовано понад 5000 кейсів фіксацій фейкових новин у різних європейських медіа. Особливу увагу приділено війні в Україні, фейкам про НАТО, міграційну кризу та санкції ЄС.

З іншого боку, ЄС активно використовує канали публічної дипломатії для інформування зовнішньої аудиторії про свої дії. Серед інструментів – соціальні мережі офіційних представництв, програми обміну журналістами, фінансування незалежних ЗМІ, проєкти медіаграмотності:

– «Young European Ambassadors» – залучення молоді до просування європейських цінностей;

– «EU Neighbours» – інформаційна підтримка в східному партнерстві, зокрема в Україні й Грузії;

– FactcheckEU» – координація фактчекерських ініціатив [19].

Стратегічне комунікування охоплює узгоджену діяльність усіх структур ЄС – від Європейської комісії до представництв за кордоном – щодо

донесення єдиної позиції, пояснення політик, нейтралізації шкідливих наративів. Такі підходи стали відповіддю на нову форму війни – когнітивну, спрямовану на підрив довіри до інституцій ЄС. Комунікаційна стратегія ЄС має подвійний вектор – зовнішній (боротьба з дезінформацією, захист партнерів, зокрема України) і внутрішній (зміцнення стійкості європейських суспільств).

З огляду на проведене дослідження зазначимо, що Європейський Союз не єдиний глобальний актор, що стикається із сучасними кіберзагрозами. Порівняльний аналіз кібербезпек ЄС, США, Китаю, НАТО та України (табл. 4) дасть змогу нам оцінити сильні сторони та відмінності підходів, що застосовуються провідними гравцями в цій сфері.

Кібербезпекова політика ЄС своїм нормативно-інституційним підходом визначає права громадян у центрі, побудована на основі законодавчої гармонізації, децентралізованого реагування та підвищення цифрової стійкості держав-членів. Стратегічним кроком стало прийняття директиви NIS2, яка оновлює правила кіберстійкості критичних секторів (енергетика, транспорт, фінанси тощо), а також Digital Services Act, Cyber Resilience Act, що врегульовують діяльність онлайн-платформ [7; 9; 10]. Важливу роль відіграє Європейське агентство з кібербезпеки, яке координує кіберготовність і розробляє стандарти сертифікації [11]. Крім того, ЄС активно використовує інструменти публічної дипломатії, зокрема через ініціативу EUvsDisinfo [13]. Попри це, Союз постійно стикається з проблемою нерівномірної імплементації стандартів серед країн-членів та потребою в посиленні оперативного реагування [14].

США, своєю чергою, зберігають лідерство у сфері наступальної й превентивної кіберстратегії, мають сильну вертикаль, коли Cybersecurity and Infrastructure Security Agency (CISA) координує критичну інфраструктуру, військові мають незалежні повноваження, а також оновлену Стратегію 2023 р., яка вперше зафіксувала принцип «відповідальності постачальника», що покладає обов'язки на великі цифрові корпорації за безпеку користувачів [15]. Ефективно впроваджується модель «defend forward» – превентивні заходи проти зовнішніх загроз, їх проактивного виявлення та нейтралізації за межами власного кіберпростору [22], але при цьому є і свої мінуси, такі як дисбаланс між приватним і державним секторами.

Китаю притаманна жорстка централізована модель цифрового суверенітету, яка поєднує кібербезпеку з політичним контролем. Закон «Про кібербезпеку» (2017 р.) [23] установлює вимоги до всіх операторів даних, обмежуючи діяльність іноземних компаній та посилюючи внутрішній контроль. Централізованими органами є Cyberspace Administration of China

(CAC) і Міністерство державної безпеки. Так, «Великий фаєрвол Китаю» й закони CSL використовуються для цензури та кібербезпека при цьому є частиною внутрішнього контролю, системного моніторингу громадян та стратегії безпеки режиму. Пекін активно розвиває експорт цифрового авторитаризму й свої підходи до інших держав через проєкт «Цифровий шовковий шлях» [19].

НАТО, своєю чергою, не є законодавчим органом, а оборонною організацією, тому його кіберполітика зосереджена на колективному реагуванні. У 2016 р. НАТО визнав кіберпростір окремим операційним доменом, а Cyber Defence Pledge закріпив зобов'язання членів щодо підвищення кіберготовності [15]. Інституційно НАТО опирається на роботу Центру кібероборони в Таллінні (CCDCOE) і NATO Computer Incident Response Capability (NCIRC), що здійснюють технічну підтримку та проводять постійні навчання, симуляції атак (Locked Shields). Щодо слабких сторін відзначимо, що не всі країни однаково активні й Альянс діє тільки на запит члена. З актуальних переваг – доступ до розвідувальної інформації та збройних сил.

До 2022 р. Україна мала лише базові структури, а вже після опинилася в умовах безперервного цифрового протистояння. Завдяки зусиллям CERT-UA, Державної служби спеціального зв'язку [20] й Міністерства цифрової трансформації, країна створила Єдину державну систему кіберзахисту, ініціативу «Армія дронів», кібервійська, розвинула хактивізм та технології штучного інтелекту в кіберпросторі [16]. Подальший ключовий вектор розвитку полягає в інтеграції до системи NIS2, ENISA, а також залучення до спільних тренінгів із НАТО [11], [21]. Україна наразі є унікальним полігоном постійного й ефективного кіберопору, із якого інші країни отримують цінні уроки. Водночас залишаються проблеми з кадровим забезпеченням, фінансуванням, кіберосвітою та ризиком атак у режимі нон-стоп.

Із практичного боку кіберпротистояння та кіберзахисту, Україна стає цінним партнером у створенні «цифрового поясу безпеки» на східних кордонах Європейського Союзу. Залучення нашої держави до спільних ініціатив, таких як участь у CSIRT Network, обмін даними через CERT-EU, спільні тренування, відкриває нові горизонти інтеграції. Перспектива повноцінної участі Києва в кібербезпековій політиці Союзу може також стимулювати модернізацію законодавства, розвиток кіберіндустрії, формування професійної спільноти фахівців.

Отже, ЄС відрізняється унікальним правовим підходом, спрямованим на баланс між безпекою та правами людини; НАТО є зразком нормативного

Таблиця 4

Порівняльний аналіз кібербезпеки глобальних акторів міжнародних відносин

Актор	Підхід	Основні документи	Інституції	Пріоритети	Обмеження	Міжнародна роль
ЄС	Регуляторний, багаторівневий, орієнтований на права людини	NIS2, DSA, Cyber Strategy	ENISA, CSIRT, EEAS, Єврокомісія, CERT-EU, East StratCom	Захист даних, кібергігієна, міждержавна координація	Нерівномірність імплементації між країнами	Кооперативна, нормотворча
США	Агресивно-профілактичний, орієнтований на військову та приватну сфери	National Cyber Strategy (2023 р.), EO	CISA, NSA, DoD, FBI	Критична інфраструктура, кібероперації, приватно-державне партнерство	Відсутність єдиного правового кодексу	Геополітична, проактивна
Китай	Централізовано-контрольований, з елементами цензури	Cybersecurity Law (2017 р.), CSL	CAC, MSS, армійські структури	Суверенітет кіберпростору, цензура, інфраструктура	Обмеження свобод, закритість системи	Конфронтаційна, авторитарна
НАТО	Колективний оборонний, військово-технічний	Cyber Defence Pledge, CCDCOE	CCDCOE, Cyber Command	Спільна реакція, навчання, кібердоктрина	Залежність від консенсусу членів	Колективна безпека
Україна	Орієнтований на оборону, стійкість, з елементами інтеграції в ЄС	Кіберстратегія (2021 р.)	CERT-UA, Держспецзв'язку, Мінцифра	Протидія рф, інтеграція у європейські структури, цифрова трансформація	Недостатнє фінансування, нестача кадрів	Партнер ЄС і НАТО

**Складено автором.*

й багаторівневого реагування та спільної координації військових зусиль; США – стратегічно наступальні, є потужною оперативною складовою частиною, але нерідко діють автономно; Китай – повна централізація й тотальна вертикаль контролю (використовується як інструмент геополітичного впливу); Україна має практичний досвід кіберопору в умовах війни, якого не має жоден із західних партнерів.

Майбутнє кібербезпеки Європейського Союзу значною мірою залежить від здатності до адаптації, технологічного прориву та стратегічного партнерства. У цьому контексті інтеграція України в цифрові структури ЄС постає як взаємовигідний і стратегічно доцільний напрям.

Розглянемо декілька сценаріїв розвитку кібербезпеки Євросоюзу:

Сценарій 1. Інтеграційно-технологічний прорив – створення повноцінного європейського цифрового суверенітету з власними хмарними системами, інфраструктурою даних та сертифікаційними інститутами;

Сценарій 2. Обмежене поглиблення – збереження високих стандартів у провідних країнах (Німеччина, Франція, Нідерланди) та збереження розриву в слабших державах;

Сценарій 3. Кризове гальмування – посилення фрагментації, бюрократизація механізмів реагування та зниження громадської довіри через серії успішних атак.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Аналіз кібербезпеки Європейського Союзу свідчить про глибоку трансформацію підходів до захисту цифрового простору. ЄС демонструє зростаючу здатність до розбудови як нормативної, так і інституційної архітектури кіберзахисту. Основними досягненнями стали оновлення директив (NIS2), створення механізмів колективного реагування, розвиток публічної дипломатії, що дає змогу протистояти зовнішнім і внутрішнім загрозам у когнітивному вимірі.

Попри досягнення, ЄС стикається із серйозними викликами – від нерівномірного рівня цифрової готовності країн-членів до зростання гібридних атак із боку авторитарних держав. Ці обставини вимагають нових стратегій, у тому числі тіснішої співпраці з партнерами, уключаючи Україну.

Партнерство з Києвом є важливим чинником не лише політичної солідарності, а й практичного зміцнення обороноздатності Союзу. Досвід України у сфері кіберопору є унікальним джерелом інновацій і моделей стійкості, які можуть бути масштабовані в межах ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Systematic Literature Review on the NIS2 Directive. URL: https://arxiv.org/html/2412.08084v1.

2. Ruohonen, J. (2024). *The Incoherency Risk in the EU's New Cyber Security Policies.* URL: https://arxiv.org/abs/2405.12043.

3. NIS2 in a European country comparison: How are the member states implementing the new EU cybersecurity legislation? URL: https://library.e.abb.com/public/bcdef3200f414d-0ba7e2f4606bdee5d8/ABB%20NIS2%20EU%20Country%20Comparison%20Study.pdf.

4. Report on the State of the Cybersecurity in the Union. URL: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

5. Ludvigsen, K. R. (2025). *Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law.* URL: https://arxiv.org/abs/2503.07250.

6. Cîrnu, Carmen-Elena, Rotună, Carmen-Ionela, Vasiloiu, Ioana-Cristina (2023). *Comparative Analysis on Cyber Diplomacy in EU and US.* URL: file:///C:/Users/user/Downloads/ Comparative_Analysis_on_Cyber_Diplomacy_in_EU_and_%20(1).pdf.

7. European Commission (2020). The EU's Cybersecurity Strategy for the Digital Decade. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

8. The EU Cyber Solidarity Act. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

9. Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2 Directive). URL: https://www.nis-2-directive.com/

10. Digital Services Act (EU) 2022/2065. URL: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A32022R2065.

11. ENISA – European Union Agency for Cybersecurity. Official Reports. URL: https://www.enisa.europa.eu/publications.

12. Questions and Answers about the East StratCom Task Force. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en.

13. EUvsDisinfo.eu platform. URL: https://euvsdisinfo.eu/.

14. European Court of Auditors (2021). Cybersecurity in the EU: Weak coordination, strong challenges. URL: https://www.eca.europa.eu/en/publications/AAR-2024.

15. NATO CCDCOE Reports on Strategic Cyber Defence. URL: https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/.

16. CERT-UA. The CERT-UA Team has processed 2,543 cyber incidents over 2023. URL: https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

17. Користін, О. Є., Свиридюк, Н. П. (2023). *Оцінювання гібридних загроз та спроможностей протидії їм при формуванні стратегічних комунікацій.* URL: file:///C:/Users/user/Downloads/ Assessment_of_hybrid_threats_and_capabilities_to_c.pdf.

18. ENISA Threat Landscape 2023. URL: https://www.enisa.europa.eu/ publications/enisa-threat-landscape-2023.

19. Kasper, A., Osula, A.-M., Molnár A. (2021). *EU cybersecurity and cyber diplomacy.* URL: file:///C:/Users/user/Downloads/oriolbueno,+387469.pdf.

20. State Service of Special Communications and Information Protection of Ukraine. URL: https://cip.gov.ua/en.

21. The National Cybersecurity Strategy (2023). URL: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/.

22. US Cyber Command reports. URL: https://www.cybercom.mil/.

23. Cybersecurity Law of the People's Republic of China (2017). URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

REFERENCES

1. A Systematic Literature Review on the NIS2 Directive. URL: https://arxiv.org/html/2412.08084v1 (in English).

2. Ruohonen, J. (2024). *The Incoherency Risk in the EU's New Cyber Security Policies.* URL: https://arxiv.org/abs/2405.12043 (in English).

3. NIS2 in a European country comparison: How are the member states implementing the new EU cybersecurity legislation? URL: https://library.e.abb.com/public/bcdef3200f414d-0ba7e2f4606bdee5d8/ABB%20NIS2%20EU%20Country%20Comparison%20Study.pdf (in English).

4. Report on the State of the Cybersecurity in the Union. URL: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union (in English).

5. Ludvigsen, K. R. (2025). *Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law.* URL: https://arxiv.org/abs/2503.07250 (in English).

6. Cîrnu, Carmen-Elena, Rotună, Carmen-Ionela, Vasiloiu, Ioana-Cristina (2023). *Comparative Analysis on Cyber Diplomacy in EU and US.* URL: file:///C:/Users/user/Downloads/ Comparative_Analysis_on_Cyber_Diplomacy_in_EU_and_%20(1).pdf (in English).

7. European Commission (2020). The EU's Cybersecurity Strategy for the Digital Decade. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (in English).

8. The EU Cyber Solidarity Act. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity (in English).

9. Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2 Directive). URL: https://www.nis-2-directive.com/ (in English).

10. Digital Services Act (EU) 2022/2065. URL: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A32022R2065 (in English).

11. ENISA – European Union Agency for Cybersecurity. Official Reports. URL: https://www.enisa.europa.eu/publications (in English).

12. Questions and Answers about the East StratCom Task Force. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en (in English).

13. EUvsDisinfo.eu platform. URL: https://euvsdisinfo.eu/ (in English).

14. European Court of Auditors (2021). Cybersecurity in the EU: Weak coordination, strong challenges. URL: https://www.eca.europa.eu/en/publications/AAR-2024 (in English).

15. NATO CCDCOE Reports on Strategic Cyber Defence. URL: https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/ (in English).

16. CERT-UA. The CERT-UA Team has processed 2,543 cyber incidents over 2023. URL: https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti (in English).

17. Korystin, O. Ye., Svyrydiuk, N. P. (2023). *Assessing Hybrid Threats and Countermeasure Capabilities when Shaping Strategic Communications.* URL: file:///C:/Users/user/Downloads/Assessment_of_hybrid_threats_and_capabilities_to_c.pdf (in Ukrainian).

18. ENISA Threat Landscape 2023. URL: https://www.enisa.europa.eu/ publications/ enisa-threat-landscape-2023 (in English).

19. Kasper, A., Osula, A.-M., Molnár A. (2021). *EU cybersecurity and cyber diplomacy.* URL: file:///C:/Users/user/Downloads/oriolbueno,+387469.pdf (in English).

20. State Service of Special Communications and Information Protection of Ukraine. URL: https://cip.gov.ua/en (in English).

21. The National Cybersecurity Strategy (2023). URL: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/ (in English).

22. US Cyber Command reports. URL: https://www.cybercom.mil/ (in English).

23. Cybersecurity Law of the People's Republic of China (2017). URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (in English).

Матеріал надійшов до редакції 11.05.2025 р.

УДК 327-049.5(438+477)

Сергій Гемберг,
аспірант 2-го курсу за спеціальністю
291 Міжнародні відносини, суспільні комунікації та регіональні студії,
Національний унівіерситет «Острозька академія»,
serhiy.gemberg@gmail.com,
ORCID ID: 0009-0009-5045-5269;

Орест Сорокопуд,
аспірант 4-го курсу за спеціальністю
291 Міжнародні відносини, суспільні комунікації та регіональні студії,
Волинський національний університет імені Лесі Українки,
sorokopud.92@gmail.com
ORCID ID: 0000-0002-0468-007X
DOI 10.29038/2524-2679-2025-02-154-175

РОЛЬ ПОЛЬЩІ У ФОРМУВАННІ НОВОЇ АРХІТЕКТУРИ БЕЗПЕКИ В ЦЕНТРАЛЬНО-СХІДНІЙ ЄВРОПІ

У статті здійснено комплексний аналіз дипломатичної стратегії Республіки Польща щодо підтримки України в умовах повномасштабного російсько-українського конфлікту, який триває з 2022 р. Досліджено політико-