УДК 327.7:351

Кондратюк Сергій Володимирович
кандидат політичних наук,
професор кафедри публічного управління та адміністрування
Державний університет інформаційно-комунікаційних технологій
Kondratiuk Serhii
Candidate of Political Sciences,
Professor of the Department of Public Management and Administration
State University of Information and Communication Technologies
ORCID: 0009-0000-2354-8763

Верховцева Ірина Геннадіївна
доктор історичних наук, професор,
професор кафедри публічного управління та адміністрування,
Державний університет інформаційно-комунікаційних технологій
Verkhovtseva Iryna
Doctor of Historical Sciences, Professor,
Professor of the Department of Public Management and Administration
State University of Information and Communication Technologies
ORCID: 0000-0002-5682-993X

Закіров Марат Борисович
доктор політичних наук, доцент,
завідувач відділу політологічного аналізу
Національна бібліотека України імені В. І. Вернадського
Zakirov Marat
Doctor of Political Science, Associate Professor,
Head of the Department of Political Analysis
V.I. Vernadsky National Library of Ukraine
ORCID: 0000-0003-4897-4325

Кондратенко Олег Юрійович
доктор політичних наук, доцент,
професор кафедри філософії, соціології та політології
Державний торговельно-економічний університет
Kondratenko Oleh
Doctor of Political Sciences, Associate Professor,
Professor of the Department of Philosophy, Sociology and Political Science
State University of Trade and Economics
ORCID: 0000-0002-1905-934X

Любченко Андрій Володимирович
кандидат наук з державного управління,
докторант кафедри публічного управління та адміністрування
Державний університет інформаційно-комунікаційних технологій
Lyubchenko Andrii
PhD in Public Administration,
Doctoral student of the Department of Public Management and Administration
Державний університет інформаційно-комунікаційних технологій
ORCID: 0009-0004-0246-7795

Хорватова Оксана Олегівна
кандидат юридичних наук, доцент
доцент кафедри публічного управління та адміністрування
Державний університет інформаційно-комунікаційних технологій

Horvatova Oksana
PhD in Law, Associate Professor,
Associate Professor of the Department of Public Management and Administration
State University of Information and Communication Technologies
ORCID: 0000-0002-1467-3797

DOI: 10.25313/2617-572X-2025-5-10976

ЗМІЦНЕННЯ ІНСТИТУЦІЙНИХ І ЗАКОНОДАВЧИХ ОСНОВ ЄВРОПЕЙСЬКОЇ КІБЕРДИПЛОМАТІЇ В УМОВАХ ЕСКАЛАЦІЇ РОСІЙСЬКИХ ГІБРИДНИХ ЗАГРОЗ

STRENGTHENING THE INSTITUTIONAL AND LEGISLATIVE FOUNDATIONS OF EUROPEAN CYBER DIPLOMACY IN THE FACE OF ESCALATING RUSSIAN HYBRID THREATS

Анотація. *Вступ. Після початку повномасштабного російського вторгнення в Україну значно зросли та постійно модифікуються гібридні загрози з боку Кремля, спрямовані на дестабілізацію Європейського Союзу та його країн-членів. Ці загрози проявляються у безпрецедентній кількості кібератак на критичну інфраструктуру, активізації діяльності російських розвідслужб, спробах втручання у виборчі процеси, поширенні дезінформації та підриві довіри до демократичних інститутів тощо.*

Таким чином, європейські еліти постали перед необхідністю термінового нарощування власних інституційних та законодавчих спроможностей у сфері кібердипломатії та оборони для забезпечення своєї безпеки, стабільності та цифрового суверенітету. Пошук адекватної протидії деструктивній діяльності Москви є досить актуально проблемою не тільки для країн Європейського Союзу, а й для його найближчого оточення, зокрема України. Спільні виклики виступають додатковим чинником зближення позицій Києва та Брюсселя, тим самим поглиблюючи європейську інтеграцію України.

Мета статті. Проаналізувати останні зміни у європейській кібердипломатії як системну відповідь на дедалі більш агресивні російські гібридні атаки на країни ЄС, дослідити ключові чинники та особливості цього процесу, а також визначити політико-інституційні наслідки для забезпечення цифрового суверенітету Європи.

Матеріали і методи. Матеріалами дослідження є: 1) новації нормативно-правового регулювання ЄС у сфері кібербезпеки, зокрема прийняття Закону про кіберстійкість, поправок до Акту про кібербезпеку, Закону про цифрову операційну стійкість (DORA) та Закону про кіберсолідарність; 2) праці вітчизняних та європейських авторів, що провадять свої науково-практичні дослідження у царині протидії російським гібридним загрозам.

У статті були використані дедуктивні підходи на базі формальної і діалектичної логіки із залученням аналітичних методів наукового дослідження.

За допомогою діалектичного підходу в роботі встановлюється причинно-наслідковий зв'язок між російськими гібридними атаками та нарощенням інституційних і законодавчих зусиль на рівні ЄС для забезпечення кіберстійкості та цифрового суверенітету Європи.

Під поняттям аналіз розуміється використання певних рамок у класифікації одержаної інформації, окреслення термінів та усвідомлення їх суті, з'ясування критеріїв певних суджень, організацію інформаційної бази з пристосуванням її до поставлених цілей. Використовуючи аналітичні методи (системний, порівняльний, структурно-функціональний тощо) автори прагнули з'ясувати ключові чинники та особливості трансформації європейської кібердипломатії на сучасному етапі.

Результати. У роботі проаналізовано зміцнення інституційних і законодавчих основ європейської кібердипломатії на тлі ескалації російських гібридних загроз. Детально розкрито гібридні операції Росії, спрямовані на підрив демократичних інститутів в країнах ЄС та суміжних державах, зокрема під час виборів у Молдові та Румунії. Висвітлено зусилля ЄС щодо посилення оборонних спроможностей, зокрема через презентацію Білої книги європейської оборони «Готовність 2030» та Плану «Переозброєння Європи».

Визначено особливості законодавчої активності ЄС у сфері кібербезпеки, зокрема прийняття Закону про кіберстійкість, поправок до Акту про кібербезпеку, Закону про цифрову операційну стійкість (DORA) та Закону про кіберсолідарність. У висновках наголошується на складності міжнародного становища ЄС через агресивну політику Кремля та непрогнозовані дії адміністрації Д. Трампа, а також на стратегічній необхідності подальшої консолідації зусиль ЄС у сфері кібербезпеки.

Перспективи. У подальших наукових дослідженнях пропонується зосередити увагу на посиленні європейської єдності, розширенні санкційних механізмів, інвестуванні у кіберосвіту та технології, а також тіснішій співпраці як всередині ЄС, так і з партнерами з НАТО, ООН та іншими міжнародними організаціями для створення ефективної архітектури протидії гібридним загрозам.

Ключові слова: *гібридні загрози, відносини ЄС – Росія, російське втручання у вибори, кіберпростір, кібердипломатія, Біла книга європейської оборони «Готовність 2030», План «Переозброєння Європи», Закон про кіберстійкість.*

Summary. *Introduction. Since the beginning of Russia's full-scale invasion of Ukraine, the Kremlin's hybrid threats aimed at destabilizing the European Union and its member states have increased significantly and are constantly being modified. These threats are manifested in an unprecedented number of cyberattacks on critical infrastructure, intensified activities of Russian intelligence services, attempts to interfere in electoral processes, spreading disinformation and undermining trust in democratic institutions, etc.*

Thus, European elites are faced with the need to urgently build up their own institutional and legislative capabilities in the field of cyber diplomacy and defense to ensure their security, stability, and digital sovereignty. Finding an adequate response to Moscow's destructive activities is a pressing issue not only for the European Union, but also for its immediate neighborhood, including Ukraine. Common challenges are an additional factor in the convergence of positions between Kyiv and Brussels, thereby deepening Ukraine's European integration.

The purpose of the article. To analyze the recent changes in European cyber diplomacy as a systemic response to the increasingly aggressive Russian hybrid attacks on EU countries, to explore the key factors and features of this process, and to determine the political and institutional implications for ensuring Europe's digital sovereignty.

Materials and Methods. The research materials are: 1) innovations in EU cybersecurity regulation, in particular the adoption of the Cybersecurity Act, amendments to the Cybersecurity Act, the Digital Operational Resilience Act (DORA) and the Cyber Solidarity Act; 2) works by domestic and European authors conducting their scientific and practical research in the field of countering Russian hybrid threats.

The article uses deductive approaches based on formal and dialectical logic with the use of analytical methods of scientific research.

Using a dialectical approach, the paper establishes a causal link between Russian hybrid attacks and the increasing institutional and legislative efforts at the EU level to ensure cyber resilience and digital sovereignty of Europe.

The concept of analysis means the use of a certain framework in classifying the information received, defining terms and understanding their essence, clarifying the criteria for certain judgments, and organizing the information base to adapt it to the goals set. Using analytical methods (systemic, comparative, structural and functional, etc.), the authors sought to identify the key factors and features of the transformation of European cyber diplomacy at the present stage.

Results. The paper analyzes the strengthening of the institutional and legislative foundations of European cyber diplomacy against the backdrop of escalating Russian hybrid threats. The author describes in detail Russia's hybrid operations aimed at undermining democratic institutions in the EU and neighboring countries, in particular during the elections in Moldova and Romania. The author highlights the EU's efforts to strengthen its defense capabilities, in particular through the presentation of the European Defense White Paper "Readiness 2030" and the "Rearmament of Europe" Plan.

The author identifies the peculiarities of the EU's legislative activity in the field of cybersecurity, in particular the adoption of the Cybersecurity Act, amendments to the Cybersecurity Act, the Digital Operational Resilience Act (DORA) and the Cyber Solidarity Act. The conclusions emphasize the complexity of the EU's international situation due to the Kremlin's aggressive policy and unpredictable actions of the Trump administration, as well as the strategic need to further consolidate the EU's efforts in the field of cybersecurity.

Prospects. Further research is proposed to focus on strengthening European unity, expanding sanctions mechanisms, investing in cyber education and technology, and closer cooperation both within the EU and with partners from NATO, the UN and other international organizations to create an effective architecture for countering hybrid threats.

Key words: *hybrid threats, EU-Russia relations, Russian interference in elections, cyberspace, cyber diplomacy, European Defense White Paper "Readiness 2030", Plan "Rearmament of Europe", Cyber Resilience Act.*

Постановка проблеми. Ключове питання, що розглядається в статті, полягає у тому, що останні роки значно зросли та постійно модифікуються гібридні загрози з боку російської федерації, спрямовані на дестабілізацію Європейського Союзу та його країн-членів. Ці загрози проявляються у безпрецедентній кількості кібератак на критичну інфраструктуру, активізації діяльності російських розвідслужб, спробах втручання у виборчі процеси, поширенні дезінформації та підриві довіри до демократичних інститутів тощо. Особливо гостро ця проблема постала на тлі повномасштабної агресії

РФ проти України, що змусило ЄС переглянути свою роль у сфері безпеки та активізувати зусилля для протидії цим викликам. Додатковим фактором, що ускладнює ситуацію, є потенційне послаблення трансатлантичної єдності та зміни в політиці США, зокрема заяви Дональда Трампа щодо НАТО.

Таким чином, ЄС стоїть перед необхідністю термінового нарощування власних інституційних та законодавчих спроможностей у сфері кібердипломатії та оборони для забезпечення своєї безпеки, стабільності та цифрового суверенітету. Пошук адекватної протидії деструктивній діяльності Кремля є досить актуально проблемою не тільки для країн Європейського Союзу, а й для його найближчого оточення, зокрема України. Спільні виклики виступають додатковим чинником зближення позицій Києва та Брюсселя, тим самим поглиблюючи європейську інтеграцію України.

Аналіз останніх досліджень і публікацій. З початку 2024 року російська федерація значно активізувала гібридні атаки проти Європейського Союзу та його східних партнерів. Ці дії є частиною ширшої стратегії Кремля, спрямованої на досягнення своїх геополітичних цілей через підрив демократичних інститутів, поширення впливу та перешкоджання євроатлантичній інтеграції. Багатогранний характер цих загроз включає дезінформаційні кампанії, кібератаки, політичне втручання, економічний тиск і використання енергетичних ресурсів як зброї тощо. Відповідне нарощення російських зусиль по дестабілізації регіону не залишилося поза увагою як інституцій і посадовців ЄС, так і дослідницької спільноти.

У березні 2025 року Європейська служба зовнішніх справ опублікувала 3-й звіт про загрози маніпулювання та втручання іноземною інформацією (Foreign Information Manipulation and Interference, або FIMI). Кая Каллас, Верховний представник ЄС із закордонних справ та політики безпеки, віце-президент Європейської комісії, зазначала, що його новизною стало «викриття величезних цифрових арсеналів, спеціально створених росією та Китаєм для проведення своїх операцій FIMI» [1, с. 2]. Зокрема у грудні 2024 року ЄС запровадив перші в історії санкції за таку поведінку.

Варто згадати звіти EUvsDisinfo, що є флагманським проєктом Оперативної робочої групи зі стратегічних комунікацій Європейської служби зовнішніх справ [2], а також публікації Центру передового досвіду НАТО зі стратегічних комунікацій (NATO StratCom COE) [3].

Експертні публікації також багато уваги присвятили аналізу російського гібридного впливу та відзначили активізацію відповідних зусиль Кремля за останній рік. У цьому зв'язку відзначимо спільне розслідування дезінформаційних кампаній та операцій впливу експертів Центру зовнішньої політики (FPC) — незалежного, позапартійного аналітичного центру з міжнародних справ, що базується у Великій Британії [4], а також праці Корнеліу Бйола [5], Йозефа Шлерки [6], Даніели Пісо [7], Василіса Нтусаса та Лауренціу Плешку [8] тощо.

Серед вітчизняних публікацій варто відзначити перше наукове видання з кібердипломатії на основі матеріалів міжнародних наукових заходів з кібердипломатії, які відбулись по лінії МЗС України у 2024 році. Виступи та праці, присвячені проблематиці протидії гібридних загроз — Гайдука О. В., Верховцевої І. Г., Мужанової Т. М., Петькун С. М., Корченка О. Г. та інших учасників «круглого столу» [9] стали вагомим кроком на шляху інституціоналізації кібердипломатії та її системного наукового вивчення в Україні.

Враховуючи, що дослідження кібердипломатії і протидії гібридних загроз є відносно новою проблематикою в Україні та ЄС, слід констатувати, що в цій сфері досліджень залишається чимало питань, що потребують вивчення і концептуального оформлення.

Мета статті. Проаналізувати останні зміни у європейській кібердипломатії як системну відповідь на дедалі більш агресивні російські гібридні атаки на країни ЄС, дослідити ключові чинники та особливості цього процесу, а також визначити політико-інституційні наслідки для забезпечення цифрового суверенітету Європи.

Виклад основного матеріалу. Повномасштабна агресія російської федерації проти України зруйнувала світовий порядок та істотно вплинула на геополітичний вибір Європейського Союзу. В умовах наростаючої зовнішньої загрози, військових і гібридних ризиків він усвідомив себе гравцем і став одним із центрів політичної сили, одним із центрів прийняття рішень [10].

Напруження між Брюсселем і Москвою, яке зростало від 2022 року, у 2024-му досягло небезпечного рівня. Зокрема, цього року було зафіксовано безпрецедентну кількість кібератак на інфраструктуру країн-членів ЄС. Водночас посилилася діяльність російських розвідслужб: шпигунські скандали, спроби втручання у вибори, підживлення ультраправих та ультралівих сил у Європі. Пошкодження критичної інфраструктури, маневри поблизу кордонів Польщі та країн Балтії — усе це частина багатошарового гібридного тиску.

Протягом 2024 року росія активно використовувала гібридні операції, спрямовані на підрив демократичних інститутів, поширення дезінформації і недовіри до урядів, соціальний розкол у суспільствах, зокрема у Німеччині [11] та Чехії [12].

У листопаді 2024 року з різницею в кілька днів у Балтійському морі було пошкоджено два телекомунікаційних кабелі — між Німеччиною та Фінляндією та між Швецією та Литвою, що викликали істотні проблеми зі зв'язком та інтернетом [13].

Безпрецедентний рівень гібридних атак, що мали значні політичні наслідки, було продемонстровано

під час виборів у Молдові та Румунії у жовтні-грудні 2024 року. Російське втручання, задокументоване розвідувальними звітами та висновками міжнародних спостерігачів, використовувало широкий спектр гібридних тактик: масова дезінформація, незаконне фінансування (включаючи криптовалюти), кібератаки, експлуатація соціальних мереж (особливо TikTok у Румунії), тренування провокаторів та використання проксі-акторів.

Вибори у Молдові. 20 жовтня 2024 року у Молдові відбувся перший тур президентських виборів та Референдум щодо ЄС. Другий тур було проведено 3 листопада. Ці вибори мали вирішальне значення для геополітичного курсу Молдови. Насамперед йшлося про переобрання проєвропейської президентки Маї Санду та закріплення в конституції стратегічної мети вступу до ЄС, що ускладнило б майбутні спроби змінити цей курс [8].

Попри те, що Референдум щодо ЄС відбувся з мінімальною перевагою (50.35% «за»), його перебіг був позначений істотним зовнішнім втручанням. Так, 21 жовтня 2024 року в Спільній заяві Високого представника Жозепа Борреля та Європейської комісії щодо президентських виборів та конституційного референдуму у Молдові зазначалося, що перший тур президентських виборів і конституційний референдум щодо вступу до ЄС проходили в середовищі, яке характеризується «занепокоєнням учасників щодо незаконного іноземного втручання та активних зусиль з дезінформації», а також що «Росія та її ставленики активно намагалися підірвати демократичний процес і процес голосування в Молдові» [14].

Розвідувально-інформаційна служба Молдови (SIS) та інші джерела задокументували багатогранну кампанію втручання, яка координувалася, зокрема, олігархом-втікачем Іланом Шором з Москви [6,8,15]:

- Дезінформаційні кампанії: Масштабні зусилля з дискредитації європейського курсу та прозахідних політиків.
- Незаконне фінансування: Використання різноманітних методів (гранти, пожертви, готівка через кур'єрів, криптовалюти через платформи Binance, Bybit, російську систему «Мир», P2P-системи для фінансування проросійських партій та підкупу виборців. Повідомлялося про спрямування понад 15 мільйонів доларів на рахунки понад 130 000 громадян.
- Вербування та навчання активістів: Створення мережі з понад 100 «рекрутерів» та майже 2000 первинних осередків, що охопили понад 33 000 активістів, завданням яких було переконати виборців (за гроші) голосувати проти ЄС.
- Навчання тактикам протестів: Організація поїздок молоді до Москви (під прикриттям проєктів «Євразія») для навчання методам провокування поліції, фізичних сутичок, використання піротехніки, нейтралізації силовиків. Тренерами виступали, зокрема, члени «Молодої гвардії Єдиної Росії». Повідомлялося також про можливе просунуте навчання в таборах у Боснії та Герцеговині (операції з дронами, підготовка запалювальних пристроїв).
- Використання Православної Церкви: Організація «паломництв» священників до Москви, де їх схиляли до антиєвропейської позиції через контракти та фінансові стимули (виплати через систему «Мир», обіцянки винагороди).
- Кібератаки: Атаки на виборчу інфраструктуру, зокрема DDoS-атаки на урядові сайти в день референдуму.
- Використання організацій ветеранів: Використання партії «ШОР», блоку «Побєда-Victorie», НКО «АНО Євразія» як політичного прикриття та платформ для операцій впливу, поширення пропаганди та незаконного фінансування.
- Маніпуляція діаспорою: Створення центрів у Росії для консолідації діаспори та маніпулювання голосуванням за кордоном.
- Кампанії в соцмережах: Активне використання TikTok, Facebook, VKontakte.
- Фізичне втручання: Повідомлення про мінування виборчих дільниць за кордоном.

Попри те, що референдум і перемога Санду у другому турі (55.35% проти 44.65% у Олександра Стояногло) закріпили проєвропейський вектор зовнішньої політики Молдови, детальний аналіз виявив тривожні тенденції та істотні наслідки російської гібридної атаки.

По-перше, Санду програла голосування серед мешканців Молдови, отримавши на 41 тисячу голосів менше, ніж у 2020 році, тоді як проросійський кандидат наростив підтримку. Її перемога була забезпечена виключно голосами діаспори.

По-друге, Референдум щодо ЄС пройшов з мінімальною перевагою (50.35% «за»), а серед мешканців всередині Молдови підтримка склала лише 38%.

По-третє, російське втручання поглибило внутрішні розбіжності в країні та суттєво підірвало підтримку ЄС серед населення Молдови, яке виявилося вразливим до гібридних операцій і передвиборних маніпуляцій.

Усе це створює виклики для майбутньої політичної стабільності Молдови, зокрема через парламентські вибори, які мають відбутися 28 вересня 2025 року.

Президентські вибори у Румунії. Російське втручання у президентські вибори в Румунії (листопад 2024 року) мали ще більш драматичні та деструктивні наслідки для країни, що по суті опинилася на грані політичної кризи.

Результати першого туру виявилися сенсаційними: незалежний ультраправий і проросійський кандидат Келін Джорджеску, який вважався другорядним кандидатом з невеликими шансами на перемогу, отримав перше місце і пройшов до другого туру. За короткий період, він швидко отримав

значну підтримку завдяки кампанії у нетрадиційних ЗМІ, таких як TikTok, отримавши особливу популярність серед тих, хто був незадоволений поточною румунською політикою, включаючи молодь, фермерів, сільських виборців і представників робітничого класу.

Другий тур мав відбутися 8 грудня 2024 року, оскільки в першому турі жоден кандидат не набрав абсолютної більшості. Натомість 6 грудня 2024 року Конституційний суд Румунії одноголосно ухвалив рішення скасувати президентські вибори та заново провести виборчий процес в терміни, які визначить уряд.

Приводом для безпрецедентного рішення Конституційного суду стали документи Вищої ради національної оборони, які оприлюднив президент Румунії Клаус Йоганніс. Згідно з цією інформацією, на користь Джорджеску проводилася агресивна рекламна кампанія в обхід національного виборчого законодавства та з використанням алгоритмів платформ соцмереж. Ця кампанія була розгорнута приблизно за два тижні до дати виборів [16].

У інформаційній записці, яку Служба зовнішньої розвідки надіслала до Вищої ради національної оборони, повідомлялося, що Румунія стала мішенню для агресивних гібридних дій росії, включаючи кібератаки, витік інформації та саботаж. Пріоритетом для ворожих дій Росії став вплив на румунське суспільство через пропаганду та дезінформацію, а також підтримка кандидатів-євроскептиків та підживлення антисистемних рухів, зокрема шляхом «залучення їх до протестів, що формують суспільний порядок денний» [17].

Ключовим чинником російського втручання стала масована кампанія в TikTok. Румунські спецслужби та міжнародні звіти вказують на скоординовану кампанію в TikTok як основний інструмент просування Джорджеску. Було задіяно близько 25 000 акаунтів (деякі неактивні з 2016 року), спостерігалася штучна маніпуляція залученням (боти, скоординоване посилення) [5].

Як зазначали автори спільного розслідування «Мережі впливу: Розшифрування іноземного втручання у вибори Румунії»: «Ця гібридна операція втручання у вибори, методично організована для дестабілізації держави-члена НАТО та Європейського Союзу (ЄС), виходить далеко за межі Румунії. Вона відображає ширший геополітичний порядок денний, спрямований на руйнування євроатлантичної єдності, послаблення регіональної стійкості та підрив підтримки продовження війни в Україні» [4].

Румунський випадок став тривожним сигналом про те, як маніпуляції в соціальних мережах, особливо в TikTok, можуть стрімко вивести на політичну арену маргінальних кандидатів і дестабілізувати демократичні процеси, аж до анулювання виборів та спричинення глибокої політичної кризи всередині країни-члена ЄС і НАТО.

Наразі через відміну виборів Румунія переживає переломний політичний момент, який характеризується масштабними протестами громадськості. Термін повноважень президента Клауса Йоганніса було продовжено до повторних виборів. Однак він зіткнувся з масовим невдоволенням, звинуваченнями в неконституційності продовження терміну та погрозами застосування процедури імпічменту. 10 лютого 2025 року Йоганніс оголосив про свою відставку, щоб уникнути поглиблення кризи. Тимчасовим президентом став спікер Сенату Іліє Боложан.

Повторні президентські вибори в Румунії призначені на травень 2025 року. Таким чином, напередодні президентських виборів у травні 2025 року румунське суспільство є розколотим і країна постала перед проблемою подолання значних політичних турбулентностей.

Варто відзначити, що наразі у Польщі також відбуваються президентські вибори і польська влада витратила 2 мільярди євро на те, щоб не допустити втручання за «румунським сценарієм». Зокрема, виступаючи перед журналістами, міністр цифрових технологій Польщі Кшиштоф Гавковський наполягав на тому, що країна готова відбити той тип цифрового втручання, який переслідує вибори по всьому світу [18].

Станом на квітень 2025 року відносини між ЄС та Росією по суті перебувають на межі відкритого конфлікту. Від самого початку повномасштабного вторгнення РФ в Україну еліти Європейського Союзу чітко зрозуміли, що безпека континенту більше не є гарантованою. Але саме останній рік відкрив новий етап — етап прямої конфронтації, хоча й без відкритого зіткнення. Ескалація триває на багатьох рівнях — інформаційному, економічному, енергетичному, військовому.

Водночас необхідно звернути увагу на ще один важливий геополітичний фактор — вплив політики Дональда Трампа на європейську безпеку. Низка заяв Трампа, зокрема про можливу відмову США захищати союзників, які не витрачають «достатньо» на оборону, суттєво підірвала впевненість у стабільності трансатлантичних гарантій. У Москві ці сигнали розцінюються як послаблення єдності Заходу, що може провокувати нові авантюри.

По всій Європі спостерігаються ознаки того, що континент готується до «найекстремальнішого» сценарію, зокрема ЄС починає серйозно ставитися до війни з Росією за «епохи Трампа — Путіна 2.0» [19].

Європейські уряди і громадяни дедалі більше занепокоєні тим, що підбадьорений Кремль може розгорнути свої армії у їхньому напрямку після України. Також широко поширена нервозність через те, що новий президент США — ізоляціоніст — припустив, що він може не захистити історичних союзників Америки по НАТО, якщо вони зазнають нападу з боку Росії. У підсумку агресивні дії Москви та риторика Трампа щодо НАТО, яку можна коротко

сформулювати як: «Європа повинна сама себе захищати», вилилась у практичну реакцію — посилення ідеї стратегічної автономії ЄС.

У відповідь на загрози з боку Росії, Європейський Союз активізував зусилля з нарощування своїх оборонних спроможностей. 19 березня 2025 року президент Єврокомісії Урсула фон дер Ляєн та Високий представник із закордонних справ та політики безпеки/Віце-президент Європейської Комісії Кая Каллас презентували Білу книгу європейської оборони — Готовність 2030. Комісія також представила, в рамках Плану «Переозброєння Європи»/»Готовність 2030», амбітний оборонний пакет на загальну суму понад 800 млрд. євро до 2030 року, що надає державам-членам ЄС фінансові важелі для стимулювання інвестиційного сплеску в оборонний потенціал. Президент Комісії Урсула фон дер Ляєн зазначила: «Епоха мирних дивідендів давно минула. Архітектуру безпеки, на яку ми покладалися, більше не можна сприймати як належне. Європа готова зробити крок вперед. Ми повинні інвестувати в оборону, зміцнювати наші можливості та застосовувати проактивний підхід до безпеки. Ми вживаємо рішучих заходів, представляючи дорожню карту «Готовність 2030» зі збільшенням витрат на оборону, значними інвестиціями в європейський оборонно-промисловий потенціал» [20].

Загалом Біла книга визначає новий підхід до оборони та інвестиційні потреби, у той час як План «Переозброєння Європи»/»Готовність 2030» зміцнює загальноєвропейський оборонний потенціал новими фінансовими засобами. Витрати обсягом понад 800 мільярдів євро будуть спрямовані за 5 основними напрямами:

- Фіскальна гнучкість: тимчасове скасування бюджетних обмежень ЄС, що дозволить країнам-членам збільшити оборонні витрати до 1,5% ВВП (без порушення фінансових правил) протягом щонайменше 4 років. Очікується, що це залучить до 650 мільярдів євро в державах-членах ЄС.
- Запровадження нового Інструменту з досягнення безпеки в Європі (SAFE, Security Action for Europe), за яким ЄС залучить кошти до 150 мільярдів євро та надасть позики державам-членам для підтримки досягнення швидкого та значного збільшення інвестицій в оборонний потенціал Європи.
- Перерозподіл бюджету: перенаправлення існуючих коштів ЄС, зокрема фондів згуртованості, на оборонні інвестиції.
- Використання групи Європейського інвестиційного банку для підтримки оборонних підприємств через зняття обмежень на кредитування.
- Інвестиційне сприяння: створення механізму для мобілізації приватного капіталу в оборонну промисловість.

Ці заходи спрямовані на підвищення обороноздатності ЄС та зменшення залежності від зовнішніх постачальників зброї та техніки. Посадовці ЄС визнають, що до заходів із посилення оборонно-промислового комплексу спонукала насамперед загроза з боку РФ, а також потреба у диверсифікації оборонної промисловості, зокрема і зменшення залежності від США. Так, Європейський комісар із питань оборони А. Кубілюс: «Ми маємо дивитися не лише на Росію як на загрозу, але й враховувати глобальні геополітичні зміни і те, куди американці спрямовують свою стратегічну увагу» [21].

Враховуючи безпрецедентний рівень гібридних атак, які Росія спрямувала на ЄС протягом останнього року, важливою складовою Плану «Переозброєння Європи»/»Готовність 2030» є необхідність подальшої консолідації зусиль ЄС у сфері кібербезпеки, подолання імплементаційних розривів, інвестування в людський капітал та технології (включаючи квантові комунікації), зміцнення державно-приватного партнерства та міжнародної співпраці, зокрема з США, для ефективної протидії гібридним загрозам та забезпечення цифрового суверенітету Європи.

Станом на кінець квітня 2025 року, ландшафт кібербезпеки Європейського Союзу характеризується безпрецедентною законодавчою активністю, спрямованою на зміцнення колективної стійкості проти все більш складних загроз.

10 грудня 2024 року набрав чинності Закон про кіберстійкість (Cyber Resilience Act, CRA). Цей документ базується на Стратегії кібербезпеки ЄС 2020 року та Стратегії Безпекового союзу ЄС. Він запроваджує обов'язкові вимоги для виробників і роздрібних торговців щодо проектування, розробки та обслуговування продуктів, що містять цифровий компонент. Ці зобов'язання мають виконуватися на кожному етапі ланцюжка створення вартості. Закон також вимагає від виробників забезпечувати турботу протягом життєвого циклу своєї продукції.

15 січня 2025 року було ухвалено цільову поправку до Акту про кібербезпеку (The Cybersecurity Act), яка розширила повноваження Агентства ЄС з кібербезпеки (ENISA) та сферу застосування Європейської системи сертифікації кібербезпеки (ECCF) на «керовані послуги безпеки» [22]. Це охоплює такі критично важливі та чутливі послуги, як реагування на інциденти, тестування на проникнення, аудити безпеки та консалтинг, з метою забезпечення їх високого рівня якості та надійності.

З 17 січня 2025 року обов'язковим для всіх держав-членів ЄС став Закон ЄС про цифрову операційну стійкість (Digital Operational Resilience Act, широко відомий як DORA), що усуває критичну прогалину у фінансовому регулюванні ЄС. До прийняття цього закону фінансові установи переважно керували операційними ризиками, розподіляючи капітал для покриття потенційних збитків. Цей підхід не охоплював усі аспекти операційної стійкості, особливо стосовно інформаційно-комунікаційних технологій (ІКТ). З впровадженням DORA фінансові установи тепер зобов'язані дотримуватися суворих рекомендацій щодо захисту від інцидентів,

пов'язаних з ІКТ. До них належать заходи щодо захисту, виявлення, стримування, відновлення та ремонту. DORA чітко спрямований на ризики, пов'язані з ІКТ, запроваджуючи чіткі правила управління ризиками, пов'язаними з ІКТ, звітності про інциденти, тестування операційної стійкості та нагляду за ризиками третіх сторін, пов'язаними з ІКТ.

З 4 лютого 2025 року набрав чинності Закон про кіберсолідарність (Cyber Solidarity Act), який має на меті посилити спроможність ЄС виявляти кіберзагрози та інциденти, готуватися до них та реагувати на них. Він запроваджує такі ключові Компоненти:

- Європейську систему оповіщення про кіберзагрози. Ця система передбачає створення загальноєвропейської мережі національних та транскордонних центрів кібербезпеки (SOC) по всьому ЄС, які використовуватимуть передові технології, такі як штучний інтелект (ШІ) та аналітика даних, для виявлення та обміну попередженнями про загрози з органами влади за кордоном. Її мета — побудова скоординованих можливостей виявлення та ситуаційної обізнаності по всьому ЄС, посилення виявлення загроз та обміну інформацією між командами реагування на комп'ютерні надзвичайні ситуації (CERT), групами реагування на інциденти комп'ютерної безпеки (CSIRT), центрами обміну та аналізу інформацією (ISAC) та операторами критичної інфраструктури. Інформація, що обмінюється, може включати дані з мереж та сенсорів, потоки розвідданих про загрози, індикатори компрометації та контекстуалізовану інформацію про інциденти, загрози, вразливості тощо.
- Механізм надзвичайних ситуацій у сфері кібербезпеки. Цей механізм призначений для підтримки держав-членів (на їхній запит) та інших користувачів у підготовці до значних та великомасштабних кіберінцидентів, реагуванні на них, пом'якшенні їхнього впливу та ініціюванні відновлення. Він також підтримує скоординоване тестування готовності та взаємну допомогу між державами-членами.
- Резерв ЄС з кібербезпеки. Як ключова частина Механізму надзвичайних ситуацій, цей резерв складається з послуг довірених постачальників керованих послуг безпеки (MSSP). Він призначений для підтримки заходів реагування та початкового відновлення для постраждалих держав-членів, інституцій ЄС та, за певних умов, третіх країн, асоційованих із програмою «Цифрова Європа».
- Європейський механізм огляду кіберінцидентів. Цей компонент дозволяє проводити огляд та оцінку конкретних значних або масштабних кіберінцидентів для аналізу причин, наслідків, заходів пом'якшення та винесення уроків на майбутнє.

Загалом прийняття Закону про кіберсолідарність є важливим кроком від політичних декларацій до створення конкретних, фінансованих ЄС механізмів для колективного захисту. Якщо попередні зусилля значною мірою покладалися на національну імплементацію директив ЄС про мережеву та інформаційну безпеку (як NIS/NIS2) та добровільний обмін інформацією, то цей документ запроваджує спільні структури (центри, резерв), що фінансуються з бюджету ЄС (відповідно до Регламенту (ЄС, Євратом) 2024/2509 та явно спрямований на «зміцнення солідарності та спроможностей». Це свідчить про перехід до більш операціоналізованої форми солідарності, підкріпленої спільними ресурсами та інфраструктурою.

24 лютого 2025 року було опубліковано проєкт Рекомендації Європейської Ради щодо оновленого Плану реагування ЄС на кібернетичні кризи (Cyber Blueprint). Цей документ має на меті представити рамки управління кіберкризами в ЄС у чіткий, простий та доступний спосіб. Оновлений план визначає відповідних суб'єктів ЄС (ENISA, Мережа CSIRT, Комісія, Рада тощо) та їхні ролі протягом усього життєвого циклу кризи: від підготовки, спільної ситуаційної обізнаності та виявлення до реагування та відновлення. Ця ініціатива тісно пов'язана з оперативними аспектами Акту про кіберсолідарність, зокрема з Механізмом надзвичайних ситуацій.

Таким чином, реагуючи на зростаючу ескалацію з боку росії Європейський Союз активно посилює свої оборонні спроможності та колективну стійкість до гібридних загроз, водночас підтримуючи Україну в її боротьбі за суверенітет та територіальну цілісність.

Ключові законодавчі акти, такі як Акт про кіберсолідарність, Акт про кіберстійкість, зміни до Акту про кібербезпеку, разом із сектор-специфічним Законом про цифрову операційну стійкість та оновленим Планом реагування на кібернетичні кризи формують в Європейському Союзі багатошарову регуляторну систему.

Однак, амбітні законодавчі цілі ЄС стикаються з серйозними викликами в імплементації, особливо тривожною виглядає ситуація з імплементацією Директиви № 2 про мережеву та інформаційну безпеку (Network and Information Security Directive 2 або NIS2), де більшість держав-членів не вклалися у визначений термін (17 жовтня 2024 року), що створює ризик фрагментації та затримок у підвищенні рівня безпеки критичних секторів.

Висновки та перспективи подальших досліджень. Узагальнюючи попередні тези, можна зробити чіткий висновок про те, що агресивна політика Кремля та непрогнозовані дії нинішньої адміністрації Д.Трампа істотно ускладнили міжнародне становище Європейського Союзу в частині забезпечення військової безпеки та політичної стабільності.

Геополітичний контекст залишається напруженим, що яскраво демонструють нещодавні вибори в Молдові та Румунії. Російське втручання, задокументоване розвідувальними звітами та висновками міжнародних спостерігачів, використовувало широкий спектр гібридних тактик: масова дезінформація, незаконне фінансування (включаючи криптовалюти), кібератаки, експлуатація соціаль-

них мереж (особливо TikTok у Румунії), тренування провокаторів та використання проксі-акторів. Хоча в Молдові прозахідна президентка Мая Санду була переобрана, аналіз результатів виявив значну вразливість населення до російського впливу та розкол між голосами діаспори та мешканців країни. У Румунії безпрецедентне втручання призвело до анулювання першого туру виборів та глибокої політичної кризи, що підкреслило потенціал соціальних мереж для швидкої дестабілізації демократичних процесів навіть у країнах-членах ЄС та НАТО. Ці події підтверджують, що метою втручання може бути не лише перемога бажаного кандидата, а й загальна дестабілізація та підрив довіри до інститутів.

Наразі політика ЄС у сфері протидії гібридним загрозам характеризується безпрецедентною політичною та законодавчою активністю, спрямованою на підвищення обороноздатності та зміцнення колективної стійкості проти все більш складних інформаційних і кібератак.

Стратегічні імперативи визначають також необхідність подальшої консолідації зусиль ЄС у сфері кібербезпеки, подолання імплементаційних розривів, інвестування в людський капітал та технології, зміцнення державно-приватного партнерства та міжнародної співпраці, зокрема з США, для ефективної протидії гібридним загрозам та забезпечення цифрового суверенітету Європи.

Література

1. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations. *European External Action Service (EEAS).* March 2025. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf (дата звернення: 15.05.2025).

2. Двійник завдає удару у відповідь: розкриття діяльності FIMI, спрямованої проти виборів до Європейського парламенту. URL: https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections; EUvsDisinfo. (2024). Російські експерименти з дезінформацією в Молдові. URL: https://euvsdisinfo.eu/russian-experiments-with-disinformation-in-moldova/; EUvsDisinfo. (2025). Ще одні вибори, ще одна спроба втручання Кремля. URL: https://euvsdisinfo.eu/another-election-another-kremlin-interference-attempt (дата звернення: 15.05.2025).

3. Morley-Davies J., Thomas J., Baines G. Russian information operations outside of the Western information environment(Revised version). The NATO strategic communicationscentre of excellence. Riga, January 2025. URL: https://stratcomcoe.org/pdfjs/?file=/publications/download/Russian-info-operations-REVISED-VERSION-DIGITAL.pdf?zoom=page-fit (дата звернення: 15.05.2025).

4. Andra-Lucia Martinescu, Sorina Stallard & other. Networks of Influence: Decoding foreign meddling in Romania's elections, A collaborative investigation into disinformation campaigns and influence operations. December 2024. URL: https://fpc.org.uk/wp-content/uploads/2024/12/Networks-of-Influence-Decoding-foreign-meddling-in-Romanias-elections-2024.pdf (дата звернення: 15.05.2025).

5. Bjola C. Algorithmic invasions: How information warfare threatens NATO's eastern flank. *NATO REVIEW*. 07 February 2025. URL: https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html (дата звернення: 15.05.2025).

6. Šlerka J. Intelligence Report Exposes Russian Meddling in Moldova's EU Vote. *VSquare*. 2025-01-17. URL: https://vsquare.org/intelligence-report-russian-meddling-in-moldova-eu-referendum-sis-ilian-sor (дата звернення: 15.05.2025).

7. Pisoiu D. Hybrid Threats and the Role of the Far Right. Trend Report 7 / January 2025. Österreichisches Institut für Internationale Politik / Austrian Institute for International Affairs. URL: https://www.oiip.ac.at/en/publications/hybrid-threats-and-the-role-of-the-far-right/ (дата звернення: 15.05.2025).

8. Ntousas V., Pleșca L. Russian Meddling in Moldova. German Marshall Fund of the United States. October 18, 2024. URL: https://www.gmfus.org/news/russian-meddling-moldova

9. Кібердипломатія: матеріали Міжнародної науково-практичної конференції (м. Київ, 15–16 травня 2024 року), Науково-практичного круглого столу «Кібердипломатія: стратегії та практики для України, Європи та світу» (м. Київ, 28 листопада 2024 року) / за заг. ред. чл.-кор. НАН України, докт. техн. наук, проф. О.Г. Корченка; упорядники: І.Г. Верховцева, О.В. Гайдук. Київ: Дипломатична академія імені Геннадія Удовенка; Державний університет інформаційно-комунікаційних технологій, 2025. 118 с. URL: https://duikt.edu.ua/uploads/p_2850_97611772.pdf (дата звернення: 15.05.2025).

10. Долгов І. Геополітичний вимір Євросоюзу: Як змінюється ЄС і як на це впливає Україна. *Укрінформ.* 22.12.2023. URL: https://www.ukrinform.ua/rubric-world/3803258-geopoliticnij-vimir-evrosouzu-ak-zminuetsa-es-i-ak-na-ce-vplivae-ukraina.html (дата звернення: 15.05.2025).

11. США, ЄС і Британія засудили кібератаки ГРУ проти партії канцлера Шольца, оборонних та ІТ-компаній Німеччини. *Голос Америки*. 03 травень, 2024. URL: https://www.holosameryky.com/a/gru-kiberataka-nimechchyna/7596822.html (дата звернення: 15.05.2025).

12. Перун В. МЗС Чехії розповіло про кібератаку угруповання APT28 на деякі свої установи. Зловмисники використали раніше невідому вразливість у Microsoft Outlook. *LB.UA*. 3 травня 2024. URL: https://lb.ua/world/2024/05/03/611525_mzs_chehii_rozpovilo_pro_kiberataku.html (дата звернення: 15.05.2025).

13. Павлюк О. У Балтійському морі пошкодили ще один кабель зв'язку. *Європейська правда.* Понеділок, 18 листопада 2024. URL: https://www.eurointegration.com.ua/news/2024/11/18/7198677/ (дата звернення: 15.05.2025).

14. Moldova: Joint Statement by High Representative Josep Borrell and the European Commission on the Presidential Election and the Constitutional Referendum. 21.10.2024. URL: https://www.eeas.europa.eu/eeas/moldova-joint-statement-high-representative-josep-borrell-and-european-commission-presidential_en (дата звернення: 15.05.2025).

15. Report by Moldova's Intelligence and Security Service (SIS): Foreign interference in electoral processes in the Republic of Moldova. December 2024. URL: https://sis.md/sites/default/files/comunicate/fisiere/Raport_SIS_Public_Interferenta_in_procesul_electoral.pdf (дата звернення: 15.05.2025).

16. Вуець П. Румунський детектив з російським слідом. Як «благодійник» з TikTok зірвав президентські вибори. *Онлайн-медіа «Інформаційне агентство «Главком».* 10 грудня, 2024. URL: https://glavcom.ua/publications/rumunskij-detektiv-z-rosijskim-slidom-jak-blahodijnik-z-tiktok-zirvav-prezidentski-vibori-1035421.html (дата звернення: 15.05.2025).

17. Document CSAT Serviciul de Informații Externe. 04.12.2024. URL: https://cutt.ly/JrlJFq42 (дата звернення: 15.05.2025).

18. Lasica J. Can Poland's cyber umbrella stop digital election meddling? Monocle: Affairs, April 23, 2025. URL: https://monocle.com/affairs/poland-cyber-umbrella-elections/ (дата звернення: 15.05.2025).

19. Smith A. Europe braces for 'most extreme' military scenario as Trump-Putin 2.0 begins. NBC News. Jan. 26, 2025. URL: https://www.nbcnews.com/news/world/trump-putin-europe-war-ukraine-attack-baltic-germany-finland-sweden-rcna187924 (дата звернення: 15.05.2025).

20. Єврокомісія оприлюднила Білу книгу європейської оборони та План «Переозброєння Європи/Готовність 2030». 19.03.2025. Press and information team of the Delegation to UKRAINE. URL: https://cutt.ly/7rzaWF4d (дата звернення: 15.05.2025).

21. ЄС посилює оборонні спроможності. *Служба зовнішньої розвідки України.* 21.03.2025. URL: https://szru.gov.ua/news-media/news/ies-posylyuie-oboronni-spromozhnosti-1742515200000 (дата звернення: 15.05.2025).

22. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services. COM/2023/208 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208 (дата звернення: 15.05.2025).

References

1. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations. European External Action Service (EEAS). March 2025. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

2. EUvsDisinfo. (2024). Doppelganger Strikes Back: Unveiling FIMI Activities Targeting European Parliament Elections. URL: https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections; EUvsDisinfo. (2024). Russian experiments with disinformation in Moldova. URL: https://euvsdisinfo.eu/russian-experiments-with-disinformation-in-moldova/; EUvsDisinfo. (2025). Another election, another Kremlin interference attempt. URL: https://euvsdisinfo.eu/another-election-another-kremlin-interference-attempt.

3. Morley-Davies J., Thomas J., Baines G. Russian information operations outside of the Western information environment(Revised version). THE NATO STRATEGIC COMMUNICATIONSCENTRE OF EXCELLENCE. Riga, January 2025. URL: https://stratcomcoe.org/pdfjs/?file=/publications/download/Russian-info-operations-REVISED-VERSION-DIGITAL.pdf?zoom=page-fit.

4. Andra-Lucia Martinescu, Sorina Stallard & other. Networks of Influence: Decoding foreign meddling in Romania's elections, A collaborative investigation into disinformation campaigns and influence operations. December 2024. URL: https://fpc.org.uk/wp-content/uploads/2024/12/Networks-of-Influence-Decoding-foreign-meddling-in-Romanias-elections-2024.pdf.

5. Bjola C. Algorithmic invasions: How information warfare threatens NATO's eastern flank. NATO REVIEW. 07 February 2025. URL: https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html.

6. Šlerka J. Intelligence Report Exposes Russian Meddling in Moldova's EU Vote. — VSquare. 2025-01-17. URL: https://vsquare.org/intelligence-report-russian-meddling-in-moldova-eu-referendum-sis-ilian-sor.

7. Pisoiu D. Hybrid Threats and the Role of the Far Right. Trend Report 7 / January 2025. Österreichisches Institut für Internationale Politik / Austrian Institute for International Affairs. URL: https://www.oiip.ac.at/en/publications/hybrid-threats-and-the-role-of-the-far-right/.

8. Ntousas V., Pleșca L. Russian Meddling in Moldova. German Marshall Fund of the United States. October 18, 2024. URL: https://www.gmfus.org/news/russian-meddling-moldova.

9. Kiberdyplomatiia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii (m. Kyiv, 15–16 travnia 2024 roku), Naukovo-praktychnoho kruhloho stolu "Kiberdyplomatiia: stratehii ta praktyky dlia Ukrainy, Yevropy ta svitu" (m. Kyiv, 28 lystopada 2024 roku) / za zah. red. chl.-kor. NAN Ukrainy, dokt. tekhn. nauk, prof. O. H. Korchenka; uporiadnyky: I. H. Verkhovtseva, O. V. Haiduk. Kyiv: Dyplomatychna akademiia imeni Hennadiia Udovenka; Derzhavnyi universytet informatsiino-komunikatsiinykh tekhnolohii, 2025. 118 s. URL: https://duikt.edu.ua/uploads/p_2850_97611772.pdf.

10. Ihor Dolhov. Heopolitychnyi vymir Yevrosoiuzu: Yak zminiuietsia YeS i yak na tse vplyvaie Ukraina. Ukrinform. 22.12.2023. URL: https://www.ukrinform.ua/rubric-world/3803258-geopoliticnij-vimir-evrosouzu-ak-zminuetsa-es-i-ak-na-ce-vplivae-ukraina.html.

11. SShA, YeS i Brytaniia zasudyly kiberataky HRU proty partii kantslera Sholtsa, oboronnykh ta IT-kompanii Nimechchyny. Holos Ameryky. 03 traven, 2024. URL: https://www.holosameryky.com/a/gru-kiberataka-nimechchyna/7596822.html.

12. Perun V. MZS Chekhii rozpovilo pro kiberataku uhrupovannia APT28 na deiaki svoi ustanovy. Zlovmysnyky vykorystaly ranishe nevidomu vrazlyvist u Microsoft Outlook. LB.UA. 3 travnia 2024. URL: https://lb.ua/world/2024/05/03/611525_mzs_chehii_rozpovilo_pro_kiberataku.html.

13. Pavliuk O. U Baltiiskomu mori poshkodyly shche odyn kabel zviazku. Yevropeiska pravda. Ponedilok, 18 lystopada 2024. URL: https://www.eurointegration.com.ua/news/2024/11/18/7198677/.

14. Moldova: Joint Statement by High Representative Josep Borrell and the European Commission on the Presidential Election and the Constitutional Referendum. 21.10.2024. URL: https://www.eeas.europa.eu/eeas/moldova-joint-statement-high-representative-josep-borrell-and-european-commission-presidential_en.

15. Report by Moldova's Intelligence and Security Service (SIS): Foreign interference in electoral processes in the Republic of Moldova. December 2024. URL: https://sis.md/sites/default/files/comunicate/fisiere/Raport_SIS_Public_Interferenta_in_procesul_electoral.pdf.

16. Vuiets P. Rumunskyi detektyv z rosiiskym slidom. Yak "blahodiinyk" z TikTok zirvav prezydentski vybory. Onlain-media "Informatsiine ahentstvo "Hlavkom". 10 hrudnia, 2024. URL: https://glavcom.ua/publications/rumunskij-detektiv-z-rosijskim-slidom-jak-blahodijnik-z-tiktok-zirvav-prezidentski-vibori-1035421.html.

17. Document CSAT Serviciul de Informații Externe. 04.12.2024. URL: https://cutt.ly/JrlJFq42.

18. Lasica J. Can Poland's cyber umbrella stop digital election meddling? Monocle: Affairs, April 23, 2025. URL: https://monocle.com/affairs/poland-cyber-umbrella-elections/.

19. Smith A. Europe braces for 'most extreme' military scenario as Trump-Putin 2.0 begins. NBC News. Jan. 26, 2025. URL: https://www.nbcnews.com/news/world/trump-putin-europe-war-ukraine-attack-baltic-germany-finland-sweden-rcna187924.

20. Commission unveils the White Paper for European Defence and the ReArm Europe Plan/Readiness 2030. 19.03.2025. Press and information team of the Delegation to UKRAINE. URL: https://cutt.ly/7rzaWF4d.

21. YeS posyliuie oboronni spromozhnosti. Sluzhba zovnishnoi rozvidky Ukrainy. 21.03.2025. URL: https://szru.gov.ua/news-media/news/ies-posylyuie-oboronni-spromozhnosti-1742515200000.

22. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services. COM/2023/208 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208.

Стаття надійшла до редакції 20.05.2025