УДК 351.862.8:001.102-029:327(477)

https://doi.org/10.52058/3041-1793-2025-7(12)-724-738

Дмитренко Степан Петрович кандидат політичних наук, доцент кафедри історії міжнародних відносин та гуманітарних дисциплін УДУ імені Михайла Драгоманова, м. Київ, тел. (093) 0417736, https://orcid.org/0009-0005-4163-0468

Дмитренко Оксана Сергіївна кандидат політичних наук, доцент кафедри історії міжнародних відносин та гуманітарних дисциплін УДУ імені Михайла Драгоманова, м. Київ, тел. (093) 2776280, https://orcid.org/0009-0000-7621-2710

ОСОБЛИВОСТІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

Анотація. Україна, яка перебуває в епіцентрі інформаційної та кібербезпекової війни, стикається з найсерйознішими викликами сучасної світової системи, які полягають у транскордонному характері взаємодії, а також вимагають безпекову взаємодію між державами. Війна в Україні посилила безпрецедентну інформаційну та кіберагресію, яка вивела її з категорії допоміжного елемента управління у державі та поставила на рівень ключового гравця, який формує глобальну стратегію кіберзахисту. Автори виокремлюють тези щодо особливостей міждержавного співробітництва в контексті інформаційної безпеки, а також роблять спробу визначити перспективи зміцнення національної стійкості України в умовах війни з урахуванням кібербезпекового та інформаційного просторів.

Розвідка представлена з метою аналізу актуального стану та ідентифікації векторні особливостей міжнародного співробітництва України в сфері інформаційної безпеки, акцентуючи на перспективах, які в подальшому зміцнять національну стійкість держави проти загроз у сфері інформаційної та кібербезпеки.

У розвідці проаналізовано актуальний стан та ідентифіковано векторні особливості міжнародного співробітництва України в сфері інформаційної безпеки, закцентовано на перспективах, які в подальшому зміцнять національну стійкість держави проти загроз у сфері інформаційної та кібербезпеки, які постійної еволюціонують. Дослідження синтезує різні рівні академічних знань та поєднує їх з практичними прикладами задля отримання бекграунду для аналізу актуальних засобів масової інформації та публікації у них. Розвідка формує комплексні рекомендації, які в подальшому можуть бути

використані як практичні поради для посилення співпраці держав у сфері інформаційної та кібербезпеки. У висновках надано рекомендації, як розвивати людський капітал, гармонізувати законодавство та зміцнити державно-приватне партнерство, використавши український досвід у війні з метою посилення світової, глобальної, кіберстійкості.

Ключові слова: Україна, міжнародне співробітництво, ЄС, кібер-безпека, інформаційна безпека, гібридні загрози.

Dmytrenko Stepan Petrovych Candidate of Political Sciences, Associate Professor of the Department of History of International Relations and Humanitarian Disciplines, Mykhailo Drahomanov UDU, Kyiv, tel. (093) 0417736, https://orcid.org/0009-0005-4163-0468

Dmytrenko Oksana Serhiivna Candidate of Political Sciences, Associate Professor of the Department of History of International Relations and Humanitarian Disciplines, Mykhailo Drahomanov UDU, Kyiv, tel. (093)2776280, https://orcid.org/0009-0000-7621-2710

FEATURES OF INTERNATIONAL COOPERATION IN THE FIELD OF INFORMATION SECURITY: PROSPECTS FOR UKRAINE

Abstract. Ukraine, being at the epicenter of the information and cybersecurity war, faces the most serious challenges of the modern global system. These challenges stem from the transboundary nature of interactions and necessitate security cooperation between states. The war in Ukraine has intensified an unprecedented wave of information and cyber aggression, which has shifted these domains from being auxiliary components of state governance to key players shaping the global cybersecurity strategy.

The authors highlight key theses concerning the specifics of intergovernmental cooperation in the context of information security and attempt to outline prospects for strengthening Ukraine's national resilience in wartime, taking into account the dimensions of the cyber and information environments.

This research aims to analyze the current state and identify the directional features of Ukraine's international cooperation in the field of information security, with a focus on the future prospects for enhancing the country's national resilience in the face of ongoing and evolving threats in the spheres of information and cybersecurity.

The study provides a detailed analysis of the current state of affairs and identifies key trends in Ukraine's international information security cooperation. It emphasizes perspectives that can contribute to strengthening state resilience against rapidly evolving threats in the information and cyber domains. The research synthesizes various levels of academic knowledge and combines them with practical

examples to provide a comprehensive background for analyzing current media and relevant publications.

The paper formulates a set of complex recommendations that may serve as practical guidelines for enhancing interstate cooperation in the field of information and cybersecurity. The conclusions offer proposals for the development of human capital, harmonization of legislation, and strengthening of public-private partnerships, using Ukraine's wartime experience as a foundation for enhancing global cyber resilience.

Keywords: Ukraine, international cooperation, EU, cybersecurity, information security, hybrid threats.

Постановка проблеми. Світопорядок актуального часу має дві стратегічні проблеми, а саме інформаційну та кібербезпекову загрози. У цих двох сферах світ стикається із серйозними викликами, які можуть зруйнувати цей світопорядок. Міжнаціональний і транскордонний вектор цих загроз спонукає держави об'єднуватися через системні атаки, які не знають географічних кордонів і підривають державний суверенітет; піддають знеціненню демократичні процеси і стирають стабільність у державах. Військова агресія росії проти України є не тільки агресією фізичною на точках зіткнення фронту, але й агресією цифровою, оскільки українці перебувають під неперервним інформаційним тиском та кіберагресією з боку держави-тирана. Ця агресія має ознакування широкого охоплення, відтак до найважливіших ідентифікаційних ознак зараховуємо такі:

1. Різні засоби, які вчиняють деструктивні дії у інформаційному просторі;
2. Інформаційно-психологічні операції, які породжують гібридну загрозу;
3. Зміну спеціального правового режиму.

Відтак для України є важливою необхідність уводити спеціальний режим правового стану інфобезпеки, який буде покликаний усувати гібридні загрози та розширювати перелік способів боротьби з ними в контексті збереження національної безпеки.

На цій підставі ми говоримо також, що розмиванням суверенітету і географічних кордонів, перетворенням інформації на ресурс, який стає непідконтрольний у власній державі, займається інформаційна війна.

Інформаційна війна - це сучасне глобалізаційне явище, яке не обмежується лише військовим конфліктом у розумінні нинішньої безпекової ситуації, зокрема нашій державі, а і також дестабілізує суспільство, підриваючи критичну інфраструктуру і дискредитує всі державні інституції.

Констатуємо те, що в Україні відсутнє ґрунтовне законодавче забезпечення єдиного підходу до збереження рівнів кібербезпеки, а також досі відсутній універсальний центр координації, який значно підвищував би захист і зупиняв руйнування національних інформаційних систем.

У такий спосіб розуміємо, що міжнародні партнерства обов'язкові для розбудови рівнів протидії таким комплексним загрозам і є важливими для збереження національної безпеки і стабільності держави, яка перебуває у війні, а також пониженні рівня впливів держави-агресора не тільки на Україну, а й на інших міжнародних партнерів.

Актуальність. Актуальним, значущим та своєчасним у контексті українського військового досвіду є дослідження міжнародного співробітництва саме у сфері інформаційної та кібербезпеки. Безпекова політика Європейського Союзу є наріжною для української держави оскільки в контексті євроінтеграції саме вона визначається ключовим напрямком.

Кібербезпека та інформаційна безпека - це невід'ємні частини української державної безпеки, які спрямовані, щоб захистити важливі життєві інтереси людини зокрема, суспільства загалом та уберегти Українську державу від інформаційних впливів, які мають характер деструктивних.

Для європейської спільноти повномасштабна війна в Україні, кіберагресія і унікальний досвід боротьби з нею є поштовхом для посилення узаємодії.

Передова гібридної війни торкнулася саме України і українська держава стає точкою тестування глобальної стратегії інформаційної та кібербезпеки в реальному часі. В обмежених ресурсах Україна стала не просто реципієнтом допомоги у розумінні міжнародної безпекової рамки, але й отримала унікальні знання, будучи учасником кібервійни, які в подальшому можуть бути трансформовані, наприклад, у методологічній або тренувальні програми і використані для навчання фахівців з кібербезпеки на міжнародному рівні.

Непомірно швидкий розвиток технологій, у тому числі і штучного інтелекту, ускладнює і без того складну специфіку кіберзагрози і загального її розуміння. Саме це вимагає від міжнародних партнерів і держав постійно зосереджуватися на модернізації рівня кібербезпеки і інформаційної безпеки.

Загальна динаміка підтверджує, що необхідно ефективно співпрацювати на міжнародному рівні, оскільки жодна держава не може власним ресурсом впоратися з множинним викликом, який може здатен посати перед нею в будь-який момент розвитку.

Україна в цьому контексті є безцінною як держава, що вже отримала певний рівень загрози і певний рівень успішно ліквідувала.

У такий спосіб дослідження міжнародного співробітництва у фокусі інформаційної безпеки та кібербезпеки, де ключовим елементом розвідки буде саме Україна, сприятиме не тільки посиленню партнерств, а й випрацюванню механізмів єдиного підходу до збереження національної безпеки та зміцнення глобальної кіберстійкості держав.

Аналіз актуальних досліджень та публікацій. Концепт «міжнародне співробітництво у сфері інфобезпеки» є складним, багатокомпонентним та варіативним явищем, якщо йдеться про його наукове обґрунтування. Ця

складність посилилася умовами війни, у яких із 2014 року перебуває Україна. На цій підставі також паралельно посилилися й теоретико-практичні аспекти й виклики у наукових доробках учених. Розглянемо деякі з них.

Розмиванням державного суверенітету, на переконання науковиць Жаровської І. та Ортинської Н. [2, с.58-60], активно опікується інформаційна війна, яка, за своїм глобалізаційним ознакуванням, має впливи на стирання географічних кордонів. Через це відбувається неконтрольованість процесів розвитку інформаційних ресурсів, наслідком чого є маніпулювання свідомістю громадян, а, отже, не просто порушенням справедливих процесів розвитку, а й негативним системним упливом на громадян.

У працях Кононенка В. та ін. [4, с.246] інфобезпека отримує характеристику стану захищеності від неконтрольованих інфовпливів на свідомості та розглянута як концепт у складі міжнародної та національної безпеки. ООН, НАТО та ЄС повинні перебирати на себе ролі гарантів протидії новітнім інфозагрозам у державах та допомагати у формуванні суверенітету і збереженні свідомості громадян.

Проблематику реалізації міжнародного співробітництва у контексті забезпечення інформаційного спокою та аспектуалізаційні принципи ролі України на цьому зрізі порушує у своїх працях Суслін С. [5, с.66-79]. Воєнний стан та активі бойові дії передбачають активізацію потреби розроблювати та впроваджувати заходи, які покликані захищати інформацію та критичну інфраструктуру (у тому числі, цифрову). Авторка пропонує шукати спільні рішення та посилювати співробітництво з державами-партнерами задля окреслення таких правових меж стратегій захисту, щоб вони були фундаментальними на нормативному рівні та актуальними для реалізації на практичному.

Худолій А. [6, с.139-141] науковою проблематикою своєї діяльності вбачає глибокий аналіз кібербезпекових викликів, що постали перед нашою державою на підставі інфозагроз, які окреслила й спровокувала росія. Автор підкреслює, що в українській науковій думці наразі відсутнє обґрунтоване нормативне врегулювання та єдиний координаційним центр протидії кібератакам. Громадяни мають слабку підготовку до виявлення й відбиття кібератак, а, отже, потребує впровадження адаптованого міжнародного досвіду.

Гібридні загрози досліджують у своїх працях Величко Л. та ін. [1, с.443-453], підкреслюючи, що важливо опрацьовувати різні форми впливу (багатовекторні, комплексні, адаптивні) на рівень дестабілізації держави. До них зараховано економічні, інформаційні, військові способи дестабілізації. Окремо охоплено аналітикою транспортну інфраструктуру, адже вона перебуває у зрізі топ-об'єктів, які можуть бути піддані кібератакам.

У ЄС розроблені стратегічні підходи до ідентифікацій гібридних загроз, на підставі яких апробовані заходи протидії. Карамишев Д. та ін. [3, с.57-61] у своїх розвідках спираються саме на них, опрацьовуючи питання реалізації

державного управління у сфері нацбезпеки. Автор вказують, що навіть попри військову агресію, потрібно впроваджувати вектори розробки комплексного документа, який зафіксує тези покрокового усунення, раннього виявлення та протидії інфозагрозам.

Чепелюк Ю. [7, с. 255] розглядає цифрову дипломатію як активний інструмент сучасної інформаційної комунікації. Цифрова дипломатія може і здатна виконувати роль антагоніста дезінформаційним виявам, роз'яснювати й поширювати розуміння інструментів міжнародної співпраці у сфері протидії загрозам.

Опрацьовані наукові джерела свідчать, що в українські науковій думці є системний підхід до опрацювання вказаної проблематики. Науковці визначають наскрізні тези, які потребують додаткового нормативного врегулювання, та ,у результаті його запровадження, - подальшої реалізації практичних вимог протидії загрозам.

Навіть зважаючи на те, що існує значна кількість опрацьованої проблематики науковцями, досі залишається відкритим і нерозробленим питання особливостей установлення правильного вектору міжнародного співробітництва і його перспектив для нашої держави з урахуванням того, що ми перебуваємо у фазі активної війни.

Мета. Наша наукова розвідка покликана проаналізувати актуальний стан та ідентифікувати векторні особливості міжнародного співробітництва України в сфері інформаційної безпеки, акцентуючи на перспективах, які в подальшому зміцнять національну стійкість держави проти загроз у сфері інформаційної та кібербезпеки, які постійної еволюціонують.

У дослідженні ми прагнемо синтезувати різні рівні академічних знань та поєднати їх з практичними прикладами задля отримання бекграунду для аналізу актуальних засобів масової інформації та публікації у них, щоби сформувати комплексні рекомендації, які в подальшому можуть бути використані як практичні поради для посилення співпраці держав у сфері інформаційної та кібербезпеки.

Опрацюванню такої комплексної мети сприятимуть якісно виконані наукові **завдання:**

1. Аналітика поточних ініціатив та механізмів у сфері міжнародного співробітництва та інформаційної безпеки, де активну участь бере Україна (тут ми опрацюємо доступ рівні доступу України до нормативних документів ЄС та можливі варіанти співпраці із Держспецзв'язку Сполучених Штатів Америки);
2. Визначення ключових безпекових елементів, що можуть бути об'єктом міжнародної співпраці, які виокремимо на основі аналізу публікації в засобах масової інформації, що дозволить ідентифікувати конкретні кібербезпекові аспекти, які медіа розглядають як варіанти захисту критичної інфраструктури, розбудови потенціалу і протидії дезінформації;

3. Дослідження рекомендацій, які надані у відкритих засобах масової інформації, що допоможе зрозуміти, як можна налагодити та поглибити співпрацю в інформаційній сфері та передбачити варіанти систематизації дій і порад, що запропоновані у цих медіа і можуть бути покладені в основу налаштування співпраці;

4. Оцінка поточного етапу існуючої міжнародної співпраці нашої держави у сфері кібер- та інформаційної безпеки, що допоможе нам зрозуміти рівень зрілості співпраці та поставити його на один із трьох етапів – початковий рівень (домовленості); активну реалізацію або стратегічне партнерство;

5. Надання практичних рекомендацій для українського законодавчого і політичного простору з метою подальшого розвитку співробітництва у сфері кібербезпеки та інформаційної безпеки.

Отже, визначені завдання дозволять нам забезпечити послідовний аналіз від описового елементу актуальної ситуації аж до рівня оцінки ефективності нинішньої співпраці та формування практичних порад.

Виклад основного матеріалу дослідження. Розуміння важливості співпраці у сфері інформаційної безпеки для держав повинні продукувати стабільність сучасного інформаційного світу, на який впливає транскордонний характер загроз.

Таке співробітництво повинно бути:

1. Законодавчо опрацьоване;
2. Спрямоване на об'єднання зусиль;
3. Містити рівні активної взаємодії між державами;
4. Нести прозорість та відповідальність у вирішенні спільних проблем;
5. Продукувати інноваційність та впровадження нових елементів забезпечення загального стану інфопростору;
6. Мати ефективні рівні співпраці у межах міжнародних організацій;
7. Опрацьовувати потенційні загрози та виокремлювати сценарії для подолання загроз у майбутньому.

Ключовий і надважливий аспект міжнародного співробітництва повинен базуватися на активній розробці нормативно-правових актів, базовим завданням яких є регуляція інформаційних відносин між державами в частині двосторонніх і багатосторонніх структур, а також розвиток власних стратегій забезпечення рівнів захисту у кожній державі окремо.

У 2021 році в Україні затверджено Стратегію кібербезпеки, яка визначила співпрацю і обов'язковий розвиток стратегічних відносин з ключовими міжнародними партнерами - Сполученими Штатами Америки, державами НАТО, ЄС.

Із урахуванням національних інтересів України в цьому розумінні необхідно зазначити, що саме національний інтерес має стати ключовим

об'єднувальним та координативним елементом в процесі напрацювань у цій сфері.

Перейдемо до аналізу публікацій у засобах масової інформації, п'яти, на наше переконання, ключових статей, які дозволять оцінити рівень практичної реалізації аспектів українського співробітництва з міжнародними донорами та виявити безпекові елементи, що в подальшому дозволять надати рекомендації з метою налагодження співпраці.

Публікація 1. ***Держспецзв'язку України співпрацюватиме зі службою кібербезпеки Держдепу, готують угоду (Algorytm-X, 2021) [12]***

У статті автори відображають фундаментальний характер двосторонньої співпраці США та України.

Базові безпекові елементи, які досліджуються: протидія російській агресії, організації взаємодії з приватним сектором, побудова галузевих операційних центрів безпеки і команд реагування, формування кадрового потенціалу.

Рекомендації, які можна залучити, щоб налагодити співпрацю: обмін досвідом щодо протидії російській агресії, розробка спільного протоколу дій, досвід США із взаємодії з приватним сектором, реалізація проектів МТД, проведення навчальних курсів.

Етап налагодженої співпраці: початковий, формалізований та планувальний; угода про встановлення лінії захищеної зв'язку станом на станом на 2021 є базовою для подальшої взаємодії держав.

Публікація 2. ***Україна офіційно приєдналася до Центру НАТО з кіберзахисту (Суспільне, 16.05.2023) [9]***

У другій публікації опрацьовано тезу важливого розвитку інтеграції України до структур кібербезпеки євроатлантичного простору.

Досліджено такі безпекові елементи: приєднання України до центру НАТО з питань співробітництва у галузі кіберзахисту, приклади кібератак на урядові сайти, російська агресія.

Рекомендації, які можна залучити, щоб налагодити співпрацю: поглиблення інтеграції до кіберзахисних структур НАТО; обмін інформацією та досвідом; зміцнення кіберзахисту як відповідь на неперервні російські загрози.

Етап налагодженої співпраці: офіційна інтеграція і поточна взаємодія; інституціоналізована співпраця та спільні оборонні можливості вже реалізовані.

Публікація 3. ***USAID виділяє грант $500 000 на впровадження інноваційних проектів у сфері кібербезпеки (Чернівецька ОВА, 02.10.2023) [11]***

У наступній статті автори демонструють, якою важливою є фінансова підтримка для посилення кібербезпеки.

У статті досліджено такі **безпекові елементи**: стан захисту критичної інфраструктури, необхідність ухвалення інноваційних рішень, протидія

щоденним атакам на органи влади комерційний сектор та урядовій неурядові організації.

Рекомендації, щоб налагодити співпрацю: залучати стартапи, компанії та розробників, щоб створювати креативні рішення у сфері; налагоджувати співпрацю задля отримання грантових програм, що дадуть змогу реалізувати власні рішення і захистити критичну інфраструктуру; сприяти державно-приватному партнерству.

Етап налагодження співпраці кваліфікується як активне фінансування та стимулювання інновацій; запуск грантової програми є конкретним кроком, який опрацьовує кіберзахисні рішення.

Публікація 4. ***Голова Держспецзв'язку на конференції TechNet: Унікальний досвід України у кібервійні стає основою для тренувань світового рівня (Держспецзв'язку, 10.06.2025) [8]***

У цій статті підкреслено трансформаційну роль України у частині глобалізації кібербезпеки, де Україна переходить від реципієнта допомоги до елемента унікального досвіду, із яким стикнулася в контексті повномасштабного вторгнення.

Автори досліджують **такі безпекові елементи:** протистояння кіберагресії; розробка тренувальних програм; захист об'єктів критичної інфраструктури; розвиток національної кіберстійкості; протидія хакерським угрупованням; Gamaredon та Sandworm.

Автори **рекомендують налагоджувати співпрацю в такий спосіб:** перетворити здобуті знання на ефективні тренувальні програми, які будуть стосуватися кіберзахисту і стануть важливим напрацюванням для українських та міжнародних фахівців; окреслити важливість міжнародної співпраці та партнерства із CYBER RANGES; залучити елементи приватного сектору, об посилити національну кіберстійкість; розробити автоматизовані системи тестування NIST 800-181.

Етапи налагодження співпраці у публікації окреслено в такий спосіб: етап активного розвитку та розширення стратегічних партнерств; у 2023 році підписано меморандум про співпрацю з CYBER RANGES, навчання на платформі TRYZUB доступне для українських військовослужбовців та публічних службовців, що свідчить про активний внесок власного досвіду в глобальний механізм розвитку кібербезпеки.

Публікація 5. ***Україна отримає доступ до Резерву кібербезпеки ЄС (Укрінформ, 03.07.2025) [10]***

У цій статті автори висвітлюють значний крок у співпраці з Європейським союзом в частині інформаційної та кібербезпеки. Стаття досліджує безпекові елементи, зосереджуючися на Резерві кібербезпеки Європейського Союзу, який є базовою ініціативою в межах нормативно-правового регулювання.

Атори акцентують увагу, що необхідно розробляти мережі сертифікованих експертів Європейського Союзу у сфері кіберзахисту та зберігати рівні захисту державних інформаційних систем, електромереж і сайтів.

Рекомендації, які надають автори, щоб Україна посилила кіберстійкість: необхідно використовувати підтримку мережі сертифікованих експертів Європейського Союзу, які можуть втручатися до національної безпекової частини і зупиняти атаки, захищати інформацію та відновлювати роботу системи.

Етап налагодження співпраці, який описаний у цій статті: просунутий у двох аспектах – формалізації та реалізації. Віце-прем'єр-міністр з розвитку інновацій, науки та освіти-Міністр цифрової трансформації України Михайло Федоров підписав зміни до угоди про участь України в програмі ЄС «Цифрова Європа», що дозволить Україні отримати доступ до Резерву кібербезпеки - це дієвий крок до подальшої операційної підтримки ЄС.

Отже, доходимо висновку, що медіапублікації демонструють чітку еволюцію міжнародного співробітництва держав з Україною. На початковій фазі це була реактивна підтримка з розбудовою потенціалу у 2021 році, потім співпраця стала етапом стратегічної інтеграції до великих міжнародних рамок, які підтверджували офіційне приєднання України до Центру НАТО із питань співробітництва галузі кіберзахисту у 2023 році. Фінальним і актуальним на сьогодні є доступ до Резерву кібербезпеки Європейського Союзу.

Окреслимо також, які існують ключові міжнародні ініціативи та партнерства України у сфері кібербезпеки.

1. Партнерство з Європейським Союзом з основним фокусом на євроінтеграцію, цифрову безпеку та кіберсолідарність через доступ до Резерву кібербезпеки ЄС, гармонізацію законодавства та підтримку мультиуправління моделі інтернет. В активному статусі інтеграції та підписанні угоди;
2. Ініціатива з НАТО з основним фокусом на колективну кібероборону та підвищення кіберстійкості на рівні ключового аспекту приєднання до центру НАТО з питань співробітництва в галузі кіберзахисту та спільних навчань у статусі офіційної інтеграції та постійної співпраці, а також обміну розвідувальними даними;
3. Співпраця зі Сполученими Штатами Америки з основним фокусом на двосторонню взаємодію, формування кадрового потенціалу, технічну допомогу у ключових аспектах роботи з Держспецзв'язку та грантовими програмами, у статусі стратегічного партнерства, фінансової підтримки та реалізації конкретних проектів;
4. Співпраця у ініціативі Таллінського механізму з основним фокусом на координацію допомоги для зміцнення кіберстійкості; з ключовими аспектами міжнародної ініціативи та координації допомоги Україні у сфері кіберстійкості; у статусі активного механізму та залучення фінансової допомоги;

5. Ініціатива з ООН та ОБСЄ з основним фокусом на міжнародно-правовій базі, протидії незаконному використанню інформаційно-комунікаційних технологій та зміцнення довіри, з ключовим аспектом участі у програмі дій для заохочення відповідальної поведінки держав та імплементації рекомендацій ОБСЄ і статусом постійної участі у діалозі на міжнародному рівні та формуванні відповідальної поведінки;

6. Ініціатива взаємодії з приватним сектором та it- компаніями з основним фокусом на обмін досвідом, технології та інновації в ключових аспектах співпраці з партнерством Cyber ranges та провідними it-компаніями, провайдерами, соціальними мережами для протидії гібридним загрозам на статусі зростаючого значення розвитку державно-приватних підприємств та залучення можливих інвестицій.

Отже, тенденція, за якої Україна може стати джерелом унікальної військової та кібербезпекової експертизи, нині актуальна, оскільки Україна є також елементом впровадження інноваційних рішень.

Досвід України у кібервійні може стати основою для впровадження методологічних рекомендацій світового рівня, а також виділенням подальших грантів на впровадження оновлених або ж інноваційних проектів у сфері інфобезпеки та кібербезпеки. Це означає, що партнери розуміють взаємну вигоду і спільне навчання задля забезпечення світового порядку. Ставлення до кібербезпеки на універсальному зрізі розуміння повинне ґрунтуватися на тому, що глобалізація інформаційної загрози може торкнутися кожної держави.

Пропоновані аналітики дозволяють зрозуміти, що міжнародні ініціативи та партнерства у сфері кібербезпеки для України наразі мають комплексний підхід. Співпраця повинна охоплювати широкий спектр напрямків, у тому числі колективну оборону, двосторонню технічну допомогу, євроатлантичну інтеграцію, координування фінансових ресурсів, залучення до роботи приватного сектору.

Кожна названа ініціатива повинна відображати основний фокус співпраці та ключові аспекти, що буде свідчити про багатовекторність підходів до зміцнення кіберстійкості України в умовах війни.

Статус або етап співпраці може варіюватися відповідним міжнародним діалогом, який буде підкреслювати або понижувати динаміку розвитку таких партнерств. Проаналізована інформація може стати основою, щоби сформулювати подальші рекомендації, оскільки вона відображає рівень досягнення успіхів і точки, де необхідно докласти додаткові зусилля.

Висновки та перспективи подальших розвідок. Отже, проаналізувавши дослідження та публікації в засобах масової інформації, ми вкотре підтвердили, що Україна, перебуваючи в умовах гібридної агресії з боку росії, продовжує активно інтегруватися в міжнародні системи забезпечення інформаційної безпеки.

Практично підтверджено, що ця взаємодія є двосторонньою: Україна вже може поділитися унікальним досвідом введення кібервійни і не лише отримувати допомогу, а й у межах власного практичого досвіду стати основою для глобальних методологічних тренувальних програм та бути учасником формування оновлених підходів до кіберзахисту.

Щоб налагодити якісну, дієву взаємодію, необхідно опиратися на такі ключові досягнення:

1. Інституціоналізація міжнародного партнерства;
2. Розбудова потенціалу;
3. Стимулювання інновацій в частині партнерства.

Україна вже досягла статусу офіційного приєднання до Центру НАТО з питань співробітництва та отримала доступ до Резерву кібербезпеки ЄС в розбудові потенціалу, зокрема отримала досвід співпраці зі Штатами та можливість розробляти спільні протоколи дій, створення операційних центрів безпеки та команд реагування в частині стимулювання інновацій; отримала значну кількість грантових програм для державно-приватного партнерства, які заохочують розробляти та впроваджувати рішення у сфері кіберзахисту та протидії дезінформації, що допомагають протидіяти загрозам, які еволюціонують.

Проте попри значні успіхи, залишається певний перелік викликів, які стосуються, зокрема, сфери адаптації нормативно-правового зрізу та координації зусиль.

На цій підставі Україні і кожній державі, яка перебуває в інформаційній війні або розуміє, що інформаційна війна відбудеться дуже скоро, необхідно:

1. Гармонізувати законодавство і стандарти. Україні в цьому контексті необхідно продовжувати адаптацію нормативно-правових актів до стандартів ЄС та НАТО, у тому числі щодо захисту критичної інфраструктури, протидії кіберзагрозам та управління даними;
2. Зміцнювати інституційну спроможність в контексті розбудови національних структур, кібербезпеки та посилювати міжвідомчу взаємодію;
3. Розвивати людський капітал та інтенсифікувати методологічні програми підготовки, перепідготовки і підвищення кваліфікації фахівців з кібербезпеки, обмінюватися експертами з міжнародними партнерами;
4. Поглиблювати державно-приватне партнерство та сприяти тіснішій співпраці держави та приватного сектору, щоб залучати інноваційні рішення та інвестиції через грантові міжнародні програми тощо;
5. Ефективно протидіяти дезінформації та гібридним загрозам і розробити ефективні стратегії протидії гібридній війні, у тому числі із застосуванням інструментів цифрової дипломатії та налагодження співпраці з провідними соціальними мережами та доступ до переліку провайдерів цифрових послуг, щоб мати можливість боротися з дезінформацією та наративами, які впливають на суспільну свідомість;

6. Використовувати унікальний досвід України, активно його просуваючи для міжнародних тренувальних програм та розробки методології навчань. Необхідно брати практичний досвід України як основу для них і в цьому розумінні Україна буде переходити зі статусу не тільки реципієнта міжнародної допомоги, а й провайдера навчальної та практичної експертизи, що зможе посилити позиції держави на міжнародній аремі та сприяти розробці практичних політик і взаємодій.

Важливість подальших наукових розвідок вбачаємо у динамічному та швидкозмінному характері загроз кібербезпекової та інформаційної сфер і розуміємо, що актуальний військовий збройний конфлікт в Україні є реальним прикладом вивчення запитів інформаційної війни, відтак необхідно проводити неперервні дослідження, щоб формувати адаптивну політику та напрацьовувати стратегічні відсічі у цій війні.

Залучення штучного інтелекту може допомогти зробити кіберстійкість критично важливою, однак це вимагатиме постійної модернізації і підготовки до нових сценаріїв загроз.

Подальше дослідження вбачаємо в глибинному аналізі вразливостей штучного інтелекту та пропонуватимемо розробку методики їх усунення. Критично важливим також вбачаємо вивчення питань міжнародного співробітництва із залучення експертів до установлення практичного рівня кібербезпеки у державі, яка перебуває у війні, що може дозволити означити ефективність та неефективність практичних механізмів і допомогти розбудувати національну кіберстійкість.

Література:

1. Величко, Л. Ю., & Білоконь, М. В. (2024). Гібридні загрози транспортній інфраструктурі: виклики для державного регулювання та національної безпеки. *Теорія та практика державного управління*, *2*(79), 442–464. https://doi.org/10.26565/1727-6667-2024-2-23

2. Жаровська, І., & Ортинська, Н. (2020). Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки", 7*(2), 56-61. https://doi.org/10.23939/law2020.26.056

3. Карамишев, Д. В., Соболь, Р. Г., Мирна, Н. В., & Євдокимов, В. О. (2023). Державне управління у сфері національної безпеки і оборони. *State Formation, 2*(34), 54–66. https://doi.org/10.26565/1992-2337-2023-2-05

4. Кононенко, В. П., Здоровко, С. С., & Корольова, А. Є. (2023). Інформаційна безпека як стан. *Uzhhorod National University Herald Series Law, 2*(76), 244-250. https://doi.org/10.24144/2307-3322.2022.76.2.39

5. Суслін, С. (2025). Правові аспекти міжнародного співробітництва України у сфері протидії інформаційним загрозам в умовах воєнного стану. *Expert Paradigm of Law and Public Administration*, *1*(33), 67-73. https://doi.org/10.32689/2617-9660-2025-1(33)-67-73

6. Худолій, А. (2019). Кібербезпека: сучасні виклики перед Україною. *Acta de Historia & Politica Saeculum XXI, (1)*, 138-146. https://doi.org/10.26693/ahpsxxi2019.01.138

7. Чепелюк, Ю. (2021). Цифрова дипломатія в контексті сучасних інформаційних комунікацій. *Цифрова платформа: інформаційні технології в соціокультурній сфері*, *4*(2), 250-258. https://doi.org/10.31866/2617-796X.4.2.2021.247492

8. Державна служба спеціального зв'язку та захисту інформації України. (2025, Червень 10). *Голова Держспецзв'язку на конференції TechNet: Унікальний досвід України у кібервійні стає основою для тренувань світового рівня*. Режим доступу: https://cip.gov.ua/ua/news/golova-derzhspeczv-yazku-na-konferenciyi-technet-unikalnii-dosvid-ukrayini-u-kiberviini-staye-osnovoyu-dlya-trenuvan-svitovogo-rivnya (дата звернення: 04.07.2025).

9. Суспільне. (2023, Травень 16). *Україна офіційно приєдналася до Центру НАТО з кіберзахисту*. Режим доступу: https://suspilne.media/478003-ukraina-oficijno-priednalasa-do-centru-nato-z-kiberzahistu/ (дата звернення: 04.07.2025).

10. Укрінформ. (2025, Липень 3). *Україна отримає доступ до Резерву кібербезпеки ЄС*. Режим доступу: https://www.ukrinform.ua/rubric-polytics/4011010-ukraina-otrimae-dostup-do-rezervu-kiberbezpeki-es.html (дата звернення: 04.07.2025).

11. Чернівецька обласна військова адміністрація. (2023, Жовтень 2). *USAID виділяє грант $500 000 на впровадження інноваційних проектів у сфері кібербезпеки*. Режим доступу: https://bukoda.gov.ua/news/usaid-vydiliaie-hrant-500-000-na-vprovadzhennia-innovatsiinykh-proektiv-u-sferi-kiberbezpeky (дата звернення: 04.07.2025).

12. Algorytm-X. (2021, Січень 29). *Держспецзв'язку України співпрацюватиме зі службою кібербезпеки Держдепу, готують угоду*. Режим доступу: https://algorytmx.com.ua/news/derzhspeczvyazku-ukrayini-spivpracyuvatime-zi-sluzhboyu-kiberbezpeki-derzhdepu-gotuyut-ugodu (дата звернення: 04.07.2025).

References:

1. Velychko, L. Yu., & Bilokon, M. V. (2024). Hibrydni zahrozy transportnii infrastrukturi. [Hybrid threats to transport infrastructure: challenges for state regulation]. *Teoriia ta praktyka derzhavnoho upravlinnia – Theory and Practice of Public Administration*, *2*(79), 442–464. https://doi.org/10.26565/1727-6667-2024-2-23 [in Ukrainian].

2. Zharovska, I., & Ortynska, N. (2020). Informatsiina viina yak suchasne hlobazatsiine yavyshche. [Information warfare as a modern globalization phenomenon]. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: "Yurydychni nauky" – Bulletin of Lviv Polytechnic National University. Series: "Legal Sciences"*, *7*(2), 56-61. https://doi.org/10.23939/law2020.26.056 [in Ukrainian].

3. Karamyshev, D. V., Sobol, R. G., Myrna, N. V., & Yevdokymov, V. O. (2023). Derzhavne upravlinnia u sferi natsionalnoi bezpeky i oborony. [Public administration in the sphere of national security and defense]. *State Formation*, *2*(34), 54–66. https://doi.org/10.26565/1992-2337-2023-2-05 [in Ukrainian].

4. Kononenko, V. P., Zdorovko, S. S., & Korol'ova, A. Ye. (2023). Informatsiina bezpeka yak stan [Information security as a special state]. *Uzhhorod National University Herald Series Law*, *2*(76), 244-250. https://doi.org/10.24144/2307-3322.2022.76.2.39 [in Ukrainian].

5. Suslin, S. (2025). Pravovi aspekty mizhnarodnoho spivrobitnytstva Ukrainy u sferi protydii informatsiinym zahrozam v umovakh voiennoho stan. [Legal aspects of international cooperation of Ukraine in the sphere of countering information threats under martial law]. *Expert Paradigm of Law and Public Administration*, *1*(33), 67-73. https://doi.org/10.32689/2617-9660-2025-1(33)-67-73 [in Ukrainian].

6. Khudolii, A. (2019). Kiberbezpeka: suchasni vyklyky pered Ukrainou. [Cybersecurity: Modern Challenges for Ukraine]. *Acta de Historia & Politica Saeculum XXI, (1),* 138-146. https://doi.org/10.26693/ahpsxxi2019.01.138 [in Ukrainian].

7. Chepeliuk, Y. (2021). Tsyfrova dyplomatiia v konteksti suchasnykh informatsiinykh komunikatsii. [Digital diplomacy in the context of modern information communications]. *Tsyfrova platforma: informatsiini tekhnolohii v sotsiokulturnii sferi – Digital Platform: Information Technologies in Sociocultural Sphere*, *4*(2), 250-258. https://doi.org/10.31866/2617-796X.4.2.2021.247492 [in Ukrainian].

8. State Service of Special Communications and Information Protection of Ukraine. (2025, June 10). *Holova Derzhspetszviazku na konferentsii TechNet: Unikalnyi dosvid Ukrainy u kiberviini staie osnovoiu dlia trenuvan svitovoho rivnia*. [Head of the State Special Communications Service at the TechNet conference: Ukraine's unique experience in cyberwarfare becomes the basis for world-class training]. Retrieved from https://cip.gov.ua/ua/news/golova-derzhspeczv-yazku-na-konferenciyi-technet-unikalnii-dosvid-ukrayini-u-kiberviini-staye-osnovoyu-dlya-trenuvan-svitovogo-rivnya [in Ukrainian].

9. Suspilne. (2023, May 16). *Ukraina ofitsiino pryiednalasia do Tsentru NATO z kiberzakhystu*. [Ukraine officially joined the NATO Cyber Defense Center]. Retrieved from https://suspilne.media/478003-ukraina-oficijno-priednalasa-do-centru-nato-z-kiberzahistu/ [in Ukrainian].

10. Ukrinform. (2025, July 3). *Ukraina otrymaie dostup do Rezervu kiberbezpeky YeS*. [Ukraine has received access to the EU Cybersecurity Reserve]. Retrieved from https://www.ukrinform.ua/rubric-polytics/4011010-ukraina-otrimae-dostup-do-rezervu-kiberbezpeki-es.html [in Ukrainian].

11. Chernivtsi Regional State Administration. (2023, October 2). *USAID vydiliaie hrant $500 000 na vprovadzhennia innovatsiinykh proektiv u sferi kiberbezpeky*. [USAID allocates a grant of $500,000 for the implementation of innovative projects in the field of cybersecurity] Retrieved from https://bukoda.gov.ua/news/usaid-vydiliaie-hrant-500-000-na-vprovadzhennia-innovatsiinykh-proektiv-u-sferi-kiberbezpeky [in Ukrainian].

12. Algorytm-X. (2021, January 29). *Derzhspetszviazku Ukrainy spivpratsiuvatyme zi sluzhboiu kiberbezpeky Derzhdepu, hotuiut uhodu*. [The State Service of Special Communications of Ukraine will cooperate with the State Department's cybersecurity service, an agreement is being prepared]. Retrieved from https://algorytmx.com.ua/news/derzhspeczvyazku-ukrayini-spivpracyuvatime-zi-sluzhboyu-kiberbezpeki-derzhdepu-gotuyut-ugodu [in Ukrainian].