УДК 327:004.056
DOI: https://doi.org/10.21564/2663-5704.65.331787

Вівчар Інна Володимирівна, кандидат політичних наук, доцент кафедри політології і міжнародних відносин, Рівненський державний гуманітарний університет, Україна
e-mail: innavivchar79@gmail.com
ORCID ID: 0000-0002-3661-101X

Постельжук Олександр Петрович, кандидат історичних наук, доцент кафедри політології і міжнародних відносин, Рівненський державний гуманітарний університет, Україна
e-mail: olexandr1506@gmail.com
ORCID ID: 0000-0002-7123-7908

Валюх Людмила Іванівна, кандидат історичних наук, доцент кафедри політології і міжнародних відносин, Рівненський державний гуманітарний університет, Україна
e-mail: lydmullav@gmail.com.
ORCID ID: 0000-0002-0212-5400

КІБЕРБЕЗПЕКА ЯК СФЕРА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА В ПЕРІОД ГЛОБАЛЬНОЇ КРИЗИ БЕЗПЕКИ

У статті досліджено кібербезпеку як ключовий компонент міжнародного співробітництва в умовах глобальної безпекової кризи. Проаналізовано трансформацію кіберзагроз у фактор стратегічної нестабільності та необхідність формування глобального режиму кібербезпеки. Розглянуто правові, технічні та інституційні аспекти реагування на кіберінциденти, діяльність міжнародних організацій (ITU, ENISA, HATO), а також європейські ініціативи (NIS2, CERT-EU). Визначено особливості участі України в міжнародних кібербезпекових механізмах і наголошено на потребі уніфікації нормативних підходів, посиленні кіберспроможностей і міждержавній координації дій. Кібербезпека трактується як глобальне публічне благо, що потребує багаторівневого управління та політичної солідарності.

Ключові слова: *кібербезпека, міжнародне співробітництво, кібератаки, глобальна безпека, інституційна архітектура, кіберзагрози, цифровий суверенітет.*

Постановка проблеми дослідження, що стосується кібербезпеки як сфери міжнародного співробітництва в умовах глобальної кризи безпеки, ґрунту-

ється на усвідомленні принципово нових викликів, які постають перед міжнародною спільнотою в цифрову епоху. Сутність проблеми полягає в тому, що стрімка цифровізація всіх сфер життєдіяльності, з одного боку, відкриває нові можливості для розвитку, але з іншого, – створює вразливі точки, які дедалі частіше використовуються державними й недержавними суб'єктами для реалізації агресивних дій у кіберпросторі.

У такому контексті кіберзагрози вже не мають локального або регіонального характеру – вони є транснаціональними за своєю природою, здатними одночасно паралізувати будь-яку інфраструктуру, дестабілізувати цілі сектори економіки, впливати на політичні процеси й підривати довіру до демократичних інституцій. Особливої гостроти проблема набуває в умовах ескалації традиційних форм конфліктів, коли кіберпростір перетворюється на один із ключових театрів бойових дій.

Це яскраво демонструє приклад повномасштабної війни Росії проти України, яка супроводжується масштабними кібератаками на урядові структури, об'єкти критичної інфраструктури, медіа, приватний сектор і громадянське суспільство. Водночас реагування на ці загрози не може бути ефективним без міждержавної координації, оперативного обміну даними про інциденти, уніфікації нормативно-правових підходів та об'єднання технічних ресурсів для протидії загрозам у реальному часі. На тлі зростання частоти та складності кібератак, виявляється дефіцит загальноприйнятих міжнародно-правових механізмів регулювання поведінки більшості держав у сучасному кіберпросторі. Відсутність консолідованих норм, які б унормовували межі допустимого в умовах конфлікту, питання відповідальності за використання шкідливих програм, захист цивільної інфраструктури або реагування на кіберінциденти, значно ускладнює можливість ефективної превенції та притягнення до відповідальності винних. Проблемою є нерівномірність кіберспроможностей різних країн, що створює глобальний цифровий розрив і посилює асиметрію у спроможності до протидії таким кіберзагрозам.

У цьому контексті надзвичайної **актуальності** набуває питання міжнародної солідарності, передачі технологій, підвищення кіберосвіченості та підтримки країн, що розвиваються у формуванні їхніх кіберзахисних механізмів. Тож проблемне поле дослідження охоплює як політико-правові, так і технологічні аспекти кібербезпеки, з акцентом на необхідності системного, міждисциплінарного підходу до формування ефективного міжнародного співробітництва в цій сфері. Розв'язання означеної проблеми потребує комплексної мобілізації багатьох ресурсів, нової моделі довіри між державами, інтеграції приватного сектору та забезпечення балансу між безпекою, правами людини та свободою інтернету.

Аналіз останніх досліджень і публікацій, присвячених проблематиці кібербезпеки як сфери міжнародного співробітництва в умовах нинішньої глобальної кризи безпеки, демонструє високий рівень міждисциплінарної зацікавленості щодо теми та наявність як теоретичних, так і практичних наукових розробок у цій галузі. Представлені джерела охоплюють спектр аспектів – від філософсько-правових основ до аналізу конкретних інституційних механізмів і практик міжнародної взаємодії. У роботі М. Барана акцентовано увагу на правових принципах регулювання інституту інформаційної безпеки, що є наразі концептуально важливим для розуміння кібербезпеки як складника ширшої інформаційної парадигми [2]. Автор підкреслює необхідність гармонізації національного законодавства із міжнародними стандартами, зокрема в частині правових визначень, що має вкрай важливе значення в умовах транснаціонального характеру кіберзагроз.

У низці робіт – С. Савчука [17], В. Гавриляка [10] – розкрито перспективи інтеграції України в європейську систему кібербезпеки. Ідеться про поступове наближення до нормативного поля ЄС включно з директивами NIS/NIS2, розвиток національної інституційної архітектури (CERT-UA, Національний координаційний центр) та зміцнення спроможності до транскордонного реагування на такі інциденти. Ці дослідження наголошують на потребі системного підходу до побудови спроможності як основи для повноцінної участі в глобальних безпекових процесах.

Дослідження М. Сливки [5] присвячено практичному виміру міжнародної взаємодії України у сфері кібербезпеки. Особливо цінною є увага до інституційних механізмів співпраці, таких як діяльність у рамках FIRST, співпраця з НАТО та ООН, а також участь у багатосторонніх платформах, що сприяють оперативному обміну інформацією. У працях О. Архипова, В. Бровка [8] та Л. Веселової [9] явно простежується прагнення до концептуального переосмислення феномену кібербезпеки.

Працю Д. Дубова присвячено аналізу кіберпростору як нового виміру геополітичного суперництва. У ній обґрунтовується, що цифрове середовище трансформує природу міжнародної конкуренції, де держави втрачають монополію на насильство, а основними загрозами стають асиметричні, децентралізовані та нелінійні форми впливу. Автор акцентує на необхідності розроблення національної кіберстратегії, що поєднує технологічну адаптивність і превентивну безпеку в умовах глобальної динаміки [11]. Робота С. Савчука зосереджена на викликах та можливостях інтеграції України в систему кібербезпеки Європейського Союзу. Автор аналізує стан нормативної сумісності, наявні бар'єри інституційного та технічного характеру, а також перспективи приєднання України до ключових європейських структур, таких як ENISA

і CERT-EU. Запропоновано заходи з посилення національного потенціалу, гармонізації законодавства та налагодження стійкої оперативної взаємодії з державами – членами ЄС [17]. Праця А. Тарасюка є фундаментальним дослідженням теоретико-правових основ кібербезпеки України. У дисертації системно висвітлено нормативне регулювання у сфері захисту кіберпростору, проаналізовано функціональну взаємодію органів національної безпеки, обґрунтовано потребу в оновленні законодавства з урахуванням принципів технологічної нейтральності, пропорційності, субсидіарності та верховенства права. Значну увагу приділено критичному переосмисленню інституційної архітектури та необхідності її трансформації відповідно до викликів кіберсередовища [18]. Узагальнено ці джерела забезпечують міждисциплінарне підґрунтя для аналізу кібербезпеки України крізь призму стратегічних, інтеграційних і правових підходів.

Формулювання цілей. Метою дослідження є теоретичне обґрунтування кібербезпеки як самостійної та стратегічно важливої сфери міжнародного співробітництва в умовах глобальної кризи безпеки з визначенням її ролі в забезпеченні цифрового суверенітету, стабільності міжнародної системи та захисту сучасної критичної інфраструктури. Основної уваги приділяється з'ясуванню того, яким чином міжнародна взаємодія у сфері кібербезпеки може протистояти зростанню транснаціональних загроз, а також зменшувати асиметрію кіберспроможностей між державами та формувати нові моделі управління цифровим середовищем.

Цілями цього дослідження виступають: розроблення науково вивірених підходів до інституціоналізації та нормативної уніфікації міжнародної кіберспівпраці, вивчення основних механізмів і практик узаємодії між державами, міжурядовими організаціями та приватним сектором у протидії кіберзагрозам, а також виявлення потенціалу національних держав (зокрема України), щодо участі у формуванні міжнародної кіберполітики як одного з ключових напрямів нової архітектури глобальної безпеки.

Виклад основного матеріалу. Теоретичні та методологічні засади дослідження кібербезпеки як феномену міжнародних відносин, ґрунтуються на міждисциплінарному синтезі сучасного безпекознавства, інформаційного та міжнародного права, а також системного аналізу, що дозволяє розглядати кіберпростір одночасно як соціотехнічну систему, правовий режим і арену політичного протиборства. Вихідним поняттям виступає «безпека» в її соціальному вимірі як збалансований стан функціонування суспільних систем, що передбачає своєчасне розпізнавання та мінімізацію загроз. Саме так його науково інтерпретують О. Довгань, В. Пилипчук, О. Баранов і І. Корж [7], пропонуючи визначити кібербезпеку як структурний компонент інформацій-

ної безпеки з власними мережевими, інтернет- та аплікативними підрівнями. Методологічний каркас формують кілька взаємодоповнювальних рівнів. На макрорівні використовуються світоглядні й філософські підходи, що спираються на концепцію глобального інформаційного суспільства та ідею цифрового суверенітету держав. Це зумовлює потребу в універсальному та інтегрованому підході до аналізу кіберзагроз, адже вони переплітаються з політичними, економічними та соціальними процесами світової системи [9].

Мезорівень охоплює соціально-правові та організаційні механізми, де, за А. Тарасюком, ключову роль завжди відіграють норми міжнародного й національного права, багаторівнева культура кібербезпеки та державно-приватне партнерство у сфері критичної інфраструктури. На мікрорівні в центрі уваги перебуває людина як найуразливіший суб'єкт інформаційних правовідносин. З методологічного погляду, визначальними є принципи комплексності, варіативності та соціальної інклюзивності, що забезпечують можливість поєднання системного, ризикологічного, правового та сучасного конструктивістського аналізу кібербезпеки. Водночас системний аналіз, за А. Тарасюком, дозволяє ідентифікувати взаємозв'язки між природними, техногенними та соціополітичними процесами в кіберсередовищі й будувати нормативні алгоритми їхнього правового регулювання [18]. Ризикологічний підхід спрямовано на кількісне оцінювання й прогнозування кіберінцидентів з урахуванням транснаціональної природи різних загроз, а правовий – на гармонізацію національного законодавства з нормами міжнародного публічного права та «Будапештської конвенції», зокрема через уточнення категорій «стан захищеності», «кіберзагроза», а також «кіберзлочин» [2].

Конструктивістська перспектива пояснює, як сучасні держави шляхом кібердипломатії формують спільні смисли та норми поведінки, утверджуючи кібербезпеку як нову «третю ділянку» безпекового порядку, поряд із сушею та морем [9]. Окрему методологічну проблему становить термінологічна невизначеність. Як слушно акцентують О. Архипов і В. Бровко, відсутність уніфікованого понятійного апарату ускладнює порівняльні дослідження й розроблення узгоджених міжнародних стандартів [8]. Це зумовлює потребу у фасетному аналізі дефініцій кібербезпеки, кіберпростору та кіберзагроз, що дозволяє виділити інваріантні ознаки й уникнути семантичних викривлень. Таким чином, теоретико-методологічні засади дослідження кібербезпеки в міжнародних відносинах спираються на поєднання світоглядних і правових концепцій безпеки, міждисциплінарних методів системного та ризикового аналізу, а також конструктивістського розуміння нормотворчої ролі держав у кіберпросторі. Такий гнучкий підхід забезпечує наукову цілісність, дозволяє інтегрувати національні інтереси в архітектуру цифро-

вої безпеки та формулювати правові й політичні механізми нейтралізації кіберзагроз [18].

У законодавчому полі України, ключовим міжнародно-правовим орієнтиром у сфері кібербезпеки виступає Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, 2001 р.), ратифікована Верховною Радою України (ВРУ) Законом №2824-IV від 7 вересня 2005 р. із застереженнями та заявами. Для України вона набрала чинності 1 липня 2006 р. Сам факт ратифікації інтегрував національну правову систему до єдиного транскордонного механізму протидії кіберзагрозам, а також поклав на державу обов'язок криміналізувати незаконний доступ, перехоплення, втручання в дані й системи, комп'ютерне шахрайство та порнографічні злочини проти дітей, запровадити корпоративну відповідальність і процедурні інструменти збереження, вилучення та міжнародного обміну електронними доказами [12].

У практичному вимірі це означає, що слідчі органи України зобов'язані оперативно співпрацювати з цілодобовою контактною мережею 24/7, забезпечувати термінове збереження всіх трафікових даних, а також використовувати спрощені процедури транскордонного доступу до відкритих інформаційних ресурсів або даних, добровільно наданих їхнім власником. Конвенція передбачає механізм екстрадиції та взаємної правової допомоги, який діє незалежно від наявності двостороннього договору, що критично підсилює можливості Києва під час розслідування здійснених кібератак за умов глобальної безпекової турбулентності. Водночас ВРУ, залишивши застереження щодо окремих процесуальних статей, зберегла суверенне право обмежувати співпрацю лише тоді, коли вона суперечить основоположним інтересам держави, що забезпечує баланс між міжнародними зобов'язаннями й внутрішньою безпекою. Отже, через ратифікацію Будапештської конвенції українське законодавство отримало нормативну рамку, яка синхронізує внутрішню кримінально-процесуальну практику з новітніми європейськими стандартами і зміцнює міжнародне партнерство у сфері кібербезпеки, особливо актуальне в умовах поточної глобальної кризи безпеки [12].

Закон України «Про основні засади забезпечення кібербезпеки України» (№2163-VIII) у редакції від 20.04.2025 встановлює комплексну нормативно-правову базу для захисту життєво важливих інтересів громадян, суспільства та держави в кіберпросторі. Він визначає правові та організаційні засади державної політики в сфері кібербезпеки, окреслює повноваження ключових суб'єктів, механізми координації їхніх дій, встановлює принципи взаємодії державного та приватного секторів, а також інтегрує міжнародні стандарти та рекомендації ЄС і НАТО в національне законодавство. Визначення базових термінів у ст. 1 є фундаментальною частиною Закону. Поняття «кібер-

інцидент», «кібератака», «кіберзагроза» і «кіберзахист» визначаються з достатньою конкретністю, що дозволяє чітко розмежувати відповідальність суб'єктів у сфері реагування на подібні події.

Так, «кіберзахист» включає організаційні, правові, інженерно-технічні заходи, криптографічний та технічний захист інформації з метою протидії кіберзагрозам, забезпечення стійкості та конфіденційності інформаційних ресурсів. Відповідно до статей 4 і 5, об'єктами кібербезпеки є не тільки критична інфраструктура, але й конституційні права громадян, суспільний розвиток, суверенітет і територіальна цілісність Української держави. Закон передбачає систему державних та громадських суб'єктів, які залучаються до забезпечення кібербезпеки. Центральним органом, відповідальним за координацію та оперативне реагування, є Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України. Уповноваженим органом у сфері реалізації політики є Державна служба спеціального зв'язку та захисту інформації України, яка керує національною системою реагування на кіберінциденти (CERT-UA). Водночас ключовими механізмами забезпечення кібербезпеки, відповідно до ст. 8, є формування та адаптація державної політики згідно зі стандартами ЄС і НАТО, нормативне регулювання, проведення навчань для профільних фахівців, створення команд реагування на кіберінциденти (CSIRT), функціонування систем оцінювання стану кіберзахисту, криптографічного захисту та резервування державних інформаційних ресурсів.

Важливою інновацією є запровадження Національного центру резервування державних інформаційних ресурсів, що передбачає зберігання всіх резервних копій критично важливих даних для безперервного функціонування державних органів навіть під час кризових ситуацій чи воєнного стану. Стаття 9 деталізує організацію національної системи реагування на кіберінциденти, що складається з національної команди CERT-UA, галузевих і регіональних команд CSIRT, Центру кіберзахисту Національного банку (CSIRT-NBU), а також військового центру кіберзахисту Міністерства оборони (MIL. CERT-UA). Координацію оперативного реагування здійснює постійно діюча Об'єднана група реагування на кіберінциденти при Національному координаційному центрі кібербезпеки. Ця модель є цілісною та забезпечує як централізоване керівництво, так і децентралізоване галузеве та регіональне реагування. Стаття 9^1 визначає порядок обміну інформацією щодо кіберінцидентів через спеціальну платформу, підтримувану Держспецзв'язком. Власники об'єктів критичної інформаційної інфраструктури зобов'язані швидко надавати обов'язкові повідомлення про значні кіберінциденти, що забезпечує прозорість, своєчасність та ефективність реагування.

У ст. 10 передбачено взаємодію держави з приватним сектором, що включає обмін інформацією про кіберзагрози, спільні освітні програми, державно-приватні проєкти, залучення експертного середовища, а також підтримку волонтерських організацій. Це дозволяє забезпечити синергію між державними структурами та приватним сектором у реагуванні на кіберзагрози. Важливим аспектом є положення ст. 13, яка визначає джерела фінансування кібербезпеки, зокрема державні бюджети, власні кошти суб'єктів, міжнародну технічну допомогу. Це дозволяє забезпечити фінансову стабільність заходів із кіберзахисту. Стаття 14 передбачає активне міжнародне співробітництво України у сфері кібербезпеки, що включає двосторонні й багатосторонні угоди, участь у міжнародних навчаннях, а також узаємодію з міжнародними організаціями. Це забезпечує інтеграцію української системи кібербезпеки в глобальний контекст. Остання редакція Закону суттєво посилює контроль та відповідальність у сфері кіберзахисту. Стаття 15 передбачає регулярний незалежний аудит суб'єктів національної кібербезпеки з обов'язковим звітуванням перед вищими органами влади, що гарантує постійний моніторинг ефективності вжитих заходів [14].

Еволюція кібербезпеки як предмета міжнародного співробітництва характеризується системною трансформацією, що відображає перехід від розрізнених національних зусиль до створення комплексних міжнародних механізмів узаємодії, які координуються впливовими міжнародними організаціями. На початковому етапі кібербезпека розглядалася переважно як суто технічна та юридична проблема, що вирішувалась окремими державами у відповідь на поодинокі інциденти та загрози. Проте з часом кіберпростір, через свою безмежну природу та транснаціональний характер кіберзлочинів, виявився неможливим для ефективного управління виключно на національному рівні, що і стало рушієм до активізації міжнародної співпраці, вироблення спільних політик та якісної уніфікації регуляторних практик. Центральну роль у цьому процесі відіграє Міжнародний союз електрозв'язку (ITU) – спеціалізована агенція ООН, яка ініціювала розроблення Глобальної програми кібербезпеки (Global Cybersecurity Agenda). Ця програма сформувала системний підхід до міжнародного управління кібербезпекою, що базується на 5 ключових стратегічних стовпах: правовому, технічному, організаційному, кадровому розвитку та міжнародному співробітництві. Кожен із цих напрямів став базисом для міжнародної координації, посилення діалогу та стандартизації кібербезпекових практик [3].

У правовій площині сучасне міжнародне співробітництво значно еволюціонувало через спроби створення спільних нормативних рамок, спрямованих на боротьбу з кіберзлочинністю та усунення прогалин у юрисдикції.

Ключовими прикладами таких зусиль є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція 2001 р.), Конвенція Африканського Союзу про кібербезпеку та захист персональних даних (2014 р.), а також інші регіональні угоди. Вони створили передумови для транскордонної правової співпраці, гармонізації юридичних визначень кіберзлочинів та ефективної взаємодії правоохоронних органів. Технічний аспект еволюції міжнародної кібербезпеки яскраво представлений розвитком і поширенням команд швидкого реагування на комп'ютерні інциденти (CERT та CSIRT) [3].

Ці спеціалізовані структури стали ключовим механізмом як для оперативного реагування на кіберзагрози, так і для проактивного забезпечення інформаційної безпеки. Регіональні мережі на кшталт «Asia-Pacific CERT» (APCERT) та «Africa CERT» (AfricaCERT) продемонстрували високий рівень координації між країнами, дозволяючи швидко поширювати важливу інформацію про загрози та ефективно реагувати на інциденти в глобальному масштабі. З організаційної точки зору, помітною є тенденція до створення спеціалізованих державних органів та агенцій, що відповідають за кібербезпекову політику та координацію національних зусиль. Такі органи, як Федеральне бюро інформаційної безпеки Німеччини, Офіс з питань кібербезпеки Великої Британії та Міністерство науки, ІКТ і майбутнього планування Республіки Корея, стали центральними елементами управління кібербезпекою в національному та міжнародному масштабах. Кадровий розвиток також суттєво змінився: від поодиноких заходів до цілісних, стратегічних програм освіти та просвіти суспільства у сфері кібербезпеки. Такі ініціативи, як австралійська кампанія «Stay Smart Online», канадська програма «Get Cyber Safe» та американська кампанія «StaySafeOnline», свідчать про системні міжнародні зусилля з формування безпечних навичок користувачів та значного підвищення рівня загальної інформаційної безпеки населення. ITU підтримує такі програми, надаючи технічні інструменти для моніторингу та аналізу кіберзагроз (наприклад, HORNET та AWARE) [3].

Найбільшу трансформацію продемонстрував напрям міжнародної співпраці, що полягає у створенні та розширенні мереж обміну інформацією, публічно-приватних партнерств і багатосторонніх цільових угод. Яскравими прикладами цього є Міжнародна стратегія кіберзалучення Австралії, співпраця держав із такими організаціями, як ENISA (Агентство ЄС із питань мережевої та інформаційної безпеки), ОБСЄ, НАТО та низка регіональних і міждержавних конвенцій і домовленостей. Узаємодія держав у рамках цих структур дозволяє ефективніше координувати дії щодо запобігання кіберзагрозам та оперативно реагувати на спільні виклики. Порівняльний аналіз ОЕСР (OECD, 2012 р.) національних стратегій кібербезпеки в 10 країнах по-

казав, що попри певні відмінності у визначеннях та термінології країни мають спільні підходи до вирішення кіберзагроз, інтегруючи у свої стратегії всі 5 основних напрямів ITU.

У своїх рекомендаціях 2018 р. щодо розроблення національних стратегій кібербезпеки ITU також запропонував включити тематичні сфери управління ризиками, захисту критичної інфраструктури, нормативного регулювання, а також поглибленої міжнародної співпраці, що стало додатковим стимулом для формування більш ефективної системи міжнародного управління кібербезпекою [11]. Інституційна архітектура міжнародної взаємодії у сфері кібербезпеки є багаторівневою та включає широкий спектр суб'єктів – міжурядові організації, спеціалізовані агентства, координаційні структури, а також багатосторонні ініціативи та платформи, що забезпечують співпрацю держав, недержавних акторів і приватного сектору. Основна мета такої архітектури полягає в координації дій, уніфікації стандартів, обміні інформацією та нарощуванні спільного потенціалу для протидії глобальним кіберзагрозам сучасності.

Одним із центральних елементів цієї архітектури є Міжнародний союз електрозв'язку (ITU), який ініціював створення Глобального порядку денного з кібербезпеки, як рамки для зміцнення безпеки та довіри в інформаційному суспільстві. Цей документ окреслює п'ять основних напрямів міжнародної взаємодії: правовий (гармонізація законодавства), технічний (реагування на інциденти та розбудова CERT/CSIRT), організаційний (стале інституційне забезпечення), освітньо-тренінговий (підвищення спроможності) і кооераційний (інформаційний обмін, партнерства). На регіональному рівні важливу роль відіграють організації, як-от Європейський Союз, зокрема через Агентство ЄС з кібербезпеки (ENISA), що здійснює координацію заходів безпеки, формує політику та підтримує держави-члени в реагуванні на кіберінциденти. ЄС також розвиває власну нормативну базу, як-от Директива NIS2 щодо безпеки мереж та інформаційних систем, що вимагає від країнчленів створення національних CSIRT, визначення операторів критичних послуг і забезпечення міждержавного обміну інформацією. На рівні НАТО інституційну взаємодію забезпечує Комітет з кібероборони, Кооперативний центр передового досвіду з кібероборони в Естонії (CCDCOE) та спеціалізовані підрозділи в рамках Спільної безпекової політики. НАТО реалізує концепцію колективної безпеки в кіберпросторі, що передбачає підтримку партнерів, зокрема України, через спільні тренінги, обмін даними, технічну допомогу та інтеграцію в навчальні програми Альянсу [3].

Україна, як активний учасник міжнародного кіберпростору, поступово вбудовується в цю архітектуру. Вона є учасницею спільних проєктів

із НАТО, ООН, ОБСЄ, FIRST, а також двосторонніх форматів зі США, Великою Британією, Ізраїлем та іншими технологічно розвинутими державами. Законодавчо закріплено можливість міжнародного співробітництва у сфері кібербезпеки, а також взаємодії з міжнародними організаціями з питань обміну інформацією, спільного розслідування інцидентів та напрацювання стандартів. Особливе значення мають багатосторонні цільові угоди, такі як Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), яка встановлює нормативно-правові основи транскордонної співпраці в сфері протидії кіберзлочинності [5].

Інші приклади – Африканська конвенція з кібербезпеки та захисту персональних даних, Арабська конвенція з протидії ІТ-злочинам тощо. Такі угоди закладають міжнародно-правові механізми взаємодії, обміну доказами, екстрадиції та спільного розслідування кіберінцидентів [6]. Також у межах інституційної архітектури важливу роль відіграють інформаційно-аналітичні платформи, як-от MISP (Malware Information Sharing Platform) та ініціативи приватного сектору, серед яких програмні рішення типу Bug Bounty. Вони розширюють рамки взаємодії до горизонтального рівня, де приватні компанії, дослідники безпеки та уряди завжди виступають партнерами у виявленні вразливостей, обміні індикаторами компрометації та відпрацюванні сценаріїв реагування. Узагальнюючи, інституційна архітектура міжнародної взаємодії у сфері кібербезпеки є динамічною, поліцентричною системою, що поєднує нормативну, технічну, операційну та освітню компоненти. Її ефективність зумовлена готовністю всіх країн до інтеграції, забезпечення прозорості у взаємодії, спільного розроблення рішень і стандартів, а також інституційної сталості та гнучкості у відповідь на новітні виклики цифрової епохи.

У сучасному цифровому середовищі кібербезпека стала ключовим елементом національної безпеки, особливо в контексті зростання загроз із боку державних акторів. Росія активно використовує кіберінструменти для впливу на політичні процеси в інших країнах, що підтверджується низкою інцидентів у континентальній Європі. У листопаді 2024 р. Румунія стала об'єктом такої масштабної кіберкампанії, спрямованої на втручання у президентські вибори. Наприклад, правий кандидат К. Георґеску несподівано здобув перемогу в першому турі виборів, що викликало підозри щодо можливого зовнішнього впливу. Розслідування виявило, що кампанія К. Георґеску отримала значну підтримку через соціальні мережі, особливо TikTok, де його повідомлення активно поширювалися за допомогою ботів і фальшивих акаунтів. Ці дії були лише частиною ширшої російської стратегії гібридної війни, спрямованої на дестабілізацію демократичних процесів у країнах Європи.

Румунський Конституційний суд анулював результати цих виборів, посилаючись на докази іноземного втручання, включаючи кібернапади на виборчі системи і незаконне фінансування кампанії самого К. Георгеску. Це рішення викликало кризу та масові протести в країні [4].

У травні 2024 р. уряд Німеччини звинуватив Росію у здійсненні кібератак на правлячу Соціал-демократичну партію Німеччини (SPD), а також на оборонні та аерокосмічні компанії. Група APT28, пов'язана з Головним управлінням Генерального штабу ЗС РФ, використовувала вразливість у Microsoft Outlook для доступу до електронної пошти та інших конфіденційних даних. Ці дії були розцінені німецьким урядом як серйозне втручання в демократичні структури країни [13]. У 2023 р. група NoName057(16), що пов'язана з Росією, здійснила DDoS-атаки на вебсайти кількох голландських прів. Ці атаки були спрямовані на дестабілізацію критичної інфраструктури країни та виявили вразливості в системах кібербезпеки [19]. У 2024 р. група APT28 провела кіберрозвідки проти чеських урядових установ, використовуючи вразливість у Microsoft Outlook для отримання доступу до конфіденційної інформації. Ці дії були частиною операції росіян з кіберрозвідки, спрямованої на збір інформації про політичні та економічні процеси в країні [16]. Такі приклади демонструють, що державні кібератаки стали системним інструментом у геополітичному протистоянні Заходу та Москви. Міжнародна інституційна архітектура кібербезпеки повинна адаптуватися до цих викликів, забезпечуючи координацію, обмін інформацією та спільну відповідь на загрози. Демократичні країни повинні об'єднати зусилля для захисту своїх інститутів від втручання та забезпечення цілісності виборчих процесів.

Еволюція кібербезпеки як предмета міжнародної взаємодії розпочалася з усвідомлення неможливості ефективної протидії кіберзагрозам в умовах ізольованої національної політики. Визначальну роль у формуванні інституційної архітектури цієї взаємодії відіграли такі організації, як Міжнародний союз електрозв'язку (ITU), який ініціював Глобальну програму з кібербезпеки (Global Cybersecurity Agenda), що передбачає п'ять стратегічних напрямів: правовий, технічний, організаційний, навчальний та кооперaційний. Ці напрями гнучко охоплюють гармонізацію законодавства, створення CERT / CSIRT-структур, різні національні стратегії кіберзахисту, системи підготовки кадрів та міжвідомчу координацію як усередині держав, так і між ними.

У межах ЄС ключовими інституціями, що забезпечують координацію та реагування на кіберзагрози, виступають ENISA, CERT-EU та EU-CyCLONe. Згідно з аналітичною статтею С. Савчука (2024 р.), саме завдяки цим структурам було закладено багаторівневу модель цифрової безпеки, яка інтегрує цивільний, військовий та приватний сектори в єдину мережу реагу-

вання на кіберінциденти. Ця система посилюється впровадженням директив NIS/NIS2, Закону про кібербезпеку та Закону про кіберсолідарність, які забезпечують нормативне підґрунтя для обов'язкової міждержавної співпраці, обміну інформацією та спільних навчань. У сучасному світі така координація стає критично важливою у світлі численних атак, зокрема з боку Російської Федерації (РФ), Китайської Народної Республіки (КНР) та Північної Кореї.

Прикладом транснаціонального кібервтручання є російські спроби вплинути на вибори в Румунії у 2024 р., які були частиною ширшої стратегії дестабілізації через втручання в демократичні процеси країн ЄС. Як зазначає Politico, румунська влада у співпраці з CERT-RO та EU-CyCLONe змогла локалізувати спроби втручання через поширення різних фейкових новин і використання ботмереж на платформах соціальних медіа, контрольованих з Росії. Іншим показовим прикладом є багаторазові атаки з боку Північної Кореї на фінансові установи в країнах Південно-Східної Азії та в США, що мають на меті не лише політичну дестабілізацію, але й безпосереднє фінансування режиму через викрадення криптовалюти. Ці атаки часто здійснюються угрупованням Lazarus Group, яке за оцінками аналітиків ENISA, використовує розгалужені інструменти соціальної інженерії, zero-day-експлойти та фішингові операції з високим рівнем адаптації до мовних і культурних контекстів жертв. Китай теж систематично використовує APT-групи, зокрема APT10 та APT41, для здійснення довгострокового кібершпигунства проти інфраструктурних об'єктів і науково-дослідних установ. У 2023 р. було зафіксовано інцидент, пов'язаний із проникненням у мережі Міністерства оборони Франції, при якому було скомпрометовано внутрішню документацію, що стосувалася співпраці в рамках PESCO. У відповідь на цей інцидент, EU-CyCLONe координував міждержавне розслідування та поширив технічні рекомендації на основі спільного аналізу CERT-EU та ENISA.

Тож кібербезпека стала не лише технічним чи юридичним завданням, а передусім інституційною формою реалізації міжнародної безпеки. Вона включає вертикальні й горизонтальні зв'язки між державами, агенціями, приватним сектором і науковою спільнотою. Як демонструє ЄС, лише інтегрована та координаційно підсилена модель сповна здатна протистояти складним асиметричним кіберзагрозам у глобальному просторі [14].

Формування глобального режиму кібербезпеки набуває особливої актуальності у зв'язку з глибокими трансформаціями, що відбуваються у сфері міжнародної безпеки, політики та технологій. На тлі стрімкої цифровізації державного управління, економіки, оборони та приватного сектора, питання розроблення й упровадження спільних глобальних норм, стандартів і ме-

ханізмів реагування на кіберзагрози стає необхідною умовою стабільності й довіри у міжнародному співтоваристві. Аналіз матеріалів В. Гавриляка свідчить про те, що європейська кібербезпекова стратегія, зокрема в рамках «Цифрового десятиліття», розглядає питання створення глобального / відкритого, стабільного та безпечного кіберпростору як ключового напряму розвитку безпекової політики ЄС. Це передбачає розбудову національних кіберспроможностей, інтеграцію стандартів у союзні системи, створення спільних інституцій типу Спільного кіберпідрозділу (Joint Cyber Unit), а також реалізацію принципу «кібербезпека за замовчуванням» у цифрових інфраструктурах [10].

У глобальному вимірі перспективи формування режиму кібербезпеки залежать від здатності держав досягти консенсусу щодо ключових принципів кіберповедінки: суверенітету в кіберпросторі, недопущення агресивного використання кіберзасобів, прозорості дій, взаємної відповідальності за кібератаки, а також взаємного визнання інцидентів кібертероризму. Таке правове поле має ґрунтуватися на міжнародному праві, зокрема на принципах ООН щодо поведінки держав у кіберпросторі. Як зазначено в дослідженні О. Семененка та колективу, центральними викликами для глобального режиму є не лише технічна складність реагування на транскордонні атаки, а й брак узгоджених механізмів ідентифікації винних акторів, що унеможливлює оперативне введення санкцій або відповідних заходів без шкоди для міждержавної співпраці. Спроби створити глобальний режим кібербезпеки стикаються з системною конкуренцією між моделями цифрового суверенітету.

Умовно можна виділити ліберальну модель (ЄС, США), яка наголошує на відкритості, інклюзивності та правових гарантіях захисту даних, і авторитарну модель (Китай, РФ), що акцентує на контролі, цензурі та «націоналізації інтернету». Ці моделі відображають не лише технічні чи політичні підходи, але й концептуальні уявлення про функціонування цифрового світу. Така дихотомія унеможливлює уніфікацію нормативного поля і гальмує процес ратифікації спільних угод, як-от Будапештської конвенції про кіберзлочинність, яку Росія категорично не визнає.

Однак створення функціонального глобального режиму кібербезпеки можливе за умови послідовної інтеграції регіональних ініціатив, таких як Стратегія кібербезпеки ЄС, зусиль ООН та спеціалізованих агенцій, як-от ITU. Ключову роль тут відіграватиме впровадження спільних механізмів сертифікації кіберзахисту, обміну вкрай важливою інформацією між національними CSIRT / CERT структурами, розвиток систем раннього попередження

та створення міжнародних груп швидкого реагування. Україна в цьому контексті виступає як регіональний хаб з унікальним досвідом гібридної кібервійни, зокрема протистояння агресії РФ, що включає сотні інцидентів – від атак на енергетичні системи (BlackEnergy, Industroyer) до впливу на вибори, інформаційні операції, DDoS-атаки на урядові сайти та спроби інфільтрації в систему оборонного управління [15].

Отже, перспективи формування глобального режиму кібербезпеки пов'язано із запровадженням гнучкої моделі багаторівневої взаємодії, що включає технічну, правову, організаційну та політичну інтеграцію зусиль ключових міжнародних акторів. Успіх цієї моделі залежить від створення механізмів довіри, підтвердження відповідальності за атаки та розроблення єдиної нормативної рамки, прийнятної для більшості цифрових держав світу.

У контексті формування глобального режиму кібербезпеки найкращі практики, викладені у звіті «Кращі практики управління кібербезпекою», підготовленому в межах проєкту ЄС-ПРООН, ілюструють еволюційні напрями, які можуть стати основою для універсалізації підходів до регулювання цифрових загроз і посилення стійкості інформаційного простору на глобальному рівні. Аналіз прикладів таких країн, як Велика Британія, Литва, Франція, Іспанія, США, Ізраїль і Нідерланди, дозволяє виділити ключові напрями, що становлять фундамент потенційного міжнародного режиму кібербезпеки. У всіх країнах, які є предметом аналізу, спостерігається високий рівень правової визначеності кіберзагроз, розвинені інституційні моделі реагування на кіберінциденти, а також активне міжвідомче й міжсекторальне співробітництво. Зокрема, у Великій Британії ключовими є правові механізми (наприклад Закон про зловживання комп'ютером), а також інституційна спроможність, що проявилася в успішному закритті понад 4 млн DDoS-атак у результаті міжнародної операції [1].

У Литві стратегія кібербезпеки включає заходи протидії деструктивному впливу РФ у кіберпросторі та чітке визначення обов'язків усіх суб'єктів, що відповідають за національну безпеку у сфері ІКТ. У США створено систему національного партнерства на базі CERT, активізовано державну підтримку приватного сектору та вдосконалено системи обміну інформацією. Окрему увагу слід звернути на діяльність Ізраїлю, який зазнав численних кібератак, але розвинув комплексну структуру кіберзахисту, включаючи ізраїльську модель CERT-IL та Інститут національного кіберуправління (INCB). Подібна структура з чітко визначеною вертикаллю відповідальності, дина-

мічною системою оцінки всіх ризиків і державно-приватним партнерством може бути прототипом глобальної моделі [1].

Інституційна архітектура таких країн вирізняється багаторівневою системою управління, що охоплює як національні урядові органи, так і спеціалізовані агентства, CERT, правоохоронні структури, органи захисту персональних даних, а також важливі освітні й наукові установи. Значущим елементом є створення правового підґрунтя для функціонування цієї архітектури, як-от у Литві, де Закон про кібербезпеку детально регламентує функції кожного учасника національної системи безпеки в цифровому просторі. На цьому тлі актуалізується необхідність посилення міжнародної координації. Формування глобального режиму кібербезпеки можливе через консолідацію національних стратегій, які існують, за допомогою, наприклад, таких інституцій, як МСЕ, Європейська комісія, ENISA, а також укладення правових угод типу Будапештської конвенції. При цьому кращі практики, напрацьовані згаданими державами, слугують взірцем для країн, що ще не мають сталої системи кібербезпеки.

У стратегічному вимірі створення такого режиму передбачає уніфікацію стандартів безпеки, обмін інцидентною аналітикою в реальному часі, гармонізацію кримінального та адміністративного законодавства у сфері боротьби з кіберзлочинністю, інтеграцію наявних регіональних платформ CERT / CSIRT, а також запровадження механізмів незалежного аудиту цифрової інфраструктури. Застосування кращих практик має відбуватися в умовах поваги до національного суверенітету, але водночас з урахуванням необхідності підвищення відповідальності національних держав за хостинг або спонсорування кібероперацій, що спрямовані на дестабілізацію інших країн. Перспективи формування глобального режиму кібербезпеки полягають у поетапній адаптації ефективних механізмів управління, які вже апробовані в практиках провідних країн, до міжнародного правового і координаційного рівня. Такий підхід сприятиме зменшенню кіберризиків, зміцненню довіри між багатьма державами, а також формуванню нового цифрового ландшафту, де поняття «безпека» стане основоположною характеристикою глобального інформаційного простору.

Висновки. У процесі еволюції міжнародного співробітництва у сфері кібербезпеки окреслилася принципово нова парадигма реагування на глобальні безпекові виклики цифрової епохи. Аналіз теоретичних засад, міжнародних практик, інституційної архітектури, нормативного поля та емпіричних прикладів дозволяє сформулювати певні висновки. По-перше, кібербезпека остаточно трансформувалася з вузькоспеціалізованої сфери

в один із ключових вимірів глобальної безпеки, що охоплює як національні стратегії, так і широку міждержавну взаємодію. По-друге, сучасний стан міжнародного правового регулювання не відповідає інтенсивності та складності кіберзагроз, що вимагає термінової уніфікації правових категорій, визначення відповідальності та розроблення міжнародно визнаних норм поведінки в кіберпросторі. По-третє, у структурному вимірі ефективна протидія кіберзагрозам передбачає багаторівневу, скоординовану модель, що включає державні органи, міжурядові організації, приватний сектор і дослідницьке середовище. По-четверте, на прикладі України, Румунії, Німеччини та інших країн Європи продемонстровано системність і транснаціональність ворожих кіберкампаній, зокрема з боку РФ, що підтверджує необхідність розроблення спільної європейської політики кіберпротидії, яка виходить за межі виключно технічного реагування. Узагальнюючи, можна стверджувати, що кібербезпека перестає бути виключно національною проблемою та стає спільною справою міжнародної спільноти, що вимагає формування нового глобального режиму з відповідними інституційними, правовими та організаційними механізмами.

З огляду на вищенаведене доцільними є такі **пропозиції**:

1. Ініціювати розроблення глобального кодексу новітньої кібернетичної поведінки держав на базі ООН із включенням норм щодо заборони втручання у виборчі процеси, атак на критичну інфраструктуру та використання кіберзасобів як інструменту гібридної війни.

2. Розширити юрисдикцію міжнародних організацій (ENISA, ITU, EU-CyCLONe) щодо координації розслідувань кібератак та обміну індикаторами компрометації між державами-членами.

3. Удосконалити механізми багаторівневої взаємодії між державами, у тому числі шляхом створення спільних CERT / CSIRT-груп із транскордонними повноваженнями на основі згоди сторін.

4. Запровадити обов'язкові незалежні (комплексні) аудити цифрової інфраструктури для країн, які беруть участь у спільних проєктах ЄС, НАТО, або програм технічної допомоги з метою забезпечення відповідності мінімальним стандартам кіберзахисту.

5. Розвивати програми кіберосвіти та обізнаності серед широкої аудиторії, включаючи державних службовців, журналістів, представників громадянського суспільства та студентів.

6. Забезпечити фінансову підтримку кіберреформ у країнах, що розвиваються за рахунок консолідованих фондів цифрової безпеки ЄС, Світового банку або ПРООН, що дозволить зменшити цифрову нерівність у кіберзахисті.

7. У межах існуючої європейської інтеграції України продовжити гармонізацію національного законодавства з Директивою NIS2, зокрема в частині визначення операторів критичних послуг, організації обміну інцидентною інформацією та розширення повноважень CSIRT-UA.

Реалізація зазначених заходів дозволить створити цілісну систему глобального управління кібербезпекою, яка буде здатною ефективно нейтралізувати новітні загрози, забезпечити суверенітет держав у цифровому середовищі та сприяти формуванню безпечного, відкритого й надійного глобального інформаційного порядку.

ЛІТЕРАТУРА

1. Кращі практики управління кібербезпекою : оглядовий звіт / підготов. Комітетом із питань цифрової трансформації ВР України в межах Проєкту ЄС-ПРООН з парламентської реформи. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf (дата звернення: 24.04.2025).
2. Baran M. V. Principles of legal regulation of the institute of information security. *Uzhhorod National University Herald. Series: Law*. 2021. Vol. 66. P. 129–134. doi: https://doi.org/10.24144/2307–3322.2021.66.22.
3. Cybercrime Module 8. Key Issues: International Cooperation on Cybersecurity Matters. *United Nations Office on Drugs and Crime*. URL: https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international -cooperation-on-cybersecurity-matters.html (Last accessed: 24.04.2025).
4. Rainsford S. Romania hit by major election influence campaign and Russian cyber-attacks. *BBC Home – Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio*. 2024. 5 Dec. URL: https://www.bbc.com/news/articles/cgq18w507dko (Last accessed: 24.04.2025).
5. Slyvka M. M. International cooperation in the sphere of ensuring cyber security of Ukraine. *Juridical scientific and electronic journal*. 2022. No. 10. P. 489–491. doi: https://doi.org/10.32782/2524-0374/2022-10/121.
6. Tietievin M. S. Experience of Ukraine in the field of international cooperation in the field of Cyber Security. *Uzhhorod National University Herald. Series: Law*. 2024. Vol. 3, No. 82. P. 263–266. doi: https://doi.org/10.24144/2307-3322.2024.82.3.41 (Last accessed: 24.04.2025).
7. *Актуальні проблеми управління інформаційною безпекою держави* : матеріали наук.-практ. конф. (Київ, 15 травня 2020 р.). Київ, 2020. 363 с. URL: file:///C:/Users/E546/Downloads/Zbirnik2020.pdf (дата звернення: 24.04.2025).
8. Архипов О. Є., Бровко В. Д. Кібербезпека – виникнення, формування, розуміння. *Інформаційна безпека людини, суспільства, держави*. 2017. №2 (22). С. 6–14. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_

DOWNLOAD=1&Image_file_name=PDF/iblsd_2017_2_3.pdf (дата звернення: 24.04.2025).
9. Веселова Л. Ю. Методологічні засади пізнання кібернетичної безпеки. *Південноукраїнський правничий часопис*. 2019. Т. 2, № 4. С. 162–165. doi: https://doi.org/10.32850/sulj.2019.4.2.35.
10. Гавриляк В. Б. Стратегія кібербезпеки ЄС на цифрове десятиліття: перспективи для України. *Вісник Національної академії державного управління при Президентові України. Серія: Державне управління*. 2021. № 1. С. 46–52. URL: http://nbuv.gov.ua/UJRN/ vnaddy_2021_1_8 (дата звернення: 24.04.2025).
11. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва. Київ : НІСД, 2014. 328 с. URL: https://www.niss.gov.ua/sites/ default/files/2015-02/Dubov_mon-89e8e.pdf (дата звернення: 24.04.2025).
12. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/ show/994_575 (дата звернення: 24.04.2025).
13. Мельник Р. Німеччина звинуватила Росію в кібератаці торік і пригрозила наслідками. *Детектор Медіа*. 2024. 3 трав. URL: https://detector.media/infospace/article/226339/2024-05-03-nimechchyna-zvynuvatyla-rosiyu-v-kiberatatsi-torik-i-prygrozyla-naslidkamy/ (дата звернення: 24.04.2025).
14. Про основні засади забезпечення кібербезпеки України : Закон України № 2163-VIII від 05.10.2017 : станом на 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 24.04.2025).
15. Рекомендації та перспективи впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері безпеки та оборони України / Семененко О., Островський С., Бондаренко М. та ін. *Social Development and Security*. 2023. Т. 13, № 4. С. 63–80. doi: https://doi.org/10.33445/sds.2023.13.4.6 (дата звернення: 24.04.2025).
16. Розвідка Нідерландів: Росія активізувала гібридні атаки проти Європи. *Інститут масової інформації*. 2025. 22 квіт. URL: https://imi.org.ua/news/rozvidka-niderlandiv-rosiya-aktyvizuvala-gibrydni-ataky-proty-yevropy-i67824 (дата звернення: 24.04.2025).
17. Савчук С. О. Виклики та можливості інтеграції України в систему кібербезпеки ЄС. *Економіка, управління та адміністрування*. 2024. № 2 (108). С. 198–203. doi: https://doi.org/10.26642/ema-2024-2(108)-198-203 (дата звернення: 24.04.2025).
18. Тарасюк А. В. Теоретико-правові основи забезпечення кібербезпеки України : дис. … д-ра юрид. наук : 12.00.077. Київ, 2021. 461 с. URL: https://ippi.org.ua/sites/default/files/disertaciya_0.pdf (дата звернення: 24.04.2025).
19. Чехія викликала посла Росії через кібератаки на уряд та критичну інфраструктуру. *Європейська правда*. 2024. 6 трав. URL: https://www.eurointegration.com.ua/news/2024/05/6/7185356/ (дата звернення: 24.04.2025).
20. Федонюк С. В. Міжнародні аспекти безпеки кіберпростору. Луцьк : Вежа-Друк, 2022. 178 с. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/20718/1/Mizhnar_asp_bezp_kiberprostoru.pdf (дата звернення: 21.05.2025).

21. Шемчук В. В. Основні напрями міжнародного співробітництва у сфері кібербезпеки. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. 2018. Т. 29, № 68. С. 125–130. URL: https://www.juris.vernadskyjournals.in.ua/journals/2018/2_2018/24.pdf (дата звернення: 21.05.2025).

REFERENCES

1. Komitet z pytan′ tsyfrovoi transformatsii Verkhovnoi Rady Ukrainy. (2025.). *Kraschi praktyky upravlinnia kiberbezpekoiu: Ohliadovyi zvit*. April 24, 2025 URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf [in Ukrainian].
2. Baran, M. V. (2021). Principles of legal regulation of the institute of information security. *Uzhhorod National University Herald. Series: Law*, *66, 129–134.* doi: https://doi.org/10.24144/2307-3322.2021.66.22
3. United Nations Office on Drugs and Crime. (2025). *Cybercrime Module 8 Key Issues: International Cooperation on Cybersecurity Matters*. 24 Apr. URL: https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html
4. Rainsford, S. (2025). Romania hit by major election influence campaign and Russian cyber-attacks. *BBC News*. 24 Apr. URL: https://www.bbc.com/news/articles/cgq18w507dko
5. Slyvka, M. M. (2022). International cooperation in the sphere of ensuring cyber security of Ukraine. *Juridical Scientific and Electronic Journal*, *10, 489–491.* doi: https://doi.org/10.32782/2524-0374/2022-10/121
6. Tietievin, M. S. (2024). Experience of Ukraine in the field of international cooperation in the field of Cyber Security. *Uzhhorod National University Herald. Series: Law*, *82(3), 263–26*6. doi: https://doi.org/10.24144/2307-3322.2024.82.3.41
7. *Aktual'ni problemy upravlinnia informatsiinoi bezpeky derzhavy* (2020): proceedings of the Scientific and Practical Conference. Kyiv. URL: file:///C:/Users/E546/Downloads/Zbirnik2020.pdf [in Ukrainian].
8. Arkhipov, O. Ye., Brovko, V. D. (2017). Kiberbezpeka – vynykannia, formuvannia, rozuminnia. *Informatsiina bezpeka liudyny, suspil'stva, derzhavy – Information security of individuals, society, and the state*, *2(22), 6–14.* http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/iblsd_2017_2_3.pdf [in Ukrainian].
9. Veselova, L. Yu. (2019). Metodolohiyni zasady piznannia kibernetychnoi bezpeky. *Pivdennoukrainskyi pravnychyi chasopys – South Ukrainian Law Journal*, *2(4), 162–165.* doi: https://doi.org/10.32850/sulj.2019.4.2.35 [in Ukrainian].
10. Havryliak, V. B. (2021). Stratehiia kiberbezpek y ES na tsyfrove desiatylittia: perspektyvy dlia Ukrainy. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry*

Prezydentovi Ukrainy. Seriia: Derzhavne upravlinnia – Bulletin of the National Academy of Public Administration under the President of Ukraine. Series: Public Administration, *1, 46–52.* http://nbuv.gov.ua/UJRN/vnaddy_2021_1_8 [in Ukrainian].

11. Dubov, D. V. (2014). Kiberprostir yak novyi vymir heopolitychnoho supernytstva. Kyiv: NISD. URL: https://www.niss.gov.ua/sites/default/files/2015–02/Dubov_mon-89e8e.pdf
12. Konventsiia pro kiberzlochynnist′. (2005). *Rada Yevropy*. *vid 23.11.2001* (stanom na 7 veres. 2005 r.). URL: https://zakon.rada.gov.ua/laws/show/994_575 [in Ukrainian].
13. Melnyk, R. (2024). Nimechchyna zvynuvatyla Rosiiu v kiberatatsi toryk i prygrozhela naslidkamy. *Detektor Media – Detector Media*. *24, Apr.* URL: https://detector.media/infospace/article/226339/2024-05-03-nimechchyna-zvynuvatyla-rosiyu-v-kiberatatsi-torik-i-prygrozyla-naslidkamy/ [in Ukrainian].
14. Verkhovna Rada Ukrainy. (2017). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy* : Zakon Ukrainy vid 05.10.2017 №2163-VIII (stanom na 20 kvit. 2025 r.). URL: https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].
15. Semenenko, O., Ostrovskyi, S., Bondarenko, M., Vovk, Y., Kutsenko, D. Rekomendatsii ta perspektyvy vprovadzhennia dosvidu inozemnykh derzhav v systemu formuvannia henezyisu rozvytku kibertekhnolohii u sferi bezpeky ta oborony Ukrainy. *Social Development and Security*, *13 (4), 63–80.* doi: https://doi.org/10.33445/sds.2023.13.4.6 [in Ukrainian].
16. Instytut masovoi informatsii. (2025). Rozvidka Niderlandiv: Rosiia aktyvizuvala hibrydni ataky proty Yevropy. *Instytut masovoi informatsii – Institute of Mass Information*. URL: https://imi.org.ua/news/rozvidka-niderlandiv-rosiya-aktyvizuvala-gibrydni-ataky-proty-yevropy-i67824 [in Ukrainian].
17. Savchuk, S. O. (2024). Vyklyky ta mozhlyvosti intehratsii Ukrainy v systemu kiberbezpeky ES. *Ekonomika, upravlinnia ta administruvannia – Economics, Management and Administration*, *2(108), 198–203.* doi: https://doi.org/10.26642/ema-2024-2%28108%29-198-203 [in Ukrainian].
18. Tarasiuk, A. V. (2021). Teoretyko-pravovi osnovy zabezpechennia kiberbezpeky Ukrainy: Doctor's thesis. Kyiv: IPPI. URL: https://ippi.org.ua/sites/default/files/disertaciya_0.pdf [in Ukrainian].
19. Chekhiia vyklikala posla Rosii cherez kiberataky na uriad ta krytychni infrastruktury. (2024). *Yevropeiska pravda – European truth*. 6 May. URL: https://www.eurointegration.com.ua/news/2024/05/6/7185356/ [in Ukrainian].
20. Fedoniuk, S. V. (2022). Mizhnarodni aspekty bezpeky kiberprostoru. Lutsk: Vezha-Druk. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/20718/1/Mizhnar_asp_bezp_kiberprostoru.pdf [in Ukrainian].
21. Shemchuk, V. V. (2018). Osnovni napriamy mizhnarodnoho spivrobitnytstva u sferi kiberbezpeky. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia: Yurydychni nauky – Scientific notes of the V. I. Vernadsky Tavrichesky National University. Series: Legal Sciences, 29(68), 125–130.* URL: https://www.juris.vernadskyjournals.in.ua/journals/2018/2_2018/24.pdf [in Ukrainian].

Vivchar Inna Volodymyrivna, Candidate of Political Sciences, Associate Professor of the Department of Political Science and International Relations, Rivne State University for the Humanities, Ukraine

Postel'zhuk Oleksandr Petrovich*, Candidate of Historical Sciences*, Associate Professor of the Department of Political Science and International Relations, Rivne State University for the Humanities, Ukraine

Valiukh Lyudmila Ivanivna, Candidate of Historical Sciences, Associate Professor of the Department of Political Science and International Relations, Rivne State Humanitarian University, Ukraine

CYBERSECURITY AS A SPHERE OF INTERNATIONAL COOPERATION DURING THE GLOBAL SECURITY CRISIS

The article examines cybersecurity as a key component of international cooperation amid a global security crisis. It analyzes the transformation of cyber threats into a factor of strategic instability and emphasizes the need to establish a global cybersecurity regime. The study explores legal, technical, and institutional dimensions of cyber incident response, the role of international organizations (ITU, ENISA, NATO), and European initiatives (NIS2, CERT-EU). Particular attention is given to Ukraine's involvement in international cybersecurity mechanisms, highlighting the importance of harmonizing regulatory approaches, strengthening national cyber capacities, and enhancing interstate coordination. Cybersecurity is conceptualized as a global public good requiring multilevel governance and political solidarity.

Keywords: *cybersecurity, international cooperation, cyberattacks, global security, institutional architecture, cyber threats, digital sovereignty.*