УДК 323.28
DOI https://doi.org/10.32782/2312-1815/2025-20-24

Наталія Ларіончева
ORCID: 0009-0000-3605-0163

МІЖНАРОДНА СПІВПРАЦЯ У СФЕРІ КІБЕРБЕЗПЕКИ

У статті здійснено порівняльний аналіз ключових аспектів міжнародної співпраці у сфері кібербезпеки в умовах сучасних глобальних інформаційних загроз. Актуальність дослідження зумовлена швидким розвитком інформаційних технологій, що потребує нових підходів до захисту від кіберзагроз та інформаційних втручань. Окрему увагу приділено важливості спільних заходів для протидії дезінформації та кібернападам, підвищення ефективності глобальної безпеки через обмін інформацією, стандартизацію процесів та розвиток національних стратегій кіберзахисту. Визначено, що поглиблене розуміння кіберзагроз вимагає нових підходів до аналізу воєнно-політичної ситуації, зокрема в контексті гібридних і мережевої війн. Проаналізовано значення міжнародної співпраці у сфері кібербезпеки, яка має сприяти не лише оперативному реагуванню на кібернапади, а й створенню єдиних стандартів безпеки. Спільні ресурси для реагування на надзвичайні ситуації, зокрема на атаки на критичну інфраструктуру, є важливим аспектом захисту глобальної кіберінфраструктури. Окрема увага приділена досвіду країн Європейського Союзу та НАТО, зокрема співпраці України з НАТО у сфері кібербезпеки. Підкреслено необхідність подальшої інтеграції України в міжнародну співпрацю, зокрема, через участь у міжнародних форумах, удосконалення національного законодавства та розвиток систем раннього запобігання та реагування на кіберзагрози.

Ключові слова: *кібербезпека, інформаційні війни, міжнародна співпраця, дезінформація, гібридні конфлікти, інформаційні операції, європейська інтеграція, НАТО, міжнародні стандарти.*

Вступ. Актуальність дослідження зумовлена тим, що міжнародна співпраця у сфері кібербезпеки є вирішальною для протидії інформаційним загрозам. Спільні стандарти, обмін інформацією та співпраця між країнами можуть підвищити ефективність заходів протидії дезінформації і кібератак. Сьогодні є необхідність розробити ефективні стратегії захисту від інформаційних загроз та протидії інформаційним втручанням. Ця стаття має на меті визначити ключові напрями міжнародної співпраці у сфері кібербезпеки для забезпечення захисту від сучасних кіберзагроз й ефективного реагування на інформаційні війни, а також визначення перспектив розвитку національних стратегій і механізмів захисту в умовах гібридних конфліктів.

Матеріал і методи дослідження. Для дослідження теми використано комплекс методів, зокрема аналіз літератури та документів, що дає змогу виявити теоретичні основи та нормативно-правову базу щодо інформаційних воєн і кібербезпеки. Застосовано контент-аналіз медіаматеріалів та кейс-метод для вивчення конкретних прикладів сучасних конфліктів, а також порівняльний аналіз підходів різних країн до захисту кіберпростору.

Результати та обговорення. З огляду на постійну еволюцію характеру сучасних воєнних конфліктів, методи та підходи до аналізу воєнно-політичної обстановки повинні також зазнавати змін. Трансформація характеристик сучасних воєнних конфліктів і військово-політичних відносин вимагає адаптації аналітичних підходів, зосереджуючи увагу на нових аспектах та елементів, що потребують детального дослідження для забезпечення об'єктивності результатів оцінки ситуації [6, с. 8]. Сучасні воєнні конфлікти суттєво відрізняються від попередніх, оскільки вони набули нових характеристик та особливостей, що вимагають поглибленого аналізу й розуміння. Якщо в минулому стратегія ведення війни ґрунтувалася переважно на силовому примусі та прямому військовому протистоянні між сторонами конфлікту, то сучасні

воєнні конфлікти виявляють значно складніші й різноманітніші риси. Виокремлення цих нових характеристик спричинило появу таких термінів, як «проксі-війна», «гібридна війна» та «мережева війна» [2].

Класичні війни до винайдення ядерної зброї зазвичай відбувалися між державами або коаліціями із чіткими політичними цілями, використовуючи великі військові формування й зосереджуючи увагу на застосуванні сили. Натомість сучасні концепції, як-от «інформаційна війна», охоплюють не лише електронний та кібернетичний складники, а й управління інформацією в комп'ютерних мережах. Термін «інформаційні операції» розширює цей підхід, включно з аналізом соціальних мереж та людським фактором, зокрема впливом на поведінку, ухвалення рішень й управлінські процеси [11] Згідно з концепцією НАТО, інформаційна війна спрямована на досягнення інформаційної переваги над противником, що є важливим елементом сучасної воєнної стратегії. Вона передбачає використання інформаційних ресурсів та технологій з метою маніпулювання інформацією, впливу на громадську думку та дезорієнтації супротивника. Досягнення інформаційної переваги не тільки забезпечує стратегічну ініціативу, а й дає змогу ефективно впливати на військові, політичні та економічні процеси в умовах конфлікту. Цей аспект стає особливо важливим в умовах глобалізації та розвитку цифрових технологій, що значно розширюють можливості для ведення інформаційних операцій [10]

Інформаційна війна, яка є одним з основних елементів сучасних воєнних конфліктів, виявляється в широкому спектрі форм і методів, що спрямовані на маніпулювання інформацією, вплив на громадську думку та дезінформацію. Цей аспект сучасних конфліктів відзначається своєю багатогранністю, що містить як технологічні, так і психологічні стратегії. Для детального розуміння та аналізу інформаційної війни доцільно розглянути основні її форми й методи:

− блокування й маніпулювання інформацією – приглушення телевізійних, інтернет- та радіопрограм для порушення зв'язку й поширення дезінформації;

− перешкоджання логістичних мереж – від'єднання комунікаційних мереж для обмеження доступу до інформації та ускладнення управління;

− атаки на соціальні медіа – підробка або перешкоджання ворожих комунікаційних мереж для створення негативного іміджу ворога;

− саботаж фінансових ринків – електронне втручання або поширення дезінформації для спричинення фінансових турбулентностей;

− використання дронів і роботизованих систем – розвідувальні операції для збору інформації з віддалених територій;

− комунікаційний менеджмент – контроль за поширенням інформації, підтримка іміджу та формування позитивного ставлення до своєї сторони;

− синтетичні носії інформації – створення фальшивих новин або матеріалів для маніпуляцій з громадською думкою.

Ці методи підкреслюють складність сучасних конфліктів і потребу в комплексних стратегіях захисту інформаційної безпеки [9]

Аналізуючи сучасні реалії інформаційної війни в контексті міжнародних відносин, можна зробити висновок про її критичне значення та вплив на геополітичні процеси. На рубежі XXI століття іміджевий складник інформаційної війни став одним з найважливіших інструментів, оскільки маніпуляція інформацією про події, перекручування фактів та створення ілюзій стали ключовими чинниками у формуванні світових поглядів і впливу на суспільну свідомість. У цьому контексті важливо підкреслити, що роль інформаційних технологій у цих процесах не лише посилюється, а й постійно змінюється, що вимагає адаптації до нових викликів і стратегій.

Зокрема, дослідження випадків інформаційних втручань у вибори, а також подій на міжнародній арені демонструють, що інформаційна війна сьогодні має не менше значення, ніж

збройні конфлікти. Вона здатна впливати на геополітичну ситуацію, змінюючи не тільки політичні ландшафти, а й економічні реалії. З огляду на це, захист від інформаційних загроз вимагає комплексного підходу, який містить не тільки технічні заходи кібербезпеки, а й розвиток медійної грамотності, підтримку незалежного журналістського середовища та сприяння прозорості в діяльності органів влади.

З огляду на глобальність сучасних загроз, міжнародна співпраця у сфері кібербезпеки набуває надзвичайно вагомого значення. Спільні стандарти, обмін інформацією та активна співпраця між державами можуть значно підвищити ефективність заходів, спрямованих на боротьбу з дезінформацією та кібератаками, що, своєю чергою, дає змогу значно знижувати ризики, пов'язані з інформаційними війнами на міжнародному рівні.

Обмін інформацією про нові кіберзагрози є критичним для своєчасного реагування на потенційні атаки. Коли одна країна виявляє нову загрозу, вона може передавати цю інформацію своїм партнерам, що дає змогу іншим державам бути підготовленими до можливих атак. Спільні дослідження та навчання у сфері кібербезпеки також допомагають країнам реагувати на нові виклики, оскільки технології та методи кібератак постійно еволюціонують. У цьому контексті важливим є обмін досвідом і знаннями між державами для створення більш надійної глобальної системи захисту. Співпраця також може сприяти зміцненню довіри між країнами, оскільки чіткі й прозорі міжнародні угоди дають змогу зменшити ризик конфліктів, що можуть виникати через кібератаки або інформаційні війни.

Крім того, кіберзагрози можуть мати серйозні наслідки для глобальної безпеки, тому важливо мати спільні ресурси для реагування на надзвичайні ситуації. Наприклад, кібератаки на критичну інфраструктуру, енергетичні системи або фінансові ринки можуть потребувати швидкої та координованої реакції з боку багатьох країн. Міжнародна співпраця дає змогу мобілізувати ресурси, включно з технічною допомогою, експертними знаннями та людськими ресурсами, для ефективного реагування на такі загрози. У разі таких надзвичайних ситуацій необхідно мати узгоджені механізми для швидкої мобілізації і дій, щоб запобігти значним шкодам або загрозам безпеці на глобальному рівні.

Ще однією важливою причиною для розвитку міжнародної співпраці є дедалі більший потенціал кібертероризму та зловживання технологіями. Взаємодія між країнами дає змогу не лише вчасно блокувати потенційно небезпечні дії, а й розробляти законодавчі ініціативи для криміналізації кібертероризму та інших злочинів у кіберпросторі. Крім того, з розвитком штучного інтелекту та великих даних важливо забезпечити спільне управління цими технологіями, створюючи міжнародні етичні принципи та стандарти їх використання, що дасть змогу забезпечити їх безпеку та ефективність у боротьбі з кіберзагрозами.

О. М. Поляков зауважує, що міжнародна співпраця надзвичайно важлива для подолання правового вакууму, який утворюється внаслідок швидкого розвитку інформаційних технологій, що випереджають законодавчі ініціативи у сфері кібербезпеки. Цей вакуум стає перешкодою для ефективної протидії кіберзагрозам, оскільки національні законодавства не завжди здатні оперативно реагувати на нові виклики, пов'язані з кіберзлочинністю та іншими видами кібернебезпеки. Вирішення цього питання можливе лише через активне міжнародну співпрацю, яка повинна стати основою для створення єдиного правового поля, що дає змогу забезпечити ефективний захист від глобальних кіберзагроз [7, с. 131].

Міжнародна співпраця має кілька ключових напрямів. По-перше, вона спрямована на зміцнення взаємної довіри між країнами у сфері кібербезпеки. Цей процес передбачає обмін інформацією про кіберзагрози, методи протидії їм, а також спільні навчання та тренування спеціалістів з кібербезпеки. Надійна міжнародна співпраця дає змогу країнам більш ефективно реагувати на загрози в кіберпросторі, що мають транснаціональний характер. По-друге, це передбачає вироблення спільних підходів до протидії кіберзагрозам. У цьому контексті

важливо узгодити стандарти безпеки, розробити єдині стратегії реагування на кіберінциденти та запровадити механізми для взаємодії в разі виникнення глобальних кіберзагроз. Такі зусилля допомагають уникнути ситуацій, коли країни, діючи окремо, можуть не досягти бажаного результату в боротьбі з кіберзлочинністю та іншими кібернебезпеками. По-третє, міжнародна співпраця у сфері кібербезпеки передбачає запобігання використання кіберпростору в протиправних цілях, як-от кібершпигунство, кібератаки на критичну інфраструктуру, фінансові операції або маніпуляції з даними. Скоординовані заходи з боку держав можуть значно знизити ймовірність таких загроз, забезпечивши більш стійку глобальну кіберінфраструктуру [8, с. 489].

Практика спільного протистояння кіберзагрозам не нова. Так, у США, Великої Британії, Ізраїлю та Німеччини вже є позитивний досвід, який свідчить про можливість створення ефективних систем кібербезпеки, які мають єдиний координувальний орган, здатний оперативно акумулювати ресурси різних державних і недержавних структур для протидії та нейтралізації кібератак. Ці системи підпорядковуються голові виконавчої влади і, як правило, містять кілька основних складників, серед яких: військовий компонент, компонент захисту критичної інфраструктури, правоохоронний аспект та дорадчо-консультативний орган. Така структура дає змогу забезпечити комплексний підхід до розв'язання проблем у сфері кібербезпеки, забезпечуючи ефективність і швидкість реагування на кіберзагрози [5, с. 92].

Останнім часом спостерігається значний прогрес та досвід Європейського Союзу в розробці та вдосконаленні механізмів забезпечення кібербезпеки європейських країн, Україна повинна активно долучитися до цих процесів. Ураховуючи європейські інтеграційні прагнення України, участь у формуванні спільних механізмів кібербезпеки допоможе країні не лише поліпшити свій міжнародний імідж, а й суттєво вплинути на розвиток організаційно-правової бази національної кібербезпеки. Така співпраця з ЄС може стати важливим кроком на шляху до підвищення рівня захищеності національних інформаційних систем і розвитку ефективної стратегії кіберзахисту в межах європейського простору. Крім того, участь у міжнародних ініціативах у сфері кібербезпеки сприятиме інтеграції найкращих європейських практик і стандартів у національне законодавство, що дасть змогу підвищити рівень захисту від кіберзагроз і створити ефективну правову основу для боротьби з кіберзлочинністю в Україні [1, с. 34].

Крім того, пріоритетним є зближення у сфері кібербезпеки України з НАТО, яка відіграє ключову роль у формуванні єдиних підходів до забезпечення кібербезпеки, що є невід'ємним складником національної безпеки країн-членів та партнерів. Перші кроки в цьому напрямі вже здійснено [4, с. 52]. У 2008 році в межах Спільної робочої групи України — НАТО з питань воєнної реформи з ініціативи Служби безпеки України започатковано створення Робочої підгрупи з питань кібернетичного захисту. Цей крок став основою для розробки концептуальних засад взаємодії між Україною та НАТО у сфері кібербезпеки, запровадження механізму консультацій та оперативного обміну інформацією в разі кібернетичних атак національного масштабу, а також розробки критеріїв оцінки кібернетичних загроз [3].

Відтоді співпраця між Україною та НАТО у сфері кібербезпеки значно розширилася. У 2023 році фахівці Міноборони та Збройних сил України з питань кібербезпеки відвідали структури НАТО, що свідчить про поглиблення співпраці та обміну досвідом у сфері кіберзахисту. У 2024 році Україна вперше офіційно взяла участь у навчаннях НАТО з кібероборони Locked Shields, що підкреслює зобов'язання глобальної спільноти боротися з кіберзагрозами. Крім того, під час візиту до штаб-квартири НАТО українська делегація представила уроки кібервійни, що триває, а також потреби та пропозиції щодо майбутньої співпраці з НАТО в цій сфері. Співпраця між Україною та НАТО у сфері кібербезпеки є важливим елементом національної безпеки України, сприяючи підвищенню ефективності протидії кіберзагрозам й інтеграції України в європейські та євроатлантичні структури безпеки.

Для подальшого посилення інтеграції України в міжнародну співпрацю у сфері кібербезпеки важливо врахувати низку стратегічних та практичних кроків, що сприятимуть зміцненню національної безпеки й ефективному реагуванню на сучасні кіберзагрози. Україні необхідно активніше брати участь у міжнародних форумах та ініціативах, що стосуються кібербезпеки, як-от Глобальний форум кібербезпеки, форум Європейського Союзу з кіберзахисту, а також у спільних військових навчаннях НАТО з кібероборони. Це дасть змогу не лише отримати доступ до передових практик та стандартів кібербезпеки, а й зміцнити взаємодію з міжнародними партнерами. Важливо працювати над гармонізацією національного законодавства з міжнародними стандартами у сфері кібербезпеки, зокрема шляхом інтеграції норм Європейського Союзу в цю сферу. Водночас необхідно розвивати національні системи раннього запобігання та реагування на кіберінциденти в межах міжнародних ініціатив. Україна повинна розвивати співпрацю з міжнародними організаціями, як-от Інтерпол та ООН, задля посилення боротьби з кіберзлочинністю, установлення більш ефективних механізмів обміну інформацією та вдосконалення процедур реагування на транснаціональні кіберзагрози. Зокрема, важливо створити ефективні канали для оперативного обміну даними й координації між правоохоронними органами різних країн у разі кіберзлочинів, що мають міжнародний характер.

Варто поглиблювати співпрацю з приватним сектором для розробки новітніх технологій і механізмів кіберзахисту, а також забезпечити захист критичних інформаційних ресурсів, які використовують державні установи. Це також передбачає спільні дослідження у сфері кібербезпеки та залучення передових технологій для підвищення рівня захисту національних інформаційних систем. Поглиблене навчання та професійна підготовка фахівців дасть змогу Україні створити висококваліфіковану команду спеціалістів, здатних оперативно реагувати на будь-які кіберзагрози. Реалізація цих рекомендацій допоможе Україні зміцнити своє місце в міжнародній співпраці з кібербезпеки, підвищити стійкість до кіберзагроз і забезпечити високий рівень національної безпеки в умовах глобальних викликів.

Висновки. Сучасні інформаційні війни відіграють ключову роль у глобальному політичному та військовому контексті. З використанням новітніх технологій масової комунікації вони стали ефективним інструментом впливу на громадську думку, формування дискурсу та маніпулювання відносинами міжнародного співтовариства.

Пропаганда й дезінформація стали ключовими стратегіями інформаційних воєн. Зловживання соціальними мережами та іншими медіаплатформами дає змогу режимам та нетиповим суб'єктам змінювати громадську думку, впливати на рішення й підривати довіру до демократичних інститутів.

Захист від інформаційних загроз потребує комплексного підходу. Крім технічних заходів кібербезпеки, важливо розвивати медійну грамотність, підтримувати незалежне журналістське середовище та сприяти прозорості у владі.

Міжнародна співпраця у сфері кібербезпеки є вирішальною для протидії інформаційним загрозам. Спільні стандарти, обмін інформацією та співпраця між країнами можуть підвищити ефективність заходів протидії дезінформації та кібератак. Для України особливо важливим є розвиток співпраці з НАТО та іншими міжнародними партнерами для зміцнення національної кібербезпеки й ефективної боротьби із сучасними загрозами, що є важливим кроком на шляху до євроатлантичної інтеграції та покращення міжнародного іміджу країни.

Література:

1. Войціховський А. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права.* 2018. № 53. С. 26–37

2. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу URL: www.niss.gov.ua/public/File/2015_ book/012315_Gorbulyn.pdf. (дата звернення: 20 грудня 2024)

3. Кудіна М. НАТО посилюватиме кіберзахист України у гібридній війні з РФ. *Інтернет Свобода.* 2022. URL: https://netfreedom.org.ua/article/nato-posilyuvatime-kiberzahist-ukrayini-ugibridnij-vijni-z-rf (дата звернення: 20 грудня 2024)

4. Лук'янчук Р. Міжнародна співпраця у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України. Серія : Державне управління.* 2015. No 4. С. 50-56.

5. Панченко В. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз. *Інформаційна безпека людини, суспільства, держави.* 2012. № 3 (10). С. 91–100

6. Погляди на характер сучасних воєнних конфліктів. *Наука і оборона* за ред. В. Бочарніков, С. Свєшніков. 2017. URL: http://nbuv.gov.ua/UJRN/nauio_2017_1_3 с.8 (дата звернення: 25 грудня 2024)

7. Поляков О. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право.* 2021. № 2 (37). С. 129–138.

8. Сливка М. Міжнародна співпраця у сфері забезпечення кібербезпеки України *Юридичний науковий електронний журнал* 2022. Вип. 10. С. 489–491

9. Haq Ehsan-Ul, Tyson Gareth, Broad Tristan, Hui Pan. Using social media for information divisiveness and warfare. *Proceedings of the 33rd ACM conference on Hypertext and social media. HT '22. New York,* New York, USA: Association for Computing Machinery, 2022. С. 259–262.

10. Information Warfare. NATO. URL: https://www.nato.int/cps/en/natolive/topics_82771.htm (дата звернення: 25 грудня 2024)

11. Stein, George J. Information Warfare. Air University (USA). Press. URL: https://universityofleeds.github.io/philtaylorpapers/vp01e61f.html (дата звернення: 25 грудня 2024)

References:

1. Voytsikhovs′kyy, A. (2018). Kiberbezpeka yak vazhlyva skladova systemy zakhystu natsional′noyi bezpeky yevropeys′kykh krayin [Cybersecurity as an important component of the national security protection system of European countries]. *Zhurnal skhidnoyevropeys'koho prava*, 53, 26–37. [in Ukrainian]

2. Horbulin, V. (2015). «Hibrydna viyna» yak klyuchovyy instrument rosiys′koyi heostratehiyi revanshu ["Hybrid war" as a key tool of Russian geostrategy for revenge]. Natsional′nyy instytut stratehichnykh doslidzhen′. Retrieved from: www.niss.gov.ua/public/File/2015_book/012315_Gorbulyn.pdf [in Ukrainian]

3. Kudina, M. (2022). NATO posylyuvatyme kiberzakhyst Ukrayiny u hibrydniy viyni z RF [NATO will strengthen Ukraine's cyber defense in the hybrid war with the Russian Federation]. Internet Svoboda. Retrieved from: https://netfreedom.org.ua/article/nato-posilyuvatime-kiberzahist-ukrayini-ugibridnij-vijni-z-rf [in Ukrainian]

4. Luk″yanchuk, R. (2015). Mizhnarodne spivrobitnytstvo u sferi zabezpechennya kibernetychnoyi bezpeky: derzhavni priorytety [International cooperation in ensuring cybernetic security: State priorities]. Visnyk Natsional′noyi akademiyi derzhavnoho upravlinnya pry Prezydentovi Ukrayiny. Seriya: Derzhavne upravlinnya, 4, 50–56. [in Ukrainian]

5. Panchenko, V. (2012). Zarubizhnyy dosvid formuvannya system zakhystu krytychnoyi infrastruktury vid kiberzahroz [Foreign experience in forming systems to protect critical infrastructure from cyber threats]. Informatsiyna bezpeka lyudyny, suspil′stva, derzhavy, 3(10), 91–100. [in Ukrainian]

6. Pohlyady na kharakter suchasnykh voyennykh konfliktiv [Views on the nature of modern military conflicts]. (2017). Nauka i oborona / V. Bocharnikov, S. Svyeshnikov (Ed.). Retrieved from: http://nbuv.gov.ua/UJRN/nauio_2017_1_3 p. 8 [in Ukrainian]

7. Polyakov, O. (2021). Aktyvizatsiya mizhnarodnoyi spivpratsi u sferi zabezpechennya kiberbezpeky: shlyakhy udoskonalennya v realiyakh s′ohodennya [ntensification of international cooperation in cybersecurity: Ways to improve in current realities]. *Informatsiya i pravo*, 2(37), 129–138. [in Ukrainian]

8. Slyvka, M. (2022). Mizhnarodne spivrobitnytstvo u sferi zabezpechennya kiberbezpeky Ukrayiny [International cooperation in ensuring Ukraine's cybersecurity]. *Yurydychnyy naukovyy elektronnyy zhurnal*, 10, P. 489–491 [in Ukrainian]

9. Haq, E.-U., Tyson, G., Broad, T., & Hui, P. (2022). Using social media for information divisiveness and warfare. *In Proceedings of the 33rd ACM conference on Hypertext and social media (HT '22)* Association for Computing Machinery. NATO. (n.d.). PP. 259–262.

10. Information warfare. NATO. Retrieved from: https://www.nato.int/cps/en/natolive/topics_82771.htm
11. Stein, G. J. Information warfare. Air University (USA) Press. Retrieved from: https://universityofleeds.github.io/philtaylorpapers/vp01e61f.html

Natalia Larioncheva. International cooperation in the field of cybersecurity

The article provides a comparative analysis of the key aspects of international cooperation in the field of cybersecurity in the context of modern global information threats. The relevance of the study is due to the rapid development of information technologies, which requires new approaches to protection against cyber threats and information interference. Particular attention is paid to the importance of joint measures to counter disinformation and cyber attacks, increase the effectiveness of global security through information exchange, standardisation of processes and development of national cyber defence strategies. It is determined that an in-depth understanding of cyber threats requires new approaches to the analysis of the military-political situation, in particular in the context of hybrid warfare and network warfare. The author analyses the importance of international cooperation in the field of cybersecurity, which should contribute not only to a prompt response to cyber attacks, but also to the creation of common security standards. Sharing resources to respond to emergencies, including attacks on critical infrastructure, is an important aspect of protecting global cyber infrastructure. Particular attention is paid to the experience of the European Union and NATO, including Ukraine's cooperation with NATO in the field of cybersecurity. The need for further integration of Ukraine into international cooperation, in particular through participation in international forums, improvement of national legislation, and development of early warning and response systems to cyber threats, is emphasised.

Key words: *cybersecurity, information warfare, international cooperation, disinformation, hybrid conflicts, information operations, European integration, NATO, international standards.*

Відомості про автора:
Ларіончева Наталія – аспірантка кафедри політичних наук,
Київський національний університет імені Тараса Шевченка.