УДК 341.24:07-049.5](477:4)
DOI https://doi.org/10.32782/apfs.v050.2024.29

М. В. Білоусов
ORCID ID: https://orcid.org/0000-0002-1008-9649
аспірант кафедри міжнародних відносин та зовнішньої політики
Чорноморського національного університету імені Петра Могили

МІСЦЕ УКРАЇНИ В БЕЗПЕКОВОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ ЄС: АНАЛІЗ НОРМАТИВНО-ПРАВОВОЇ БАЗИ

Постановка проблеми. Слід зазначити, що повномасштабний наступ РФ на Україну 24 лютого 2022 р. став справжнім переломним моментом в історії і України і Європи XXI ст.. Це радикально змінило європейський стан безпеки, зокрема інформаційної. Російська агресія є не невиправданим нападом на Україну, а й нападом на кардинальні цінності Європи – свободу, демократію та права людини. Сьогодні, підтримка України в інформаційному просторі залишається стратегічним пріоритетом ЄС.

Протягом 2022-2024 рр. була виявлена зростаюча кількість широкого спектру дій з боку РФ проти ЄС та його держав-членів, включаючи кібератаки, інформаційні маніпуляції та кампанії втручання, порушення супутникового зв'язку, випадки підпалів, вандалізму та саботажу, зокрема проти критичної інфраструктури держав-членів ЄС. Ці зловмисні дії є частиною широкої скоординованої гібридної кампанії, спрямованої РФ як спроба розділити європейське суспільство, дестабілізувати, послабити ЄС та його держави-члени, а також підірвати європейську підтримку України та її здатність захищатися.

Завдяки рішенню встановити спеціальну систему обмежувальних заходів з огляду на деструктивну діяльність РФ, ЄС робить рішучі кроки у цьому напрямку саме на законодавчому рівні. Відповідно до нової законодавчої бази, ЄС може переслідувати тих, хто відповідальний за протиправні дії в інформаційній сфері, реалізує, підтримує або отримує вигоду від дестабілізуючих дій РФ в усьому світі, а також їхніх спільників і прихильників. ЄС продовжує зміцнювати свою інформаційну стійкість, тісно співпрацювати з партнерами та повною мірою використовувати існуючий інструментарій ЄС, включаючи дипломатичні та обмежувальні заходи, а також усі доступні інструменти для запобігання, стримування та реагування на гібридну діяльність Росії [20].

Хоча країни-члени ЄС не були безпосередньо залучені в російсько-українську гібридну війну, їхні мережі та інформаційний простір зазнали атак, що потребувало серйозних заходів для посилення їх кібербезпеки. Збройний напад РФ на Україну в лютому 2022 р. трансформував концепцію безпеки ЄС. Багато в чому це можна розглядати як кульмінацію тривалого конфлікту, який йому передував. Гібридна війна, яка тривала майже десятиліття до її повномасштабної фази, також активно вплинула на формування концепції безпеки ЄС. Зміна ставлення та нормативних актів щодо кібербезпеки була невід'ємною частиною цієї трансформації. Адже, високий рівень цифровізації в державах-членах та їхніх суспільствах зробив їх надзвичайно вразливими в кіберпросторі. Слід зазначити, що протягом 2022-2024 рр. ЄС активно працює над вдосконаленням нормативно-правової бази у сфері захисту безпекового інформаційного простору і проявляє ініціативну у співпраці з Україною, яка постраждала від впливу російської гібридної війни.

Актуальність обраної проблематики посилюється недостатньою розробкою тематики та невисоким ступенем висвітлення у вітчизняній науковій школі і потребує детального аналізу.

Аналіз останніх досліджень і публікацій. Актуальність обраної нами теми дослідження підкреслює наявність результатів напрацювання зарубіжних науковців, зокрема, європейських та американських дослідників, які ми застосували для врахування напрацювань закордонних фахівців у нашому дослідженні. Варто згадати такі прізвища: Р. Келемен [24], Й. Пшетачник, Л. Тотова [26], Е. Валтонен [32]. Ця категорія дослідників приходить до висновку, що ЄС має тісну співпрацю у сфері інформаційної безпеки та кібербезпеки, як з міжнародними партнерами, так і з Україною. А з початком повномасштабного вторгнення РФ в Україну у лютому 2022 р. ця співпраця постійно посилюється і набуває обертів як на двосторонньому, так і на тристоронньому рівнях.

З іншого боку маємо відмітити, що обрана проблематика мало висвітлена у працях українських дослідників, що ще більше актуалізує тему. Зокрема, серед українських дослідників, які звертали увагу на місце України в безпековому інформаційному просторі ЄС з точки зору нормативно-правової бази, слід згадати роботи вітчизняних дослідників С. С. Троян [4], А. О. Хмель [6;7], М. Гончар, А. Чубик, С. Жук, О. Чижова, Г. Максак, Ю. Тищенко, О. Зварич [1], А. Правдюк [25].

Ця категорія дослідників аналізує стан інформаційної безпеки ЄС та України, зокрема, як комплексне явище і робить акцент на потребі вдосконалення існуючої нормативно-правової бази у сфері інформаційної безпеки з урахуванням посилення гібридних загроз з боку РФ.

Слід зазначити, що не тільки науковці, але й безпосередні практики, такі як Ю. Шипілова [8]; О. Кабанов та Т. Олексіюк [3]; К. Федоренко, Л. Поляков, І. Козій [19] аналізують проблеми інформаційної безпеки ЄС та місце в ній України в своїх аналітичних доробках.

Виділення невирішених раніше частин загальної проблеми. Розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий завдяки інформаційній безпеці. Зростання кількості масштабних дезінформаційних кампаній, інформаційна політика РФ, яка є агресивною, виступає як загроза демократії та суверенітету не тільки нашої держави, а й всіх країн-учасниць ЄС, викликає нагальну потребу в удосконаленні та розширенні законодавчих ініціатив з боку України та ЄС.

Автор вважає, що невирішеними частинами загальної проблеми залишаються: 1) гармонізація законодавства України з чинним законодавством ЄС у сфері підвищення ефективності системи захисту персональних даних громадян; 2) посилення відповідальності за порушення встановлених вимог; 3) врегулювання питання державно-приватного партнерства у сфері кібербезпеки між Україною та ЄС на законодавчому рівні.

Метою статті є здійснення аналізу місця України в безпековому інформаційному просторі ЄС на законодавчому рівні.

Виклад основного матеріалу дослідження. Варто зазначити, що протягом 2014-2022 рр. РФ активно вела гібридну війну, в якій військові заходи не були основними. Головними заходами в російській гібридній війні (2014-2022 рр.) проти ЄС стали: інформаційний тиск, пропаганда, економічна війна і т.д. Однак, у лютому 2022 р. з початком повномасштабного вторгнення військова складова – стала основною. Тобто, звичайна війна посилилася потужною дезінформаційною кампанією РФ проти України і проти ЄС.

Сьогодні, РФ активно використовує розвиток інформаційних технологій для поширення дезінформації та пропаганди. Антизахідна пропаганда є частиною інформаційної війни РФ. На відміну від РФ, однією з головних цінностей в Європі є свобода слова, тому контролювати дезінформацію майже неможливо, що ще раз підкреслює важливість прийняття відповідних рішень країнами-учасницями ЄС на законодавчому рівні, з метою усунення цієї проблеми.

Про російські дезінформаційні операції проти України йдеться в українській Доктрині інформаційної безпеки 2017 р.. У документі перераховані загрози дезінформації, серед яких, зокрема, проведення спеціальних інформаційних операцій, спрямованих на розпалювання етнічного та релігійного конфлікту в Україні, створення негативного іміджу України за кордоном та зниження морального духу української армії [3]. До цих загроз також можна додати: політичну та лобістську діяльність на Заході проти України, а також діяльність, що підриває позитивне сприйняття українцями ЄС; інформаційну ізоляцію окупованих територій від України; створення і підтримка російської пропаганди та відтворення її на проросійських каналах, які зловживають свободою слова для дискредитації України та поширення інформаційної продукції з метою розколу суспільства та підготовки соціальної бази для нових протестів і провокацій [26].

Слід зазначити, що ЄС протягом останнього десятиліття більш активно протидіє гібридним загрозам, в яких більш впливовим фактором є саме інформаційний вплив. Зазначимо, що гібридні загрози – сукупність дій, які застосовуються державними або ж недержавними акторами з метою маніпуляції вразливими системами конкретних держав або організацій [7, с. 119].

Варто пригадати той факт, що ще на початку 2010-х рр. ЄС визнав необхідність втручання у сферу кібербезпеки, оскільки змістовно проблема є транскордонною і охоплює все суспільство [1, с. 55].

У 2016 р. ЄС прийняв Спільну програму про протидію гібридним загрозам [22], спрямовану на сприяння координації на рівні ЄС, покращення обізнаності про ситуацію та підвищення стійкості. Того ж року ЄС створив Центр аналізу гібридних загроз для сприяння обміну інформацією між державами-членами про гібридні загрози [10]. У 2017 р. ЄС створив Набір інструментів кібердипломатії для спільної дипломатичної реакції на зловмисну поведінку в кіберпросторі. А в 2018 р. ЄС опублікував Спільну програму про «Підвищення стійкості та зміцнення можливостей протидії гібридним загрозам» [19; 21].

У Стратегічному компасі безпеки та оборони ЄС на 2022 р. [11] гібридні загрози та захист критичної інфраструктури визнано за ключові сфери, де ЄС має покращити свої зусилля. Стратегічний компас пропонує плани щодо створення гібридного інструментарію ЄС для координації відповіді ЄС і держав-членів на гібридні атаки шляхом поєднання всіх доступних цивільних і військових інструментів, які можна використовувати проти гібридних загроз. ЄС також планує створити гібридні групи швидкого реагування ЄС, які надаватимуть спеціалізовані національні, цивільні та військові експертизи для підтримки держав-членів, місій Спільної політики

безпеки та оборони і країн-партнерів у протидії гібридним загрозам.

Стратегія кібербезпеки України на 2021-2025 рр., яка координується Національним координаційним центром кібербезпеки, спрямована на створення «умов для безпечного функціонування кіберпростору» [2]. Документ стосується концепцій стримування, стійкості та взаємодії стосовно кіберпростору України. 25 жовтня 2021 р. Рада національної безпеки і оборони України (РНБО) запропонувала створити галузевий центр кібербезпеки, який зосередиться на захисті критичної енергетичної інфраструктури (наприклад, енергетики, нафти та газу). Ще до повномасштабного вторгнення Україна шукала подальшої підтримки від ЄС і НАТО на тлі підвищених загроз нападу на такі основні активи [25, с. 43].

Тоді як 22 листопада 2022 р. Україна вирішила законодавчо визнати – на експериментальній основі – кваліфіковані електронні підписи, що походять з держав-членів ЄС, 25 січня 2023 р. Комісія опублікувала інструменти (список довірених країн третіх країн), які полегшують перевірку електронних підписів або печаток, створених у третіх країнах. Україна стала першою третьою країною в цьому списку.

1 грудня 2022 р. Верховна Рада прийняла Закон про внесення змін до деяких законодавчих актів щодо забезпечення укладення угоди між Україною та ЄС про взаємне визнання кваліфікованих електронних довірчих послуг та імплементацію законодавства ЄС у сфері електронної ідентифікації. Закон передбачає обов'язкову оцінку відповідності кваліфікованих постачальників довірчих послуг незалежними органами відповідно до моделі сертифікації, подібної до моделі ЄС [16].

28 лютого 2022 р., через кілька днів після того, як РФ розпочала повномасштабну війну проти України, Київ офіційно подав запит на прискорену процедуру, щоб стати країною-кандидатом на членство в ЄС. Прохання було позитивно сприйняте багатьма лідерами ЄС та Європейським парламентом. У вівторок, 1 березня 2022 р., Європарламент прийняв резолюцію на підтримку надання Україні статусу кандидата, а 10-11 березня 2022 р. це питання обговорювалося на неформальному саміті Європейської ради в Парижі, де лідери ЄС визнали «європейський вибір України», але не схвалили прискорене членство країни [31].

Поряд з цим, з моменту прийняття в березні 2022 р. ЄС швидко реалізував багато цілей, поставлених у Стратегічному компасі. Агресивна війна РФ проти України додала ще більшої гостроти зусиллям зробити ЄС сильнішим і надійнішим учасником безпеки та оборони. Країни-члени ЄС швидко запустили «Компас» і мобілізували інструменти, передбачені на його чотирьох стовпах. Це включало надання летального та нелетального обладнання, а також навчання понад 40 000 українських військових та нарощування потенціалу Збройних сил України. Стратегічний компас – це амбітний план дій щодо зміцнення політики безпеки та оборони ЄС до 2030 р. [11].

ЄС та Україна підтримували діалог у сфері кібербезпеки з початку війни, зосереджуючись на посиленні стійкості. Європейська служба зовнішніх дій оцінює, що «завдяки тісній співпраці з ЄС та іншими міжнародними партнерами у сфері кібербезпеки та кібербезпеки оборони, Україна продемонструвала величезний потенціал для відбиття кібератак і захисту своєї критичної інфраструктури» [28].

Слід зазначити, що початок російсько-української війни призвів до посилення співпраці між ЄС та НАТО, що дало значні результати у сфері кібербезпеки, часто вираженої військовими термінами. Відомо, що центральною темою саміту НАТО у Мадриді у 2022 р. була російсько-українська війна та підтримка України. Підсумковий документ наголошує на зміцненні стратегічного партнерства при повазі цілісності ЄС та НАТО, посиленого їхньою спільною прихильністю до України. Кіберпростір залишався центральною темою. У комюніке саміту зазначено, що кібернетичні, космічні, гібридні та інші асиметричні загрози, а також зловмисне використання нових і руйнівних технологій, повинні вирішуватися у співпраці.

Обидві організації зобов'язуються продовжувати підтримку України проти РФ, включаючи надання нелетального оборонного обладнання для посилення кіберзахисту та стійкості України. З російсько-українською війною енергетична безпека стала пріоритетом. Вони спрямовані на прискорення адаптації Альянсу та підвищення стійкості до кібернетичних і гібридних загроз шляхом інтегрованого застосування політичних і військових інструментів [24, с. 86].

Також, відповідно до Підсумкового документа, ЄС зробив значні кроки для посилення кібербезпеки України після початку війни. З березня 2022 р. по лютий 2023 р. ЄС виділив на ці цілі майже 11 млн євро. Його основною метою була підтримка потреб української влади в кібербезпеці та безпеці даних, зосереджуючись на заміні знищеного обладнання та забезпеченні безперервної роботи державних послуг під час війни. Естонська академія електронного урядування очолила реалізацію проекту, використовуючи свій досвід цифрового управління та кібербезпеки для підтримки України в цей критичний час.

Наступним кроком був Вільнюський саміт НАТО 2023 р., у підсумковому документі якого було підтверджено, що російсько-українська

війна поглибила співпрацю ЄС-НАТО з непохитною відданістю подальшій підтримці України, наприклад, шляхом створення спільної Координаційної групи ЄС-НАТО. У результаті обговорень під час Саміту було досягнуто значного прогресу в таких сферах, як протидія дезінформації, гібридним і кіберзагрозам, тероризм, а також розбудова обороноздатності, оборонна промисловість і дослідження. Тим не менш, співробітництво слід і далі розширювати в таких сферах, як стійкість, захист критичної інфраструктури, нові та революційні технології, космос, геостратегічна конкуренція та тісніша співпраця з промисловістю та академічними колами [33].

Наступною важливою подією на законодавчому рівні стало підписання 12 липня 2023 р. Спільної декларації підтримки України [23], згідно з якою: «ЄС і Україна посилюватимуть співпрацю у сфері стійкості, зосереджуючись на протидії гібридним і кіберзагрозам, маніпулюванню іноземною інформацією та втручанню, а також захисту критичної інфраструктури. ЄС підтримуватиме Україну у запобіганні, стримуванні та реагуванні на ці загрози шляхом інтегрованого використання наборів інструментів ЄС, а також для підвищення кіберстійкості шляхом навчання з кібербезпеки, підтримки законодавчої та політичної розробки, методологічної сумісності та технічної допомоги» [23].

Також у Спільній декларації підтримки України зазначається, що: «ЄС та Україна прагнутимуть і далі активізувати політичну та технічну співпрацю з кібернетичних питань, у тому числі використовуючи створений кібердіалог. Україна прагнутиме посилити співпрацю в рамках Європейського центру передового досвіду з протидії гібридним загрозам (м. Гельсінкі, Фінляндія)» [23].

ЄС є провідною організацією у світі за діяльністю, розробленими стратегіями та проектами з точки зору кібербезпеки. Кібербезпека часто є головною темою різноманітних конференцій та зустрічей ЄС, більше того, кібератака вважається найактуальнішою проблемою в ЄС. Цю тему контролюють спеціальні агентства: «Агентство мережевої та інформаційної безпеки ЄС» (ENISA), Європейський центр боротьби з кіберзлочинністю (EUROPOL/EC3), Європейське оборонне агентство (EDA) [15, с. 200].

У грудні 2023 р. Агентство ЄС з кібербезпеки (ENISA) оформило робочу домовленість з українськими колегами. Робоча домовленість базується на дискусії, розпочатій у 2022 р. у Варшаві під час Діалогу з кібербезпеки між Україною та ЄС. Ця домовленість спрямована на розбудову спроможностей, обмін найкращими практиками та підвищення обізнаності про ситуацію. Угоду про партнерство з ENISA, з української сторони, підписали Національний координаційний центр з кібербезпеки та Адміністрація Державної служби спеціального зв'язку та захисту інформації України. Секретар РНБО України, голова Національного координаційного центру кібербезпеки Олексій Данілов так описав значення згаданої домовленості: «Це історичний день для нашої країни і, безперечно, важливий крок на шляху України до ЄС. Співпраця з ENISA відкриває нові можливості для посилення співробітництва у сфері кібербезпеки та обміну найкращими практиками з державами ЄС. Що особливо важливо зараз, коли Україна перебуває в авангарді глобальної кібервійни, яку веде РФ. Об'єднання наших зусиль зміцнить європейську систему кібербезпеки, а Україна братиме участь у формуванні стратегічних підходів та розробці нових політик у сфері кібербезпеки та кіберзахисту на міжнародному рівні» [17].

Голова Державної служби спеціального зв'язку та захисту інформації України (ДССЗІ) Юрій Щиголь додав: «… Кіберпростір став повноцінною складовою війни, яку РФ веде проти України. Ця війна також дала всьому світу чітке розуміння того, що цивілізований світ лише разом може протистояти агресії в кіберпросторі. Ми готові обмінюватися інформацією та ділитися досвідом України у першій у світі кібервійні, щоб допомогти кожній країні стати сильнішою перед лицем нових загроз» [5].

Передбачається співпраця в таких сферах:

1. Розвиток кіберобізнаності та потенціалу для підвищення кіберстійкості: включаючи сприяння участі в якості представників третіх країн у конкретних загальноєвропейських навчаннях або тренінгах з кібербезпеки, можливі домовленості про відрядження, а також обмін та просування інструментів і програм кіберобізнаності.

2. Обмін найкращими практиками для забезпечення узгодження законодавства та впровадження, зокрема такого як NIS-2, і таких секторів, як телекомунікації та енергетика.

3. Систематичний обмін знаннями та інформацією щодо ландшафту загроз кібербезпеці для підвищення загальної обізнаності про ситуацію серед зацікавлених сторін і спільнот [17].

21 травня 2024 р. Європейська рада схвалила висновки згідно яких державні та недержавні суб'єкти все частіше використовують гібридну тактику, створюючи зростаючу загрозу безпеці ЄС, його держав-членів і партнерів, а також закликала інституції ЄС і країни-члени активізувати дії для моніторингу спроб іноземних акторів втрутитися в демократичний процес ЄС.

Через місяць, 27 червня 2024 року, Європейська рада рішуче засудила всі типи гібридної діяльності, яка збільшується та спрямована проти ЄС, його держав-членів і партнерів. Крім того, Європейська Рада закликала, серед іншого, продовжити роботу в Раді щодо встановлення нового

режиму санкцій з огляду на гібридні загрози [27]. Цього ж дня, у Брюсселі Президент України Володимир Зеленський, Президент Європейської ради Шарль Мішель і Президент Європейської комісії Урсула фон дер Ляєн підписали Спільні зобов'язання щодо безпеки між Україною та ЄС. Документ підтверджує готовність усіх держав-членів посилити санкції ЄС проти РФ, протидіяти спробам їх обійти, а також співпрацювати у протидії гібридним загрозам і кіберзагрозам та забезпеченні вільного судноплавства в Чорному та Азовському морях [29].

Багатогранний характер гібридного втручання РФ становить серйозну загрозу європейській безпеці. Ерозія довіри, дестабілізація економічних і політичних систем і руйнування критичної інфраструктури можуть мати драматичні наслідки. ЄС, як суб'єктові, який заснований на принципі співпраці, варто визначити комплексні стратегії боротьби з гібридними загрозами, посилити заходи кібербезпеки та підвищити стійкість держав-членів до кампаній з дезінформації [7, с. 120].

Роботу, яка виконується в Гельсінкі Європейським центром боротьби з гібридними загрозами, що відкритий як для держав-членів ЄС, так і для держав-членів НАТО, було посилено і тепер вона здатна допомагати ще ефективніше розширювати можливості держав-учасниць боротися з гібридними загрозами та запобігати їм.

Боротьба зі складними та взаємопов'язаними загрозами безпеці вимагає цілісного підходу. Це означає, що безпека є змінною концепцією, яка виходить за рамки традиційної військової оборони та об'єднує інформаційні, економічні, соціальні, екологічні та політичні аспекти [32].

15 липня 2024 р. ЄС та Україна провели III рауд кібердіалогу у Брюсселі. Сторони домовилися про подальшу співпрацю у сфері кібербезпеки. Міністерство цифрової трансформації України продовжує працювати над стратегією кіберуправління та проектами з кібербезпеки, а також над посиленням міжнародної співпраці в рамках Талліннського механізму. Кібербезпека є наскрізним елементом цифрової інтеграції, тому є головним пріоритетом, особливо в рамках Українського механізму. Флагманські проекти, такі як «CyberEast», спрямовані на підвищення кіберстійкості в країнах Східного партнерства, також триватимуть. Крім того, зусилля з кіберпідтримки будуть координуватися з державами-членами та партнерами, в тому числі через Талліннський механізм [30].

Крім того, Міністерство цифрової трансформації України працює над посиленням спроможності органів державної влади та реформуванням українського законодавства відповідно до стандартів ЄС. Україна прагне приєднатися до роумінгової зони ЄС «Роумінг, як вдома» та інтегруватися в єдиний цифровий ринок ЄС.

ЄС та Україна обговорили мінливий ландшафт кіберзагроз, поділилися новинами щодо останніх законодавчих розробок. Ключовим пріоритетом для України є подальше узгодження з Директивою ЄС щодо безпеки мережевих та інформаційних систем. Україна рухається до приведення у відповідність до вимог, встановлених на рівні ЄС Директивою NIS-2 [9].

Також Україна та країни ЄС працюють у двосторонньому форматі в напрямку кібербезпеки. Так, у лютому 2024 р. між Україною та Італією була підписана Угода про співробітництво у сфері безпеки. Задля розвитку Спільної декларації країн «Групи семи», яка була підписана у Вільнюсі 12 липня 2023 р., Італія спільно з іншими країнами буде сприяти у питаннях безпекових зобов'язань для України. Сторони приділили увагу також співробітництву у сфері інформаційної безпеки. Україна та Італія будуть вести співробітництво задля покращення можливостей України протистояти інформаційним загрозам, російському або ж будь-якому інформаційному маніпулюванню, зловмисній пропаганді та дезінформаційним кампаніям, які негативно впливають на національну безпеку. В Угоді також зазначається, що сторони будуть сприяти розробці спільних освітніх і навчальних програм для фахівців з інформаційної безпеки та постійному обміну досвідом у цій сфері [12].

16 лютого 2024 р. була підписана Угода про співробітництво та довгострокову підтримку у сфері безпеки між Україною та ФРН. Сторони погодились продовжувати взаємну співпрацю у сфері протидії російській та будь-якій іншій інформаційній маніпуляції та пропаганді. Україна та Німеччина спільно сприятимуть розвитку спроможності України протистояти загрозам інформаційній безпеці, вживатимуть спільних заходів для протидії дезінформації з боку іноземних держав та організацій, а також прагнутимуть розробити спільні освітні та навчальні програми для експертів у сфері стратегічної комунікації та публічної дипломатії, регулярний обмін досвідом та професійні заходи із залученням експертів у сфері стратегічної комунікації та публічної дипломатії [13].

В Угоді про співробітництво у сфері безпеки між Україною та Францією, яка була підписана того ж дня зазначається, що сторони співпрацюватимуть для покращення спроможностей України протистояти іноземному втручанню та маніпулюванню інформацією, насамперед російським пропагандистським та дезінформаційним кампаніям, обмінюватимуться досвідом та сприятимуть розробці спільних освітніх та тренінгових програм для фахівців з інформаційної цілісності [14].

Висновки та перспективи подальших розвідок у цьому напрямі. У сучасному світі інформаційна війна стала такою ж потужною зброєю, як

і фізична. Підсумовуючи, варто зазначити, що Україна, борячись за своє існування, також знаходиться і на передовій захисту європейської системи та європейських цінностей. РФ прагне досягти політичних цілей шляхом гібридної війни чи інформаційної кампанії, не вдаючись до військової сили, або використовуючи її обмежено. ЄС вжив заходів для пом'якшення кіберризиків, пов'язаних із гібридною війною, посилення мережевої та когнітивної безпеки. Однак наступальні кібероперації все частіше можуть призвести до відкритого збройного конфлікту. Під час існуючих конфліктів деякі кібероперації можуть підірвати довіру суспільства та ще більше загострити ситуацію. ЄС та його державам-членам варто приділяти пильнішу увагу динаміці ескалації у своєму законодавстві та практиці. Дуже важливо уважно вивчати кіберполітику, встановлювати конкретні цілі та терміни та регулярно їх оновлювати. Це вимагатиме від зацікавлених сторін пошуку відповідних нормативних рівнів і узгодження національних норм, практики та стандартів.

ЄС та його держави-члени рішуче засуджують посилення кампанії гібридної діяльності РФ проти ЄС, його держав-членів і партнерів. Автор статті здійснив аналіз місця України в безпековому інформаційному просторі ЄС на законодавчому рівні і виокремлює в законодавчій базі три рівні: 1) двосторонні угоди між Україною та державами-членами ЄС (зокрема, Угода про співробітництво у сфері безпеки між Україною та Італією; Угода про співробітництво та довгострокову підтримку у сфері безпеки між Україною та ФРН (лютий 2024 р.); 2) двосторонні угоди між Україною і ЄС (Спільна декларація підтримки України у 2023 р.); 3) тристоронні угоди Україна-ЄС-НАТО (підсумковий документ Вільнюського саміту НАТО у 2023 р., в якому було підтверджено, що російсько-українська війна поглибила співпрацю ЄС-НАТО з непохитною відданістю подальшій підтримці України, наприклад, шляхом створення спільної Координаційної групи ЄС-НАТО). Підписані документи наголошують на тому, що засобом протидії інформаційним загрозам є інтеграція України в регіональний європейський інформаційний простір.

З моменту повномасштабного вторгнення РФ в Україну, ЄС та країни-члени вжили широких правових та політичних заходів для підтримки України. ЄС зазнав багатьох правових та інституційних змін. Європейський парламент, Комісія та Рада швидко погодили статус кандидата для України. ЄС та Україна мають намір продовжувати тісну співпрацю між відповідними органами, включаючи структуровану співпрацю, яка забезпечується робочою домовленістю з ENISA – Агентством ЄС з кібербезпеки та операційною угодою з Європолом. ЄС значно посилив свою кібер-підтримку України з початку неспровокованої та невиправданої російської агресії в лютому 2022 р. та має намір продовжувати підтримувати Україну для зміцнення її кіберстійкості, зміцнення взаємодії та підтримки щодо запобігання, виявлення та стримування і реагування на кіберзагрози, зокрема щодо критичної інфраструктури та мереж.

У цьому контексті перспективним напрямом для подальших наукових розвідок є дослідження ефективного нормативно-правового забезпечення для системи інформаційної безпеки України з урахуванням її місця в безпековому інформаційному просторі ЄС.

Література

1. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і східного партнерства. Аналітичний документ. М. Гончар, А. Чубик, С. Жук, О. Чижова, Г. Максак, Ю. Тищенко, О. Зварич. Київ, 2018. 106 с.

2. Стратегія кібербезпеки України (2021 – 2025 роки). *РНБО: офіційний сайт.* 2021. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 23.11.2024).

3. Кабанов О., Олексіюк Т. Відповідність законодавства України окремим положенням правового регулювання сфери відкритих даних у Європейському Союзі. Аналітичний звіт. Київ, 2023. URL: https://eef.org.ua/wp-content/uploads/2023/07/Vidpovidnist-zakonodavstva-Ukrayiny-okremym-polozhennyam-pravovogo-regulyuvannya-sfery-vidkrytyh-danyh-u-YEvropejskomu-Soyuzi.pdf (дата звернення: 23.11.2024).

4. Троян С. С. Інформаційно-безпекова політика Європейського Союзу. *Зовнішні справи : суспільно-політичний журнал.* 2019. № 2/3. С. 28–32.

5. Україна посилює співпрацю з ЄС у сфері кібербезпеки: НКЦК підписав Угоду про співпрацю з ENISA. *РНБО: офіційний сайт*. 2023. URL: https://www.rnbo.gov.ua/ua/Diialnist/6706.html?PRINT (дата звернення: 23.11.2024).

6. Хмель А. О. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). *Acta de Historia & Politica: Saeculum XXI*. Вип. 4. 2022. С. 91–101.

7. Хмель А. О. Місце гібридних загроз у Стратегії безпеки ЄС 2020. *The European Union's Experience of Responding to Security Challenges.* Proceedings of the All-Ukrainian scientific-methodical seminar. Within the Erasmus+ Jean Monnet Modules project 621046-EPP1-2020-1-EN-EPPJMO-MODULE European political integration: historical retrospective and nowadays. Hlukhiv. 2021. P. 117–123.

8. Шипілова Ю. Правова база української кібербезпеки: загальний огляд і аналіз. *Міжнародна фундація виборчих систем в Україні*, 2019. 40 с. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf (дата звернення: 23.11.2024).

9. 3rd EU-Ukraine Cyber Dialogue takes place in Brussels. *The Ministry of foreign affairs of Ukraine: official*

web-site. 2024. 16 of July. URL: https://mfa.gov.ua/en/news/tretij-raund-kiberdialogu-ukrayina-yes-vidbuvsya-u-bryusseli (дата звернення: 23.11.2024).

10. A Europe that protects: good progress on tackling hybrid threats. *European Commission: official web-site*. 2019. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2788 (дата звернення: 23.11.2024).

11. A Strategic Compass for Security and Sefence. *European Union: official web-site*. 2022. URL: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en (дата звернення: 23.11.2024).

12. Agreement on security ccoperation between Ukraine and Italy. *Governo Italiano Presidenza del Consiglio dei Ministri: official web-site*. 2024. URL: https://www.governo.it/sites/governo.it/files/Accordo_Italia-Ucraina_20240224_1.pdf (дата звернення: 23.11.2024).

13. Agreement on security cooperation and long-term support between the Federal Republic of Germany and Ukraine. *Bundesregierung: offcial web-site*. 2024. URL: https://www.bundesregierung.de/resource/blob/2196306/2260158/d84fa168bdd3747913c4e8618bd196af/2024-02-16-ukraine-sicherheitsvereinbarung-eng-data.pdf?download=1 (дата звернення: 23.11.2024).

14. Agreement on security cooperation between Ukraine and France. *President of Ukraine: official web-site*.2024. URL: https://www.president.gov.ua/en/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-89005 (дата звернення: 23.11.2024).

15. Bitsadze T. EU's Cyber Security Strategy Before and During the War in Ukraine. 2023. P. 193-210. URL: https://www.researchgate.net/publication/374641321_EU's_Cyber_Security_Strategy_Before_and_During_the_War_in_Ukraine (дата звернення: 23.11.2024).

16. Commission staff working document, Ukraine 2023, Report. *European Commission: official web-site*. 2023. URL: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_699%20Ukraine%20report.pdf (дата звернення: 23.11.2024).

17. Enhanced EU-Ukraine cooperation in Cybersecurity. *European Cybersecurity Competence Centre and Network: official web-site*. 2023. 08 of December. URL: https://cybersecurity-centre.europa.eu/news/enhanced-eu-ukraine-cooperation-cybersecurity-2023-12-08_en (дата звернення: 23.11.2024).

18. European Parliament resolution of 11 February 2021 on the implementation of the EU Association Agreement with Ukraine (2019/2202(INI)). *European Parliament: official web-site*. 2021. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0050_EN.html (дата звернення: 23.11.2024).

19. Fedorenko K., Polyakov L., Koziy I. Cooperation between Ukraine and the European Union in the Security Sector Public Monitoring Report. *The Institute for Euro-Atlantic Cooperation*, 2019. 25 p. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/Cooperation-between-Ukraine-and-the-European-Union-in-the-Security-Sector.-Public-Monitoring-Report.pdf

20. Hybrid threats/Russia: Statement by the High Representative on behalf of the EU on Russia's continued hybrid activity against the EU and its Member States. *Delegation of the European Union to Ukraine*. 2024. 08 of October. URL: https://www.eeas.europa.eu/delegations/ukraine/hybrid-threatsrussia-statement-high-representative-behalf-eu-russia%E2%80%99s-continued-hybrid-activity_en (дата звернення: 23.11.2024).

21. Joint Communication: Increasing resilience and bolstering capabilities to address hybrid threats. *European Union: official web-site*. 2018. URL: https://www.eeas.europa.eu/node/46397_en (дата звернення: 23.11.2024).

22. Joint Framework on countering hybrid threats, Joint communication to the European Parliament and the council. *European Union: official web-site*. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (дата звернення: 23.11.2024).

23. Joint security commitments between the European Union and Ukraine. *European Council Council of the European Union*. 2023. URL: https://www.consilium.europa.eu/media/oredhmis/eu-ukraine-security-commitments-en.pdf (дата звернення: 23.11.2024).

24. Kelemen R. The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations. *The Quarterly Journal*. Vol. 22. No 2. 2023. P. 75–90. URL: https://doi.org/10.11610/Connections.22.2.55 (дата звернення: 23.11.2024).

25. Pravdiuk A. Problems of legal regulation of the information security system in Ukraine. *European Political and Law Discourse*. № 9 (2). 2022. P. 40–47. URL: https://eppd13.cz/wp-content/uploads/2022/2022-9-2/07.pdf

26. Przetacznik J., Tothova L. EU-Ukraine relations and the security situation in the country. *European Parliament: official web-site*. 2022. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698907/EPRS_BRI(2022)698907_EN.pdf (дата звернення: 23.11.2024).

27. Russia: New sanctions framework against those responsible for destabilising activities against the EU and its member states. *European Council: official web-site*. 2024. 08 of October. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/russia-eu-sets-up-new-framework-for-restrictive-measures-against-those-responsible-for-destabilising-activities-against-the-eu-and-its-member-states/ (дата звернення: 23.11.2024).

28. Ukraine and EU Held the Second Round of the UA-EU Cybersecurity Dialogue. *European External Action Service*. 2022. 29 of September. URL: https://www.eeas.europa.eu/ eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en. (дата звернення: 23.11.2024).

29. Ukraine and the EU Signed the Joint Security Commitments. *President of Ukraine: official web-site*. 2024. 27 of June. URL: https://www.president.gov.ua/en/news/ukrayina-ta-yes-pidpisali-spilni-bezpekovi-zobovyazannya-91813 (дата звернення: 23.11.2024).

30. Ukraine: 3rd Cyber Dialogue with the European Union takes place in Brussels. *European Commission: official web-site*. 2024. URL: https://digital-strategy.ec.europa.eu/en/news/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels (дата звернення: 23.11.2024).

31. Ukraine's EU application: A new paradigm for EU Enlargement? *The Institute of International and European Affairs*. 2022. URL: https://www.iiea.com/blog/ukraines-eu-application-a-new-paradigm-for-eu-enlargement?gad_source=1&gclid=Cj0KCQjwpvK4BhDUARIsADHt9sQ4lgPcKzj6hpz9XcbycCxCuKSm2KuYjJukWZN07UosShWdSMmD7TQaAhG5EALw_wcB (дата звернення: 23.11.2024).

32. Valtonen E. Europe's defence against Russia. *Fondation Robert Schuman*. 2024. 17 of September. URL: https://www.robert-schuman.eu/en/european-issues/760-europe-s-defence-against-russia (дата звернення: 23.11.2024).

33. Vilnius Summit Communiqu . *NATO: official website*. 2023. 11 of July. URL: https://www.nato.int/cps/en/natohq/official_texts_217320.htm (дата звернення: 23.11.2024).

Анотація

Білоусов М. В. **Місце України в безпековому інформаційному просторі ЄС: аналіз нормативно-правової бази.** – Стаття.

Охарактеризовано основні нормативно-правові акти, які регулюють сферу безпеки в інформаційному просторі ЄС та України на сучасному етапі, з урахуванням аналізу трьох рівнів у законодавчій базі, а саме двосторонні угоди між Україною та провідними державами-учасницями ЄС; двосторонні угоди Україна-ЄС; тристоронні угоди Україна-ЄС-НАТО.

Зазначено, що Доктрина інформаційної безпеки України (2017 р.); Стратегія кібербезпеки України на 2021-2025 рр.; Резолюція Європарламенту щодо імплементації Угоди між Україною та ЄС від лютого 2021 р.; Закон про внесення змін до деяких законодавчих актів щодо забезпечення укладення угоди між Україною та ЄС про взаємне визнання кваліфікованих електронних довірчих послуг та імплементацію законодавства ЄС у сфері електронної ідентифікації (2022 р.), спрямовані на наближення українського законодавства у сфері інформаційної безпеки до законодавства та стандартів ЄС.

Акцентовано, що Спільна програма ЄС про протидію гібридним загрозам (2016 р.); Стратегічний компас безпеки та оборони ЄС на 2022 р., який є амбітним планом дій щодо зміцнення політики безпеки та оборони ЄС до 2030 р.; Спільна декларація підтримки України (2023 р.); Спільні зобов'язання щодо безпеки між Україною та ЄС (2024 р.) виступають основними законодавчими ініціативами з боку ЄС для підтримки України в безпековому інформаційному просторі від моменту повномасштабного вторгнення РФ в Україну у лютому 2022 р..

Зроблено висновок, що важливою подією стало оформлення у 2023 р. робочої домовленості між Агентством ЄС з кібербезпеки (ENISA) та українськими партнерами, яка дозволяє сторонам співпрацювати у протидії гібридним загрозам і кіберзагрозам з боку РФ. Двосторонні угоди між Україною та Італією, Францією, ФРН підписані у 2024 р. дозволяють спільно протистояти російському або ж будь-якому інформаційному маніпулюванню, зловмисній пропаганді та дезінформаційним кампаніям, які негативно впливають на національну безпеку України.

Завдяки охарактеризованим нормативно-правовим актам Україна братиме участь у формуванні стратегічних підходів та розробці нових політик у сфері кібербезпеки та кіберзахисту на міжнародному рівні.

Ключові слова: Україна, Європейський Союз, НАТО, РФ, інформаційна безпека, інформаційні загрози, нормативно-правова база.

Summary

Bilousov M. V. **Ukraine's place in the EU information space: analysis of the regulatory framework.** – Article.

The main normative legal acts regulating the sphere of security in the information space of the EU and Ukraine at the present stage are characterized, taking into account the analysis of three levels in the legislative base, namely bilateral agreements between Ukraine and the leading EU member states; bilateral agreements Ukraine – EU; trilateral agreements Ukraine – EU – NATO.

It is noted that the Doctrine of Information Security of Ukraine (2017); Cybersecurity Strategy of Ukraine for 2021-2025; Resolution of the European Parliament on the implementation of the Agreement between Ukraine and the EU (February 2021); Law on Amendments to Certain Legislative Acts to Ensure the Conclusion of an Agreement between Ukraine and the EU on the Mutual Recognition of Qualified Electronic Trust Services and the Implementation of EU Legislation in the Field of Electronic Identification (2022), aimed at bringing Ukrainian legislation in the field of information security closer to EU legislation and standards.

It is emphasized that the EU Joint Programme on Countering Hybrid Threats (2016); the EU Strategic Compass for Security and Defence (2022), which is an ambitious action plan to strengthen the EU's security and defence policy until 2030; the Joint Declaration of Support for Ukraine (2023); the Joint Security Commitments between Ukraine and the EU (2024) are the main legislative initiatives on the part of the EU to support Ukraine in the information security space since the full-scale invasion of Ukraine by the Russian Federation in February 2022.

It was concluded that an important event was the formalization in 2023 of a working agreement between the EU Agency for Cybersecurity (ENISA) and Ukrainian partners, allowing the parties to cooperate in countering hybrid threats and cyber threats from the Russian Federation. Bilateral agreements between Ukraine and Italy, France, Germany signed in 2024 allow jointly countering Russian or any information manipulation, malicious propaganda and disinformation campaigns that negatively affect the national security of Ukraine.

Thanks to the described regulatory and legal acts, Ukraine will take part in the formation of strategic approaches and the development of new policies in the field of cybersecurity and cyber defense at the international level.

Key words: Ukraine, European Union, NATO, Russian Federation, information security, information threat, legal framework.