УДК 327.7:002.1-049.5](477+4ЄС)
DOI https://doi.org/10.32782/apfs.v053.2025.30

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

СПІВРОБІТНИЦТВО УКРАЇНИ ТА ЄС У БЕЗПЕКОВОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ РФ: ПРАКТИЧНА ПЛОЩИНА

Постановка проблеми. Російсько-українська війна показала необхідність реформування системи європейської безпеки та впровадження нових ініціатив. В основі стратегічного зовнішньополітичного курсу України лежить європейська інтеграція, яка передбачає розвиток та поглиблення відносин з ЄС та його державами-членами в багатьох сферах спільного інтересу. Однією з таких сфер є співробітництво України та ЄС в безпековому інформаційному просторі, яка є ключовою з точки зору забезпечення конкурентоспроможності та технологічної безпеки країн у довгостроковій перспективі.

Російські гібридні операції в Європі стають все більш частими та агресивними, особливо після початку повномасштабного вторгнення РФ на територію України у лютому 2022 р.. Російське повномасштабне вторгнення до України стало переломним моментом для глобальної кіберсфери та підтвердило необхідність посиленого та ширшого міжнародного співробітництва. Оскільки кібербезпека є органічною частиною інформаційної безпеки, а РФ здійснює постійні кібератаки на цифрову інфраструктуру ЄС та України, то для України важлива співпраця з європейськими партнерами в цій сфері. Протягом останніх років Україна та ЄС вжили заходів для поглиблення співпраці у напрямку кібербезпеки, оскільки російські гібридні атаки, спрямовані на підрив підтримки Києва, і напруга на континенті продовжує зростати. Ключовим аспектом цього партнерства є приведення українського законодавства у відповідність до Директиви NIS-2, яка регулює кібербезпеку в Європі.

Слід зауважити, що плани щодо створення українських кібервійськ існували ще до повномасштабної війни, але останнім часом пріоритети змінилися. Крім захисту критичної інфраструктури, кібервійська проводили б наступальні або контрнаступальні кібероперації. Автор статті вважає, що Україні необхідно переймати, просувати та поширювати цей досвід.

Актуальність обраної проблематики посилюється недостатньою розробкою тематики, невисоким ступенем висвітлення у вітчизняній і європейській наукових школах і динамічними зміна актуальних обставин, що, відповідно, потребує детального аналізу.

Аналіз останніх досліджень і публікацій з даної теми. Слід відмітити, що обрана проблематика мало висвітлена у працях українських дослідників, що ще більше актуалізує тему. Зокрема, І. Підберезних, О. Коваль, Ю. Соломін, В. Кривошеїн, Т. Плазова [20] досліджують інформаційну безпеку України як складову в системі міжнародної інформаційної безпеки і надають перелік основних загроз інформаційній безпеці країни в умовах російсько-української війни.

Серед українських дослідників, які звертали увагу на практичний аспект співробітництва України та ЄС у безпековому інформаційному просторі, слід згадати такі прізвища: І. Дудко, В. Пашковський [12], Я. Ізмайлов, І. Єгорова [16], які висвітлюють політико-правові основи, а також процес практичної співпраці України з ЄС, що є впливовою силою для протидії РФ та захисту інформаційної сфери України в умовах російської гібридної війни.

А. Ю. Морозов, Н. Б. Шуст [5], В. Ю. Горєлова, С. М. Вихрист [4], Л. Веселова [31] звертають увагу на удосконалення нормативно-правового забезпечення інформаційної безпеки України з урахуванням європейського досвіду. В. Омельяненко [19], І. Семенець-Орлова, А. Клочко [22], О. Цебенко, О. Івасечко [28], Н. Голованова [3] досліджують співпрацю України та ЄС у сфері кіберзахисту та деталізують практичні дії останніх у сфері цифрової дипломатії. В. Федоренко, Н. Литвин, Д. Лученко, І. Панова, Н. Цибульник [15] аналізують правові аспекти управління інформаційною безпекою в умовах європейської інтеграції України.

Окремо можна зазначити українських авторів, які висвітлювали співробітництво України та окремих країн ЄС в сфері інформаційної безпеки: Л. В. Буга [1], В. В. Шемчук [8], А. О. Хмель [7].

Щодо представників європейської наукової школи слід згадати такі прізвища: Дж. Крістов [10], М. Цану [27], Дж. Рерл [21], Р. Келемен [17]. Вказані автори займалися дослідженням впливу російської гібридної війни на політику та регулювання ЄС у сфері кібербезпеки, але не висвітлювати конкретні факти співробітництва ЄС та України у цій площині, що ще раз підкреслює проблематику обраного дослідження.

Метою статті є аналіз практичного аспекту співробітництва України та ЄС в безпековому інформаційному просторі.

Виклад основного матеріалу дослідження. Одними з основних викликів та загроз інформаційній безпеці для України сьогодні є інформаційна війна, інформаційний тероризм та інформаційні злочини. Вони зумовлені глобальними інформаційними процесами, прогресом у розвитку інформаційних технологій та інформаційною складовою гібридної війни РФ проти України. Використання РФ технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протистояння. Саме проти України РФ використовує новітні інформаційні технології для впливу на свідомість громадян, спрямовані на розпалювання міжнаціональної та релігійної ворожнечі, пропаганду агресивної війни, силову зміну конституційного ладу чи порушення суверенітету та територіальної цілісності України [22, с. 79], спотворює історичні факти і намагається спростувати право України на незалежність, самостійність, суверенність, суб'єктність у світовій політиці.

З 2014 р. Україна отримує практичний досвід боротьби з кібератаками, будучи основним випробувальним майданчиком для РФ. Україна здійснила низку ініціатив для забезпечення своєї кіберстійкості перед повномасштабним вторгненням – створення багаторівневої системи кіберзахисту для державної ІТ-інфраструктури, переміщення обладнання та резервне копіювання баз даних у безпечніші райони України, створення хмарних сховищ даних в інших державах тощо [8, с. 35].

Україна розвиває власну кібербезпеку у напрямках захисту комп'ютерних мереж і протидії кіберзлочинності, орієнтуючись на модель ЄС. Слід зазначити, що ще у 2015 р. було ратифіковано Меморандум про взаєморозуміння між Україною та Європейським поліцейським офісом щодо створення захищеної лінії зв'язку SIENA [2]. У 2017 р. було підписано Меморандум про конфіденційність та забезпечення захисту інформації. У 2018 р. українським спеціалістам з кібербезпеки вдалося заблокувати близько 400 кібератак. Деякі з них, на думку СБУ, могли мати наслідки не менші, ніж результати вірусу Petya-A.11 [1, с. 176; 29].

У 2016 р. була створена Європейська міжсекторальна організація ESCO як контрактний партнер Європейської Комісії для здійснення партнерства у сфері кібербезпеки [10, с. 111]. ECSO, яка представляє основу європейської екосистеми кібербезпеки та об'єднує весь спектр зацікавлених сторін європейської кібербезпеки, проявляє солідарність з Україною та її громадянами у їхній поточній боротьбі. З моменту повномасштабного вторгнення РФ на територію України у лютому 2022 р. членство в ECSO надається всім українським державним і приватним організаціям без будь-яких комісій. Партнерство між ECSO та Україною буде зосереджено на 9 пріоритетних сферах:

1. Створення осередку "Women4Cyber" в Україні. "Women4Cyber" – це некомерційна європейська приватна фундація, метою якої є сприяння, заохочення та підтримка участі жінок у сфері кібербезпеки. Сьогодні "Women4Cyber" має 20 національних представництв і онлайн спільноту з 35 тис. членів. У рамках співпраці ECSO з Україною створення відділення "Women4Cyber" розглядається як пріоритет і одна з перших дій.
2. Доступ до HR-спільноти ECSO.
3. Організація днів кіберінвестора для українських стартапів.
4. Доступ до ринку "Cyber Solution Days" для українських малих та середніх підприємств (МСП). МСП, як постачальники кібербезпеки, так і кінцеві користувачі, є основою європейської економіки. Зміцнення їхніх можливостей та спроможності вимагає спеціальних дій та ініціатив. ECSO добре розуміє цю потребу та впроваджує багатовимірні дії, які будуть поширені на українську екосистему.
5. Доступ до фінансування ЄС для цифрових питань.
6. Співпраця між головними менеджерами з інформаційної безпеки (CISOs).
7. Підтримка впровадження політики ЄС щодо кібербезпеки.
8. Обмін найкращими практиками між екосистемами кібербезпеки ЄС та України.
9. Підтримка зв'язку з органами державної влади [32].

Щорічно Агентство з кібербезпеки України проводить аудит своїх поточних стратегій. У рамках процесу вступу до ЄС Україна оновлює свою стратегію кібербезпеки до 2021 р., щоб вона відповідала європейським стандартам. Україна також працює над створенням кібервійськ. Декілька законопроєктів в українському парламенті пропонують створення спеціальних кібервійськових підрозділів, причому, найімовірнішим сценарієм, вони будуть розміщені у складі Збройних сил України (далі – ЗСУ).

17–19 травня 2021 р. у Києві відбулися навчання з кібербезпеки для представників українських державних органів за кошти ЄС. Понад 30 співробітників Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України та Кіберполіції України взяли участь у тренінгу з протидії кібератакам. Українська команда займалася полюванням на загрози та іншими конкретними заздалегідь визначеними завданнями, які розкривалися

учасникам лише під час навчань. Українські ІТ-фахівці дізналися, як працюють зловмисники, оскільки імітаційні атаки були запущені організаторами на заздалегідь визначену ІТ-інфраструктуру. Навчання проводилися в рамках проєкту "EU4DigitalUA", що фінансується ЄС, Естонською академією електронного урядування на базі оновленого Кіберцентру UA30, де розміщено унікальний для України навчальний центр. Таких центрів у світі лише 20 [13].

"EU4DigitalUA" є частиною підтримки України з боку ЄС та продовжує роботу проєкту EGOV4UKRAINE, який реалізовувався у 2016–2021 рр. у рамках Програми "U-LEAD з Європою". З бюджетом 20,5 млн євро "EU4DigitalUA" зосереджена на подальшому розвитку цифрової урядової інфраструктури, публічних електронних послуг, кібербезпеки та захисту даних. Проєкт фінансується ЄС, а також спільно реалізується Академією електронного урядування (Естонія) та Міжнародною Іберо-американською фундацією з управління та публічної політики (Іспанія) [12, с. 180].

Протягом останніх чотирьох років проєкт "EU4DigitalUA", фінансований ЄС, підтримував цифрову трансформацію України. Станом на кінець березня 2024 р. команда Академії електронного урядування завершила реалізацію трьох компонентів проєкту загальним бюджетом 10 млн євро. Ці компоненти включають взаємодію та цифрову урядову інфраструктуру, розвиток електронних послуг і кібербезпеку. За майже чотири роки існування проєкту "EU4DigitalUA" Україна зробила великий ривок у сфері цифровізації державного управління.

Сторонами проведено дві хвилі практичних кібернавчань, а експерти проєкту розробили рекомендації щодо обміну інформацією про кіберзагрози, що допомогло гармонізувати українське законодавство з нормами ЄС та покращити реакцію на масштабні російські кібератаки під час війни. Крім того, розроблено та технічно впроваджено Підсистему моніторингу доступу до персональних даних, яка допоможе українцям краще контролювати свої персональні дані.

«Україна створила унікальну ефективну систему електронного урядування та ефективно використовує цифрові інструменти для подолання викликів, спричинених війною. "EU4DigitalUA" продемонстрував, як спільними зусиллями ЄС та України можна досягти реальних змін та покращити якість життя людей», – зазначила Катаріна Матернова, Посол ЄС в Україні [24].

Одним із пріоритетних напрямків є інституційна співпраця між європейськими та українськими органами. Державна служба спеціального зв'язку та захисту інформації України, Національний координаційний центр кібербезпеки України та Агентство ЄС з кібербезпеки підписали угоду про співпрацю у сфері кібербезпеки. У листопаді 2023 р. Україна підписала угоду з Агентством ЄС з кібербезпеки (далі – ENISA). Угода потребувала спеціального схвалення Європейської комісії, оскільки ENISA вперше співпрацювала з країною, що не входить до ЄС. У рамках угоди Україна тепер співпрацює з ENISA щодо загроз кібербезпеці, регулярно зустрічаючись з європейською стороною для обміну аналітикою загроз [14].

15 липня 2024 р. ЄС та Україна провели ІІІ кібердіалог у Брюсселі, під час якого домовилися про подальше поглиблення співпраці у сфері кібербезпеки [9].

У березні 2025 р. українські та європейські агенції з кібербезпеки підписали Меморандум про взаєморозуміння на Київському міжнародному форумі кіберстійкості для підтримки спільних досліджень, інновацій та проєктів, що фінансуються ЄС у транскордонних проєктах з кібербезпеки. Меморандум є рамковою угодою, яка дає змогу обом сторонам почати практичну співпрацю [18].

«Ми розраховуємо, що зможемо залучити український бізнес до цих програм підтримки, що дасть йому змогу ефективніше взаємодіяти з європейським бізнесом і розвиватися разом. … Стрімкий розвиток в Україні військової техніки та штучного інтелекту, всі ці інновації, які з'являються в Україні на тлі війни, також цікаві європейцям, і ми також будемо з ними взаємодіяти в цьому напрямку», – зазначив Сергій Прокопенко, заступник начальника управління кібербезпеки РНБО України [30].

Під час Форуму сторони домовились організувати додаткове навчання для цивільних і військових організацій на основі потреб України Європейським коледжем безпеки та оборони, Консультативною місією ЄС і Військовою місією ЄС з підтримки України.

Українські державні інституції, університети та бізнес зможуть брати участь у програмах, доступних за рахунок фінансування ЄС, шляхом організації додаткового навчання. Закон ЄС про кіберсолідарність наразі залучає компанії для реагування на інциденти, до яких сподіваються приєднатися українські компанії. Такі проєкти, як "CyberEast", який зосереджується на покращенні кіберстійкості в країнах Східного партнерства, також триватимуть.

Нагадаємо, що "CyberEast" є спільним проєктом ЄС та Ради Європи протягом 2019–2022 рр., який реалізується в регіоні Східного партнерства. Країнами-учасницями проєкту є Молдова, Вірменія, Білорусь, Грузія, Азербайджан та Україна. Проєкт був спрямований на прийняття законо-

давчих та політичних рамок, які відповідають Будапештській конвенції про кіберзлочинність та пов'язаних з нею інструментів, зміцнення спроможності судових і правоохоронних органів і міжвідомчої співпраці, а також підвищення ефективної міжнародної співпраці та довіри щодо кримінального правосуддя, кіберзлочинності та електронних доказів, у тому числі між постачальниками послуг та правоохоронними органами [11].

За допомогою Європейського фонду миру ЄС підтримує ЗСУ у вдосконаленні навичок кіберзахисту. Внеском у 3 мільйони євро ЄС підтримав встановлення кіберлабораторії та кіберкласу. «Кіберлабораторія, клас, додаткове програмне та апаратне забезпечення безпеки та відповідні тренінги сформували комплексний підхід, який підвищив потенціал кіберзахисту України та зміцнив нашу співпрацю з Україною у сфері безпеки та оборони» – зазначає Пітер Вагнер, директор Європейської служби інструментів зовнішньої політики [23].

Протягом останніх двох років діяльність проєкту очолювала Академія електронного урядування. Кіберлабораторія та відповідні тренінги були проведені спільно з компанією "CybExer Technologies". Варто відмітити, що кіберлабораторія – це онлайн-середовище для навчання, вправ і досліджень. Технологія кіберлабораторії дозволяє користувачеві створювати реалістичне, потужне та надійне віртуальне середовище, яке вимагає від слухачів відповіді на симуляції кібератак і захисту в режимі реального часу. У змодельованій мережі військовослужбовці ЗСУ можуть краще навчитися справлятися з високим рівнем стресу, виявляючи та досліджуючи вразливі місця в різних мережевих системах.

Кіберклас містить 15 робочих станцій та необхідне обладнання для проведення тренінгів і навчань з питань кіберзахисту. У рамках проєкту також було закуплено, встановлено та налаштовано апаратне та програмне забезпечення безпеки для ЗСУ та проведено відповідні навчання [23].

Оскільки цифрова політика ЄС постійно розвивається, Україні необхідно враховувати дві речі. По-перше, імплементація цифрових і кіберрегуляторних актів ЄС є ціллю, яка постійно рухається, і вимагає послідовності та тісної координації з ЄС. По-друге, Україні потрібно розглянути не лише те, як реалізувати цифрову політику ЄС, а й як просувати власні найкращі практики на рівні ЄС і адаптувати файли ЄС до національного контексту [15, с. 482].

На внутрішньому рівні Україна має низку найкращих практик стійкості у кіберпросторі, використання технологій у війні та розвитку застосунку «Дія». Екосистема, покликана зробити Україну найзручнішою цифровою державою у світі. Крім того, опір України у війні на цифровому фронті сформував інтереси інших держав і провідних світових ЗМІ до її способу «довести справу» до цифрової та кіберполітики [19].

Виходячи з аналізу позитивного досвіду країн ЄС, для забезпечення інформаційної безпеки України необхідно:

1. Здійснювати активний технологічний розвиток та розвиток комп'ютерних та інформаційних систем.

2. Удосконалити нормативно-правове забезпечення інформаційної безпеки. Зокрема, чинний Закон України «Про основні засади забезпечення кібербезпеки України» не передбачає жодної діяльності з оцінки ризиків у сфері кібербезпеки [6]. Оцінка ризиків у сфері кібербезпеки України є не лише необхідністю сучасного етапу розвитку суспільства, але й вимогою формально-правового міжнародного законодавства, зокрема, європейського, подальша імплементація якого в Україні вимагає впровадження та забезпечення дотримання [31, с. 71]. Важливим елементом подальшого розвитку системи кібербезпеки України, особливо в умовах гібридної війни, є необхідність імплементації положень Директиви NIS від 6 липня 2016 р. про заходи щодо високого загального рівня безпеки мережевих та інформаційних систем в ЄС. Загалом, у тексті Директиви NIS термін «ризик» використовується 17 разів. У ст. 4 «Терміни та визначення» зазначено, що «ризик» означає будь-які обставини або події, які можна обґрунтовано ідентифікувати, що можуть негативно вплинути на безпеку мережевих та інформаційних систем. У ст. 14 та 16 зазначено, що держави-члени повинні забезпечити, щоб оператори базових послуг, а також постачальники цифрових послуг вживали відповідних та пропорційних технічних та організаційних заходів для управління ризиками безпеки мережевих та інформаційних систем, які вони використовують у своїй діяльності [31, с. 70]. У зв'язку з імплементацією європейського законодавства в Україні, нам необхідно імплементувати ці положення Директиви NIS до вітчизняного законодавства.

3. Залучати ЗВО та роботодавців до професійної підготовки фахівців з інформаційної безпеки, проводити навчання громадськості у формі курсів з інформаційної безпеки.

4. Вживати заходів щодо розвитку інформаційної культури та інформаційного суспільства, а саме розробити морально-правові механізми регулювання інформаційного суспільства в Україні на рівні державної стратегії. Реалізація національної стратегії розвитку інформаційного суспільства, метою якої є підвищення якості життя громадян, а також всебічний розвиток культурної та духовної сфер українців забезпечить повноцінне членство нашої держави в сучасній цифровій цивілізації [5, с. 27].

5. Рекламувати правила інформаційної гігієни, обачність і розбірливість при зверненні до інформації.

6. Виховувати у громадян України критичне мислення та вміння розпізнавати негативний інформаційний вплив, маніпуляцію, дезінформацію, фальсифікацію тощо [16, с. 39]. Ефективна система реагування на такі виклики повинна включати систему прогнозування, здатність швидко виявляти та спростовувати дезінформаційні повідомлення, стратегічні комунікації, тісну взаємодію між урядовими та громадянськими інституціями, а також розвиток медіаграмотності серед населення України. Стійкість українського народу до дезінформації та маніпуляцій має вирішальне значення для захисту державності та успішного розвитку країни під час воєнного стану та у повоєнний період. Для підвищення стійкості населення України до впливу дезінформації вкрай важливо впроваджувати міжсекторальну роботу з медіаграмотності в країні. Це вимагає посилення координації зусиль держави, громадянського суспільства, міжнародних організацій та медіа-спільноти [26].

Україна прийняла та продовжує застосовувати європейські та міжнародні стандарти у сфері кібербезпеки; вона створила та розвиває відповідні органи, які можуть ефективно взаємодіяти з відповідними органами ЄС. Водночас досвід України дозволяє їй бути не лише отримувачем допомоги від ЄС, а й джерелом нових знань, умінь та методів протидії сучасним кіберзагрозам [29].

Вдосконалення державної інформаційної політики України з урахуванням досвіду ЄС в умовах гібридної війни РФ полягає у створенні національної системи інформаційної безпеки України, яка передбачає:

1. Розробку та вдосконалення нормативно-правової бази інформаційної безпеки, яка нині фрагментована та повністю відповідає нагальним потребам.

2. Створення (визначення) у структурі органів державної виконавчої влади органу управління та координації системи інформаційної безпеки України.

3. Визначення (уточнення) переліку суб'єктів, відповідальних за стан інформаційної безпеки.

4. Дослідження та визначення вимог до технічних, фінансових і людських ресурсів для системи.

5. Активізацію діяльності в Міністерстві оборони та Генеральному штабі ЗСУ щодо створення власної системи захисту інформації у складі національної системи захисту інформації [22, с. 79].

Висновки та перспективи подальших пошуків у даному науковому напрямку. Таким чином, на тлі повномасштабного вторгнення РФ в Україну та початку Україною переговорів про вступ до ЄС обидві сторони погодилися посилити співпрацю у сфері кібербезпеки у зв'язку зі зростанням російських гібридних загроз. ЄС значно посилив свою кіберпідтримку України з початку неспровокованої та невиправданої агресивної війни РФ в лютому 2022 р. та має намір продовжувати підтримувати Україну для зміцнення її кіберстійкості, посилення взаємодії та підтримки запобігання, виявлення, стримування і реагування на кіберзагрози, зокрема щодо критичної інфраструктури та мереж.

Українські військові професіонали мають дуже високу мотивацію отримати нові цифрові навички та використовувати надане обладнання від ЄС для захисту українського кіберпростору. ЄС і Україна обрали шляхи, які дозволять Україні отримати вигоду від використання Резерву кібербезпеки ЄС, а також організувати додаткові тренінги для цивільних і військових організацій на основі потреб України Європейським коледжем безпеки та оборони, Консультативною місією ЄС і Військовою місією ЄС з підтримки України. У такий спосіб ЄС профінансував і поставив ЗСУ обладнання для кіберлабораторії, програмне забезпечення безпеки та апаратне забезпечення в рамках своєї поточної підтримки Україні в рамках Європейського фонду миру. Завдяки цій підтримці Україна може нарощувати та розвивати потенціал кіберзахисту своїх збройних сил для виявлення вторгнень в інформаційні системи, боротьби з кібератаками та зміцнення їхньої загальної спроможності у сфері кібербезпеки. Ця кіберлабораторія забезпечить навчальне середовище для перевірки та зміцнення практичних навичок військових професіоналів із кіберзахисту за допомогою реалістичних віртуальних сценаріїв і симуляцій у реальному часі, які допомагають швидше та ефективніше виявляти, контролювати та захищати від майбутніх кібератак.

Завдяки співпраці в рамках проєкту "EU4DigitalUA" Україні вдалося побудувати цифрову інфраструктуру, покращити кібербезпеку та швидко і якісно запустити ще зручніші електронні послуги для мільйонів українців. ЄС має продовжувати підтримувати Україну в її цифровій трансформації та зміцнювати її кіберстійкість під час війни, оскільки її кібербезпека також залежить від кібербезпеки в Україні та в регіоні.

Важливу роль у практичній площині співробітництва України та ЄС у сфері забезпечення інформаційної безпеки відіграє приватний сектор. Зокрема, нещодавно в Україні був створений осередок "Women4Cyber", що виступає некомерційною європейською приватною фундацією, метою якої є сприяння, заохочення та підтримка участі жінок у сфері кібербезпеки. Слід зазна-

чити, що деякі проєкти від ЄС (EU4DigitalUA та EGOV4UKRAINE) реалізовуються інвесторами з конкретних країн, зокрема Естонії (Академія електронного урядування) та Іспанії (Міжнародна Іберо-американська фундація з управління та публічної політики). Проєкти мають на меті підтримувати цифрову трансформацію України та впроваджувати європейські стандарти у сфері кібербезпеки останньої.

Перспективи подальших пошуків у даному науковому напрямку автор вбачає у дослідженні практичного аспекту зміцнення кіберстійкості ЄС та України, який полягає у здійсненні таких заходів: 1) створення спільних координаційних центрів з кібербезпеки; 2) посилення обміну інформацією про нові форми кіберзлочинності та кіберзлочинців, нові технології; 3) трансфер новітніх європейських технологій та розробок для України у сфері кібербезпеки; 4) посилення підготовки фахівців у сфері кіберзахисту; 5) прискорення уніфікації законодавства України з європейськими стандартами та вимогами; 6) збільшення фінансування ЄС на реформи кіберсфери України.

Література

1. Буга Л. В. Досвід США та Німеччини щодо забезпечення інформаційної безпеки в Збройних силах України. *Наукові записки Львівського університету бізнесу і права.* 2018. № 19. С. 174–178. URL: https://nzlubp.org.ua/index.php/journal/article/view/68

2. Верховна Рада України ухвалила Закон «Про ратифікацію Меморандуму про взаєморозуміння між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку». *Верховна Рада України: офіційний веб-сайт.* 2015. URL: https://www.rada.gov.ua/news/Novyny/110873.html

3. Голованова Н. Інформаційна політика України як європейської держави в умовах сучасних загроз (архетипний підхід). *Публічне урядування.* Вип. № 3 (18). 2019. С. 144–158.

4. Горєлова В. Ю., Вихрист С. М. Правове забезпечення та перспективи розвитку державної політики у сфері інформаційної безпеки. *Legal Bulletin*. 2024. Вип. № 13. С. 79–85.

5. Морозов А. Ю., Шуст Н. Б. Становлення інформаційного суспільства в Україні: виклики та перспективи. Освітній дискурс: збірник наукових праць. Вип. 41 (7-9). Київ, 2022. С. 26–37. URL: https://www.journal-discourse.com/en/catalog-of-articles/2022/2022-y-41-7-9/the-establishment-of-the-information-society-in-ukraine-challenges-and-prospects

6. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 2017 р. (із змінами внесеними згідно із Законом № 4336-IX від 20.04.2025 р.) *Верховна Рада України: офіційний вебсайт*. 2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. Хмель А. О., Біляєв Д. В. Місце безпекової сфери в італо-українських відносинах у 2011–2018 рр. *Наукові праці. Політологія.* Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2017. Т. 309. № 297. С. 71–77. URL: http://politics.chdu.edu.ua/article/view/200657

8. Шемчук В. В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Порівняльно-аналітичне право.* 2019. № 2. С. 34–40. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6820/1/%D0%A8%D0%B5%D0%BC%D1%87%D1%83%D0%BA.pdf

9. 3rd EU-Ukraine Cyber Dialogue takes place in Brussels. *National Security and Defense Council of Ukraine: official web-site*. 2024. URL: https://www.rnbo.gov.ua/en/Diialnist/6933.html

10. Christou G. Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy New Security Challenges. *Springer*, 2016. 176 p.

11. CyberEast. *Council of Europe: official web-site.* 2022. URL: https://www.coe.int/en/web/cybercrime/cybereast

12. Dudko I., Pashkovskyi V. Cooperation with EU as a mechanism of functional support of the system of information security of Ukraine. *KELM (Knowledge, Education, Law, Management)*. Lublin, 2022. № 2(46). P. 179–184.

13. EU helps Ukraine strengthen its cybersecurity. *EU NEIGHBOURS east: official web-site.* 2021. URL: https://euneighbourseast.eu/news/latest-news/eu-helps-ukraine-strengthen-its-cybersecurity/

14. EU, Ukraine strengthen cybersecurity ties amid escalating threats at third Cyber Dialogue. *Industrial Cyber*. 2024. 16 of July. URL: https://industrialcyber.co/events/eu-ukraine-strengthen-cybersecurity-ties-amid-escalating-threats-at-third-cyber-dialogue/

15. FedorenkoV., Lytvyn N., Luchenko D., Panova I., Tsybulnyk N. Legal aspects of information security management in the conditions of Ukraine's European integration. *Journal of Security and Sustainability.* 2020. Issues 10(2). Vol. 10 P. 477–489. URL: https://jssidoi.org/jssi/papers/papers/journal/41

16. Izmailov Ya, Yegorova I. Possibilities of adapting the EU experience in information security to the conditions of Ukraine. *Economics and Technical Engineering*. 2023. Vol.1. № 1. P. 35–43.

17. Kelemen R. The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations. *Connections: The Quarterly Journal 22.* 2023. № 2. P. 75–90. URL: https://connections-qj.org/article/impact-russian-ukrainian-hybrid-war-european-unions-cybersecurity-policies-and-regulations

18. Long-term EU support and strengthening Ukraine's role as a regional leader in the field of cybersecurity: The International Cyber Resilience Forum 2025 was held in Kyiv. *National Security and Defense Council of Ukraine: official web-site.* 2015. 21 of March. URL: https://www.rnbo.gov.ua/en/Diialnist/7142.html

19. Omelianenko V. EU's and Ukraine's approaches to digital diplomacy in the geopolitics of technologies. *The Foreign Policy Council "Ukrainian Prism"*. 2023. URL: https://prismua.org/en/englisheus-and-ukraines-approaches-to-digital-diplomacy-in-the-geopolitics-of-technologies

20. Pidbereznykh I., Koval O., Solomin Y., Kryvoshein V., & Plazova T. Ukrainian policy in the field

of information security. *Amazonia Investiga*. 2022. Вип. № 11(60). P. 206–213.

21. Rehrl J. Handbook on Cybersecurity: the Common Security and Defence Policy of the European Union. *Vienna: Federal Ministry Republic of Austria, Luxembourg Publications Office of the European Union*, 2018. 232 p.

22. Semenets-Orlova I., Klochko A., Amro T. Public management in the sphere of information security and democracy development in Ukraine in war time. *Public management*. № 5(33). 2022. P. 73–82. URL: https://journals.maup.com.ua/index.php/public-management/article/view/2562

23. The European Union strengthens Ukrainian cyber defence. *European Union: official web-site*. 2024. 20 of March. URL: https://www.eeas.europa.eu/delegations/ukraine/european-union-strengthens-ukrainian-cyber-defence_en?s=232

24. The European Union supports Ukraine's digital transformation: results of EU4DigitalUA's work. *European Union: official web-site*. 2024. URL: https://www.eeas.europa.eu/delegations/ukraine/european-union-supports-ukraines-digital-transformation-results-eu4digitaluas-work_en?s=232

25. The EU-Ukraine security partnership: status and prospects. *Razumkov center: official web-site.* Kyiv, 2021. URL: https://razumkov.org.ua/uploads/article/2021_eu_ukraine_security.pdf

26. The Strategy of the Ministry of culture and information policy of Ukraine for media literacy development until 2026. *Національний проєкт з медіа грамотності «Фільтр»*. 2024. URL: https://filter.mkip.gov.ua/wp-content/uploads/2024/06/strategyeng.pdf

27. Tzanou M. Personal Data Protection and Legal Developments in the European Union. *IGI Global*, 2020. P. 37–40.

28. Tsebenko O., Ivasechko O. EU-Ukraine cooperation in cybersecurity. *Conference: Sustainable development of the EU – best practices for Ukraine : Materials of the Internet conference (February 22, 2024)*. Lviv: Lviv Polytechnic National University, 2024. P. 34–38. URL: https://lpnu.ua/sites/default/files/2022/pages/18734/8-tsebenko-ivasechkoatezi-internet-konferencii-2024.pdf

29. Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere. *Centre for Global Studies "Strategy XXI"*. Kyiv, 2019. URL: http://www.encouncil.org/wp-content/uploads/2019/10/ENG-Ukraine-EU-NATO-cooperation-to-counter-hybrid-threats-in-cyber-sphere.pdf

30. Ukraine, EU move to deepen cybersecurity cooperation as Russian threat rises. *The Kyiv Independent: official web-site.* 2015. 14 of March. URL: https://kyivindependent.com/ukraine-eu-look-to-deepen-cybersecurity-cooperation-as-russian-threat-rises/

31. Veselova L. Improving Ukraine's administrative-legal support for cyber security: EU and NATO experience in countering hybrid cyber threats. *Public Administration and Law Review*. Issue 3. 2020. P. 67–73. URL: https://public.scnchub.com/palr/index.php/palr/article/view/45

32. Working Paper ECSO-Ukraine collaboration January 2024 ECSO and the Ministry of Digital Transformation of Ukraine. *European Cyber Security Organisation: official web-site.* 2024. URL: https://ecs-org.eu/ecso-uploads/2024/01/Collaboration-between-ECSO-and-Ukraine-Dec-2023.pdf

Анотація

Білоусов М. В. **Співробітництво України та ЄС у безпековому інформаційному просторі в умовах гібридної війни РФ: практична площина.** – Стаття.

У статті розглядається розвиток відносин України та ЄС у безпековому інформаційному просторі, що є основоположним фактором у підвищенні конкурентоспроможності нашої держави та зміцненні її технологічного потенціалу з урахуванням впливу російських гібридних загроз. Автор зазначає, що починаючи з 2014 р. Україна розвиває власну кібербезпеку у напрямках захисту комп'ютерних мереж і протидії кіберзлочинності, орієнтуючись на модель створену в ЄС. Основними документами, які регулюють цю сферу співробітництва є: 1) Меморандум про взаєморозуміння між Україною та Європейським поліцейським офісом щодо створення захищеної лінії зв'язку SIENA; 2) Меморандум про конфіденційність та забезпечення захисту інформації; 3) Угода з Агентством ЄС з кібербезпеки. Також Україна приводить у відповідність до європейських стандартів Стратегію кібербезпеки до 2021 р.. Європейська міжсекторальна організація ESCO виділяє 9 основних напрямів співпраці з українською стороною у сфері забезпечення інформаційної безпеки, шляхом залучення українських державних і приватних організацій на безоплатній основі.

Автор статті виділяє такі основні досягнення у сфері співробітництва України та ЄС у безпековому інформаційному просторі в умовах гібридної війни РФ: 1) створення осередку "Women4Cyber" в Україні; 2) отримання українськими малими та середніми підприємствами доступу до ринку "Cyber Solution Days"; 3) запровадження унікальної ефективної системи електронного урядування в Україні завдяки реалізації проєкту "EU4DigitalUA"; 4) триває постійна робота над проєктом створення спеціальних кібервійськових підрозділів у складі Збройних сил України; 5) щорічна організація навчання з кібербезпеки для представників українських державних органів; 6) проєкт "EU4DigitalUA" зосереджений на подальшому розвитку цифрової урядової інфраструктури, публічних електронних послуг та захисту даних українців.

Автор приходить до висновку, що досить важливим є удосконалення нормативно-правового забезпечення інформаційної безпеки України з урахуванням чинного європейського законодавства, а саме адаптація законодавчої бази України до Директиви NIS (2016 р.).

Ключові слова: Україна, Російська Федерація, Європейський Союз, гібридна війна, інформаційна безпека, кібербезпека.

Summary

Bilousov M. V. **The cooperation between Ukraine and the EU in the information security sphere in the context of the Russian Federation's hybrid war: practical aspects.** – Article.

The article examines the development of relations between Ukraine and the EU in the information security sphere, which is a fundamental factor in increasing the competitiveness of our state and strengthening its technological potential, taking into account the influence of Russian hybrid threats. The author notes that, since 2014, Ukraine has been developing its own cybersecurity in the areas of protecting computer networks and combating cybercrime, focusing on the model created in the EU. The main documents regulating this area of cooperation are: 1) Memorandum of Understanding between Ukraine and the European Police Office on the establishment of a secure communication line SIENA; 2) Memorandum on confidentiality and ensuring information security; 3) Agreement with the EU Agency for Cybersecurity. Ukraine is also bringing its Cybersecurity Strategy until 2021 into line with European standards. The European intersectoral organization ESCO identifies 9 main areas of cooperation with the Ukrainian side in the field of ensuring information security by involving Ukrainian public and private organizations on a free basis.

The author of the article highlights the following key achievements in the field of cooperation between Ukraine and the EU in the information security sphere in the context of the Russian hybrid war: 1) the creation of the "Women4Cyber" cell in Ukraine; 2) Ukrainian small and medium enterprises gaining access to the Cyber Solution Days market; 3) the implementation of a unique effective e-government system in Ukraine thanks to the implementation of the "EU4DigitalUA" project; 4) ongoing work on the project to create special cyber military units within the Armed Forces of Ukraine; 5) annual organization of cybersecurity training for representatives of Ukrainian government agencies; 6) the "EU4DigitalUA" project focuses on the further development of digital government infrastructure, public e-services and data protection of Ukrainians.

The author comes to the conclusion that it's quite important to improve the regulatory framework for information security in Ukraine taking into account the current European legislation, namely, the adaptation of the legislative framework of Ukraine to the NIS Directive (2016).

Key words: Ukraine, Russian Federation, European Union, hybrid warfare, information security, cybersecurity.