УДК 35.078.3:004.056
DOI: https://doi.org/10.31470/2786-6246-2026-15-79-88

Пасічник Василь, кандидат політичних наук, доктор наук з державного управління, доцент, доцент кафедри публічного врядування Інституту адміністрування, державного управління та професійного розвитку Національного університету «Львівська політехніка»

Pasichnyk Vasyl, Candidate of Political Science, Doctor of Public Administration, Associate Professor, Associate Professor of the Department of Public Governance of Institute of Administration, Public Administration and Professional Development at Lviv Polytechnic National University

ORCID ID: https://orcid.org/0000-0002-2447-2374

Недошитко Ангеліна, студентка спеціальності D4 «Публічне управління та адміністрування» ННІ Адміністрування, державного управління та професійного розвитку Національного університету «Львівська політехніка»

Nedoshytko Anhelina, student of specialty D4 «Public Management and Administration» of Institute of Public Administration, Governance and Professional Development at Lviv Polytechnic National University

ORCID ID: https://orcid.org/0000-0001-9874-6182

ІНСТИТУЦІЙНІ МЕХАНІЗМИ КІБЕРБЕЗПЕКИ: ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРАКТИК УКРАЇНИ ТА КРАЇН НАТО

INSTITUTIONAL CYBERSECURITY MECHANISMS: COMPARATIVE ANALYSIS OF THE PRACTICES OF UKRAINE AND NATO COUNTRIES

Анотація. У статті досліджено інституційні механізми кібербезпеки України та країн НАТО в контексті забезпечення національної безпеки в умовах гібридних загроз. Актуальність теми зумовлена зростанням кількості та складності кібератак, що перетворюються на стратегічний інструмент впливу на державне управління та критичну інфраструктуру. Для України, яка перебуває у стані збройної агресії з боку російської федерації, кіберпростір став важливою складовою сучасної війни. У цьому контексті актуальним постає створення ефективної системи інституційного управління кіберзахистом, що забезпечує координацію, аналітику та оперативне реагування.

Метою статті є порівняльний аналіз інституційних механізмів кібербезпеки України та країн НАТО, з акцентом на діяльності Національного координаційного центру кібербезпеки при РНБО України (НКЦК) та NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) у Таллінні. Використано системний і порівняльно-аналітичний підходи для виявлення структурних подібностей і відмінностей між моделями управління кібербезпекою, а також для узагальнення натівських практик міжвідомчої координації, розвитку аналітичної спроможності, проведення навчань Locked Shields та застосування підходу «whole-of-society».

Результати дослідження свідчать, що Україна поступово наближається до стандартів НАТО, однак система кібербезпеки ще потребує інституційного зміцнення, сталого фінансування та розвитку кадрового потенціалу. Натомість модель НАТО, представлена CCDCOE, відзначається

ISSN 2786-6246 (print)
ISSN 2786-9091 (online)

*Corresponding author

комплексністю, високим рівнем координації та практичним спрямуванням. Запропоновано рекомендації щодо поглиблення співпраці України з CCDCOE, створення внутрішніх аналітичних підрозділів і впровадження системи моніторингу кіберготовності як передумови підвищення національної стійкості у цифрову добу. Для зміцнення національної кіберстійкості Україні доцільно імплементувати низку підходів НАТО у сфері кібербезпеки: інституційне посилення НКЦК – перетворити НКЦК на повноцінний центр стратегічної координації та аналітичного прогнозування, закріпивши його право ініціювати міжвідомчі рішення; впровадження «whole-of-society» – перевести залучення приватного сектору, академічної спільноти та ГО у формат постійних офіційних партнерств; розширення системи навчань – створити власну національну програму комплексних кібернавчань, побудовану за моделлю Locked Shields, із залученням усіх операторів критичної інфраструктури та центральних органів влади; оцінка кіберготовності – інституціоналізувати механізми регулярної оцінки кіберготовності (наприклад, через NCSI) з подальшим публічним звітуванням та інтеграцією результатів у стратегічне планування.

Ключові слова: кібербезпека, національна безпека, НАТО, РНБО України, кібероборона, інституційна стійкість.

Abstract. The article examines the institutional mechanisms for cybersecurity in Ukraine and NATO countries, in the context of national security and hybrid threats. The study's relevance is driven by the growing number and complexity of cyberattacks that have become strategic tools for influencing governance and critical infrastructure. For Ukraine, facing ongoing Russian aggression, cyberspace has become a crucial dimension of modern warfare. Thus, the development of an effective institutional system for cyber defense, combining coordination, analytics, and operational response, has become a key national priority.

The article aims to conduct a comparative analysis of the institutional mechanisms of cybersecurity in Ukraine and NATO, focusing on the National Coordination Center for Cybersecurity (NCCC) under the NSDC of Ukraine and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. A systemic and comparative approach is applied to identify structural similarities and differences between governance models and to summarize NATO's best practices in interagency coordination, analytical capacity building, cyber exercises such as Locked Shields, and the implementation of the "whole-of-society" approach.

The findings indicate that Ukraine is gradually aligning with NATO standards, though its cybersecurity system still requires institutional consolidation, sustainable funding, and professional development. Meanwhile, NATO's model, represented by CCDCOE, is characterized by its integrated, research-driven, and training-oriented structure. The article proposes recommendations for strengthening Ukraine's cooperation with CCDCOE, establishing analytical units, and introducing cyber readiness monitoring as essential steps toward enhancing national resilience in the digital era. To strengthen national cyber resilience, Ukraine should implement a number of NATO approaches in the field of cybersecurity: institutional strengthening of the NCSC – to transform the NCSC into a full-fledged center of strategic coordination and analytical forecasting, consolidating its right to initiate interagency decisions; implementation of «Whole-of-Society» – to translate the involvement of the private sector, the academic community, and NGOs into the format of permanent official partnerships; expansion of the training system – to create its own national comprehensive cyber training program, built on the Locked Shields model, with the involvement of all critical infrastructure operators and central government bodies; cyber readiness assessment – to institutionalize mechanisms for regular cyber readiness assessment (for example, through NCSI) with subsequent public reporting and integration of the results into strategic planning.

Keywords: cybersecurity, national security, NATO, NSDC of Ukraine, cyber defense, institutional resilience.

Постановка проблеми. Кібербезпека є ключовим чинником національної безпеки в умовах гібридної війни, яку веде РФ проти України та країн НАТО. Масштабні кібератаки на критичну

інфраструктуру демонструють, що цифрові загрози безпосередньо впливають на фізичну безпеку держави. Для України, яка прагне інтегруватися до євроатлантичного безпекового простору, актуальним є вивчення досвіду НАТО, де кібероборона розглядається як самостійний домен колективної безпеки.

Аналіз останніх досліджень і публікацій. Інституційна організація кібербезпеки є критично важливою для здатності держави ефективно реагувати на загрози та забезпечувати стійкість критичної інфраструктури. Українські науковці ідентифікують такі ключові проблеми української системи: А. Давидюк та О. Потої [3], проаналізувавши структуру управління кібербезпекою України, вказують на фрагментарність її політики цій сфері, обмеженість ресурсів і недостатню інтеграцію аналітичних процесів, а також відзначать ті елементи української моделі, які наближають її до стандартів НАТО, але потребують подальшого вдосконалення; А. Свінцицький [4], розглядаючи повноваження державних органів у сфері кібербезпеки, виявив проблеми дублювання функцій між СБУ, Держспецзв'язку, МВС та Міноборони, відсутність єдиного центру аналітичної підтримки, що значно знижує ефективність кібероборони. Стратегічні пріоритети, механізми реагування та принципи роботи НКЦК окреслено у документах РНБО України [2; 5; 6] та Держспецзв'язку [1; 17]. Звіти PRISM UA [15] та e-Governance Academy [16] акцентують на необхідності гармонізації законодавства та підвищення інституційної спроможності у світлі євроатлантичної інтеграції.

Досвід НАТО та CCDCOE у сфері кібербезпеки розкрито у стратегічних публікаціях НАТО [7–9], в яких кіберпростір концептуалізовано як самостійний оперативний домен колективної оборони, що визначає принципи розвитку національних спроможностей держав-членів. Особливе значення мають матеріали Cooperative Cyber Defence Centre of Excellence (CCDCOE) [10–13], які містять аналіз методів багаторівневої координації, кризового управління та оцінювання готовності. Висвітлено діяльність CCDCOE, що включає організацію міжнародних навчань Locked Shields [13] – масштабної платформи для відпрацювання спільного реагування, технічного аналізу та стратегічного керування.

Незважаючи на значну теоретичну базу, недостатньо висвітленими залишаються питання інституційної сумісності української моделі кібербезпеки з архітектурою кібероборони НАТО, практичні аспекти імплементації моделей CCDCOE у національні умови (інтеграція аналітичних функцій, спільні тренувальні програми, розвиток кадрів), а також застосування підходу «whole-of-society» у національному масштабі, який є ключовим у країнах НАТО.

Мета статті – здійснення порівняльного аналізу інституційних механізмів кібербезпеки України та країн НАТО, визначення ключових спільних і відмінних рис їх організаційних моделей, а також формування рекомендацій щодо адаптації практик НАТО у національну систему України.

Виклад основного матеріалу. Сфера кібербезпеки є ключовим виміром національної безпеки, а кіберпростір став окремим театром бойових дій. Для України, яка з 2014 р. перебуває під постійним тиском, а з 2022 р. в умовах вже повномасштабної війни з РФ, – стійкість до масових кібератак на органи влади, критичну інфраструктуру та логістичні ланцюги є невід'ємним елементом обороноздатності та суверенітету [3; 4]. Приклад масштабної кібератаки на онлайн-сервіси АТ «Укрзалізниця» (навесні 2025 р.), попри збереження руху поїздів завдяки резервним протоколам, яскраво продемонстрував прямий зв'язок кіберстійкості з фізичною безпекою населення та функціонуванням критичної інфраструктури [3; 15].

Базою для формування національної системи кібербезпеки України є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає суб'єктів кібербезпеки, загальні принципи їхньої взаємодії, а також розмежування відповідальності між сектором оборони, розвідки, правоохоронними органами та регуляторами [1]. Закон закріплює роль Президента та Ради національної безпеки і оборони України (далі – РНБО) як ключових суб'єктів стратегічного управління у сфері кібербезпеки.

НКЦК, створений як наймолодша ланка системи кібербезпеки, виконує роль національного координатора та аналітичного центру з поточних і перспективних кіберзагроз [3; 5]. Він організовує обмін інформацією між суб'єктами, готує пропозиції щодо політики, а також забезпечує публічно-

приватну взаємодію. При НКЦК діє постійна Об'єднана група реагування на кіберінциденти та кібератаки, до якої входять технічні фахівці основних кіберсуб'єктів держави [6].

Таблиця 1.

Повноваження між ключовими органами в українській моделі кібербезпеки

Суб'єкт	Основна функція
РНБО	Стратегічна координація та контроль.
Національний координаційний центр кібербезпеки (НКЦК) при РНБО	Національний координатор, аналітичний центр, платформа публічно-приватної взаємодії [5]. Представляє Україну у CCDCOE [18].
Держспецзв'язок	Урядовий зв'язок, криптографічний захист, операційні функції кіберзахисту (через CERT-UA).
СБУ, Міноборони, Нацполіція	Контррозвідувальна, військова та правоохоронна діяльність у кіберсфері.

Стратегія кібербезпеки України на 2021–2025 рр. [2; 3], затверджена Указом Президента № 447/2021, деталізувала пріоритети та передбачає інтеграцію України в євроатлантичний простір. На її виконання Урядом було затверджено план заходів на 2025 р., який конкретизував кроки з посилення кіберстійкості держави, розвитку інфраструктури, механізмів реагування та підготовки персоналу [17].

Під впливом російської агресії проти України, країни НАТО суттєво переглянули свою безпекову архітектуру, визнавши кіберпростір окремою операційною сферою та закріпивши кіберзахист як ключовий напрям колективної безпеки [7-9]. Важливу роль у цьому відіграє Кооперативний центр кібероборони НАТО (CCDCOE) у Таллінні. Він є провідним міжнародним хабом знань, навчання та спільних кібернавчань [10-13]. Аналіз його інституційних механізмів є критично необхідним для України задля посилення власної системи національної безпеки в кіберпросторі. НКЦК представляє Україну у CCDCOE, а також ініціює участь українських фахівців у спільних навчаннях з країнами НАТО [18]. Це безпосередньо пов'язано з національною безпекою, адже дозволяє отримувати практичний досвід колективної оборони у кіберпросторі. Поглиблення співпраці України з ЄС і НАТО, участь у програмах посилення кіберзахисту та оцінки індексів кіберготовності (зокрема National Cyber Security Index) дозволили Україні адаптуватися до стандартів партнерів, враховуючи вимоги до інституційної зрілості, наявності стратегій, планів реагування та системи моніторингу [15; 16]. Це формує перехід від «точкових» рішень до цілісної моделі управління кібербезпекою як складової національної безпеки.

НАТО розглядає кіберзахист як одну з ключових складових колективної оборони. На брюссельському саміті 2021 р. держави-члени схвалили оновлену Всеохопну політику кібероборони (Comprehensive Cyber Defence Policy), яка підтримує три основні завдання Альянсу – колективну оборону, кризове управління та кооперативну безпеку [7; 9]. Ця політика передбачає:

- визнання кіберпростору операційною сферою нарівні з сушею, морем, повітрям та космосом;
- розвиток спроможностей держав-членів для стримування та реагування на кібератаки;
- інтеграцію кіберкомпоненти в планування операцій і колективну оборону, включно з можливістю застосування статті 5 Вашингтонського договору у разі масштабних кібератак [7; 8].

Для реалізації своєї політики НАТО розвиває інституційну архітектуру, до якої належать Комітет з кібероборони, Об'єднаний центр кібероперацій (Cyberspace Operations Centre) та мережа акредитованих центрів передового досвіду, серед яких провідну роль у кібербезпеці відіграє CCDCOE [8; 11].

CCDCOE, розташований у Таллінні (Естонія), є акредитованим НАТО центром передового досвіду, що поєднує функції аналітичного центру (think-tank), навчальної платформи та організатора міждержавних кібернавчань [10-12]. Місія центру – підтримувати держави-члени НАТО та партнерів міждисциплінарною експертизою у сферах технологій, стратегії, операцій та права кібероборони, сприяти розвитку спроможностей, кооперації та обміну інформацією [10; 12].

Ключові напрями діяльності CCDCOE охоплюють, по-перше, проведення міждисциплінарних досліджень у сфері національних систем кібербезпеки, правового регулювання кіберконфліктів, а також розроблення стратегій стримування та підвищення стійкості до кіберзагроз. По-друге, центр забезпечує навчання та підготовку фахівців через спеціалізовані курси, тренінги й сертифікаційні програми, формуючи професійне середовище для експертів із кібероборони. По-третє, CCDCOE організовує масштабні міжнародні кібернавчання, зокрема щорічні комплексні навчання Locked Shields, які вважаються найбільшими у світі «live-fire» кібернавчаннями у сфері кібероборони [13; 14].

Структурно CCDCOE не входить до командної чи силової структури НАТО, але є частиною ширшої системи підтримки командних спроможностей Альянсу, будучи спонсорованим усіма державами-членами НАТО та низкою партнерів, включно з Україною [11; 12].

Україна є країною-партнером CCDCOE та поступово розширює свою участь у діяльності центру. НКЦК та Держспецзв'язок представляють Україну в CCDCOE, розглядається можливість посилення участі за рахунок фахівців СБУ та Міністерства оборони [18].

Важливим елементом інтеграції є участь українських спеціалістів у навчаннях Locked Shields, де національні та багатонаціональні команди відпрацьовують захист критичних систем, реагування на інциденти, юридичні та комунікаційні аспекти кіберконфліктів [13; 14]. У 2024 р. Україна вперше взяла участь у Locked Shields у складі спільної команди з Чеською Республікою, що дозволило протестувати на практиці спроможності, напрацьовані у ході реальної війни [14].

Таким чином, НАТО через CCDCOE не лише формує загальні стандарти, але й надає країнам-партнерам (зокрема, Україні) платформу для практичного наближення національних механізмів кібербезпеки до вимог колективної оборони.

Україна і НАТО мають оновлені стратегічні документи у сфері кібербезпеки, що розглядають кіберзагрози як компонент національної та колективної безпеки, а не виключно IT-проблему [2; 7-9].

Порівняння стратегічних підходів України та НАТО у сфері кібербезпеки демонструє як спільні, так і відмінні риси. Обидві сторони мають комплексні стратегічні документи, розраховані на середньострокову перспективу: Україна реалізує Стратегію кібербезпеки на 2021–2025 рр., а НАТО у 2021 р. ухвалило оновлену Всеохопну політику кібероборони. В обох випадках кібербезпека інтегрована у загальну систему національної або колективної безпеки, що свідчить про її визнання як ключового елементу державної стійкості. Крім того, Україна і НАТО приділяють значну увагу захисту критичної інфраструктури та розвитку людського капіталу, вбачаючи у підготовці фахівців один із пріоритетів безпекової політики.

Разом з тим, існують суттєві відмінності. НАТО має виразний колективний вимір кібероборони, який передбачає реалізацію статті 5 Вашингтонського договору та спільне використання оборонних спроможностей держав-членів, тоді як Україна наразі формує переважно національні механізми кіберзахисту з окремими елементами міжнародної кооперації [7; 15]. Крім того, стратегічні документи НАТО спираються на багаторічний досвід розвитку кіберінституцій та уніфіковані стандарти, узгоджені для всіх союзників. Українська ж система продовжує перебувати у фазі інституційної консолідації, де триває вдосконалення нормативно-правової бази й узгодження компетенцій між органами, що відповідають за національну безпеку в кіберпросторі [3; 4].

І в Україні, і в НАТО існує багаторівнева система управління кібербезпекою: стратегічний рівень (політика і координація), операційний рівень (центри реагування, CERT, військові структури) та рівень взаємодії з приватним сектором.

Українська модель кібербезпеки має свої відчутні особливості, що зумовлені як безпековими реаліями, так і етапом розвитку інституційної системи. Центральне місце в ній посідають Рада національної безпеки і оборони України та Національний координаційний центр кібербезпеки, які виконують роль основних координаторів у цій сфері. Саме вони забезпечують політичне лідерство, аналітичну підтримку та координацію дій між усіма суб'єктами, що відповідають за захист державного кіберпростору [5; 6]. Водночас практична реалізація політики кібербезпеки покладена на низку виконавчих органів – Державну службу спеціального зв'язку та захисту інформації, Службу безпеки України, Міністерство внутрішніх справ і Міністерство оборони. Така багаторівнева

структура потребує чіткої взаємодії, постійного узгодження рішень і розмежування компетенцій, аби уникнути дублювання функцій та забезпечити ефективне реагування на загрози [3; 4]. Окремим напрямом розвитку є створення сектору кібервійськ і спеціальних підрозділів, орієнтованих на активні дії у кіберпросторі, що свідчить про перехід від пасивного захисту до більш проактивної оборонної позиції [23].

Натомість модель кібербезпеки має інший характер НАТО. Вона ґрунтується на принципі, за яким кожна країна-член відповідає за власний кіберзахист, тоді як НАТО забезпечує координацію, узгодження стандартів і спільну підтримку у випадку масштабних загроз [7; 8]. У межах Альянсу функціонують спеціалізовані структури – зокрема Cyberspace Operations Centre та CCDCOE, а також низка інших центрів передового досвіду, що займаються плануванням, аналітикою, навчанням і підготовкою кадрів. Важливим елементом є закріплення комплексного підходу «whole-of-government» і «whole-of-society», коли до процесу кібероборони залучаються не лише державні органи, а й приватні компанії, наукові установи та громадянське суспільство. Такий підхід дозволяє створити справді стійку екосистему безпеки, де відповідальність розподілена між усіма учасниками [7; 26].

Тобто Україна поступово рухається в напрямі моделі багаторівневого управління кібербезпекою НАТО. Проте вітчизняна система ще зберігає певну фрагментарність і стикається з нестачею ресурсів, що уповільнює реалізацію ухвалених рішень. Попри це, динаміка реформ і поглиблення міжнародної співпраці свідчать про незворотний рух до інтеграції з євроатлантичним безпековим простором.

НАТО вибудувало розгалужену систему навчань, у якій CCDCOE відіграє ключову роль. Locked Shields як найбільші у світі «live-fire» кібернавчання об'єднують тисячі експертів із десятків країн, моделюючи захист національних систем від масштабної кіберкризи з технічними, правовими, комунікаційними та стратегічними компонентами [13; 14]. Україна активно залучається до цієї екосистеми, використовуючи навчання для відпрацювання взаємодії між власними структурами та партнерами, а також для адаптації підходів до управління інцидентами й кризової комунікації [14; 18]. Водночас на національному рівні система регулярних комплексних навчань ще перебуває в стадії розвитку й часто залежить від зовнішнього фінансування та підтримки донорів [15; 25].

НАТО, як альянс розвинених демократій, має потужну фінансову та технологічну базу для кібероборони, яка посилюється останніми рішеннями щодо збільшення оборонних витрат та пріоритизації кіберзахисту [7; 26]. Україна ж, попри значний прогрес, залишається більш вразливою до ресурсних обмежень, у тому числі залежності від зовнішньої допомоги у сфері кібербезпеки, що особливо проявилось на тлі змін у міжнародному фінансуванні цифрових проєктів [15]. Це створює додатковий виклик для довгострокової сталості національної кіберсистеми, яка включає не лише технічну інфраструктуру, але й утримання кваліфікованого персоналу та постійне оновлення спроможностей, зокрема і інституційних.

Таблиця 2.

Основні відмінності та виклики України та НАТО у сфері кібербезпеки

Критерій	Україна (НКЦК)	НАТО (CCDCOE)
Вимір безпеки	Переважно національні механізми захисту з елементами кооперації.	Колективна кібероборона (можливість застосування ст. 5).
Інституційна зрілість	У фазі інституційної консолідації; потребує узгодження компетенцій та усунення фрагментарності.	Висока інституційна зрілість, уніфіковані стандарти.
Залучення суспільства	На рівні окремих ініціатив.	Принцип "whole-of-society" (залучення приватного сектору, науки, громадянського суспільства).
Ресурси	Вразливість до ресурсних обмежень; залежність від зовнішньої допомоги.	Потужна фінансова та технологічна база.

Одним із ключових напрямів розвитку української системи кібербезпеки має стати посилення ролі міжвідомчих координаційних структур, насамперед, Національного координаційного центру кібербезпеки. Досвід НАТО демонструє ефективність моделі, коли стратегічні рішення ухвалюються на рівні політичних органів, а їхня практична реалізація здійснюється через спеціалізовані центри – такі як Cyberspace Operations Centre або CCDCOE. Подібний підхід може стати орієнтиром для подальшої еволюції НКЦК у форматі «мозкового центру» української кіберсистеми. Для цього необхідно інституційно закріпити право НКЦК ініціювати міжвідомчі рішення, формалізувати механізми обміну інформацією та спільного аналізу ризиків, а також зміцнити кадровий потенціал центру, залучивши висококваліфікованих фахівців [3; 5; 11].

Ще одним напрямом є впровадження системного підходу «whole-of-society», який давно став нормою у країнах НАТО. Його суть полягає у тому, що до забезпечення кібербезпеки залучаються всі складові суспільства – приватний сектор, академічні установи, експертна спільнота та громадські організації. Для України важливо перевести цю практику з рівня окремих ініціатив у формат постійних офіційних партнерств, що дозволить створити справжню екосистему кіберстійкості та підвищити ефективність державної політики у сфері кіберзахисту [7; 22].

Одним із найуспішніших прикладів практики НАТО є щорічні міжнародні навчання Locked Shields, організовані CCDCOE. Вони демонструють дієвість сценарного підходу, коли під час одного тренування одночасно відпрацьовуються технічні, правові, комунікаційні та стратегічні аспекти реагування на кіберінциденти [13; 14]. Для України доцільно створити власну національну програму комплексних кібернавчань, побудовану за аналогічним принципом. Це може включати щорічні тренування із залученням центральних органів влади, регіональних адміністрацій, операторів критичної інфраструктури, засобів масової інформації та громадських структур. Результати участі у Locked Shields варто використовувати як основу для національних сценаріїв навчань, адаптуючи їх до українських реалій. Не менш важливим є питання стабільного інституційного фінансування таких заходів, аби вони не залежали виключно від донорської підтримки, а стали сталою частиною системи національної безпеки.

Розвиток аналітичної спроможності України у сфері кібербезпеки значною мірою пов'язаний із поглибленням співпраці з Центром передового досвіду з кібероборони НАТО (CCDCOE). Цей центр реалізує серію міждержавних досліджень **National Cybersecurity Governance Series**, у межах яких проаналізовано й українську модель управління кібербезпекою [3]. Системна участь українських фахівців у таких аналітичних проєктах сприяє імплементації кращих міжнародних практик управління, формуванню внутрішніх аналітичних підрозділів при НКЦК та профільних міністерствах, а також забезпечує передачу знань у сфері правового регулювання кіберконфліктів – надзвичайно актуальну в умовах триваючої війни.

Важливою складовою зміцнення національної кіберстійкості є інституціоналізація механізмів регулярної оцінки кіберготовності. Використання міжнародних індексів, зокрема **National Cyber Security Index (NCSI)**, а також участь у спільних ініціативах ЄС і НАТО дають можливість оцінювати рівень зрілості української системи кібербезпеки за єдиними міжнародними критеріями та адаптувати державну політику до зовнішніх стандартів [15; 16]. Україні доцільно закріпити на рівні урядових рішень вимогу проводити систематичну оцінку кіберготовності з подальшим публічним звітуванням. Результати таких оцінок мають стати невід'ємною частиною процесів стратегічного планування – як у межах Стратегії національної безпеки, так і під час оборонного планування.

Для ефективної реалізації цих напрямів необхідно дотриматися кількох базових умов. Насамперед, забезпечити **стабільність фінансування**, адже кібербезпека має розглядатися не як короткостроковий проєкт, а як довгострокова інвестиція в національну безпеку. Не менш важливо сформувати **системну політику управління персоналом**, орієнтовану на створення професійного корпусу кіберфахівців у державному секторі з гідною оплатою праці, можливостями підвищення кваліфікації та кар'єрного розвитку. Потребує подальшої роботи **нормативна узгодженість** – гармонізація українського законодавства з правом ЄС та стандартами НАТО, особливо у сферах

захисту критичної інфраструктури, обміну інформацією та відповідальності за кібератаки [1; 2; 15]. Нарешті, ключовою передумовою є **політична незворотність євроатлантичного курсу**, адже інтеграція в систему кібербезпеки НАТО можлива лише за умови послідовного руху України до членства в НАТО та подальшого поглиблення секторальної взаємодії у сфері безпеки.

Висновки. Інституційні механізми кібербезпеки України прискорено трансформуються в результаті повномасштабної війни з росією, стратегічним курсом на євроатлантичну інтеграцію та стрімким розвитком технологій. Створення НКЦК, оновлення Стратегії кібербезпеки, формування сектору кібервійськ, розбудова CERT-спроможностей та розширення міжнародної кооперації поступово формують контури сучасної української моделі кібероборони як багаторівневої системи, що інтегрує політичне керівництво, аналітику, міжвідомчу взаємодію та співпрацю з партнерами.

Модель НАТО, представлена через діяльність CCDCOE, демонструє високий рівень інституційної зрілості та комплексності. Її ключова сила – у синергії аналітики, досліджень, підготовки кадрів, стандартів реагування та масштабних міжнародних навчань. Locked Shields, системні огляди національних кіберсистем, розвиток інституційних компетенцій та підхід «whole-of-society» утворюють цілісну екосистему кібероборони, у якій кожен компонент підсилює інший. Для України участь у цих форматах НАТО означає не лише ознайомлення з досвідом, а й можливість тестувати власні спроможності в умовах повномасштабної війни.

Українська система кібербезпеки еволюціонує до моделі НАТО, хоча зберігає певні інституційні виклики, зокрема фрагментарність координації та наявність ресурсних обмежень. Україна потребує створення сталих інституційних механізмів, здійснення переходу від реактивних рішень на кіберзагрози до стратегічного управління кіберризиками.

Для зміцнення національної кіберстійкості Україні доцільно імплементувати низку підходів НАТО у сфері кіберзбезпеки: *інституційне посилення НКЦК* – перетворити НКЦК на повноцінний центр стратегічної координації та аналітичного прогнозування, закріпивши його право ініціювати міжвідомчі рішення; *впровадження «whole-of-society»* – перевести залучення приватного сектору, академічної спільноти та ГО у формат постійних офіційних партнерств; *розширення системи навчань* – створити власну національну програму комплексних кібернавчань, побудовану за моделлю Locked Shields, із залученням усіх операторів критичної інфраструктури та центральних органів влади; *оцінка кіберготовності* – інституціоналізувати механізми регулярної оцінки кіберготовності (наприклад, через NCSI) з подальшим публічним звітуванням та інтеграцією результатів у стратегічне планування.

Ключовими умовами успішної імплементації цих підходів є стабільне фінансування кібербезпеки як довгострокової інвестиції, формування професійного кадрового корпусу, нормативна гармонізація з правом ЄС та НАТО, а також політична незворотність курсу на євроатлантичну інтеграцію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Державна служба спеціального зв'язку та захисту інформації України. Правова основа діяльності Центру операцій безпеки (включає положення Закону України «Про основні засади забезпечення кібербезпеки України»). URL: https://scpc.gov.ua (дата звернення: 22.11.2025).
2. Рада національної безпеки і оборони України. Президент України затвердив нову Стратегію кібербезпеки України (Указ № 447/2021). URL: https://www.rnbo.gov.ua (дата звернення: 22.11.2025).
3. Давидюк А., Потої О. *National Cybersecurity Governance: Ukraine.* Таллінн: NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/library/publications/national-cybersecurity-governance-ukraine (дата звернення: 22.11.2025).
4. Свінцицький А.В. Система органів кібербезпеки в Україні. *Cuestiones Políticas.* 2022. №40(72). С. 49–66. URL: https://www.redalyc.org/journal/5717/57177064004/html (дата звернення: 22.11.2025).
5. Рада національної безпеки і оборони України. Перше координаційне засідання Національного координаційного центру кібербезпеки при РНБО України. URL: https://www.rnbo.gov.ua (дата звернення: 22.11.2025).
6. Рада національної безпеки і оборони України. Національний координаційний центр кібербезпеки має постійну Об'єднану команду реагування на кіберінциденти/кібератаки. URL: https://www.rnbo.gov.ua (дата звернення: 22.11.2025).
7. НАТО. Кібероборона. URL: https://www.nato.int/cps/en/natolive/topics_78170.htm (дата звернення: 22.11.2025).

8. НАТО. *Cyber defence – Factsheet*. Підрозділ публічної дипломатії НАТО. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160718_1607-factsheet-cyber-defence-en.pdf (дата звернення: 22.11.2025).
9. НАТО. Брюссельське комюніке Саміту НАТО. URL: https://www.nato.int/cps/en/natohq/news_185000.htm (дата звернення: 22.11.2025).
10. Центр передового досвіду НАТО з кібероборони (CCDCOE). Про нас. URL: https://ccdcoe.org/about-us (дата звернення: 22.11.2025).
11. Стратегічне командування НАТО з трансформації. Центри передового досвіду НАТО – Cooperative Cyber Defence CCD COE. URL: https://www.act.nato.int/article/nato-centres-of-excellence-cooperative-cyber-defence-ccd-coe (дата звернення: 22.11.2025).
12. Сили оборони Естонії. NATO Cooperative Cyber Defence Centre of Excellence. URL: https://mil.ee/en/defence-forces/ccdcoe (дата звернення: 22.11.2025).
13. Центр передового досвіду НАТО з кібероборони (CCDCOE). Locked Shields. URL: https://ccdcoe.org/exercises/locked-shields (дата звернення: 22.11.2025).
14. Рада національної безпеки і оборони України. (2024). Україна візьме участь у кібернавчаннях Locked Shields CCDCOE. URL: https://www.rnbo.gov.ua (дата звернення: 22.11.2025).
15. PRISM UA. *ЄС, НАТО і Україна: Dream Team чи Трикутник?* Київ: Рада зовнішньої політики «Українська призма». URL: https://prismua.org/eu-nato-ukraine (дата звернення: 22.11.2025).
16. Академія електронного врядування (e-Governance Academy). National Cyber Security Index – Ukraine. URL: https://ncsi.ega.ee/country/ua (дата звернення: 22.11.2025).
17. Державна служба спеціального зв'язку та захисту інформації України. Робота над посиленням кіберстійкості держави: затверджено План дій на 2025 рік з реалізації Стратегії кібербезпеки. URL: https://cip.gov.ua/en/news/action-plan-for-2025-to-implement-cybersecurity-strategy-approved (дата звернення: 22.11.2025).
18. Рада національної безпеки і оборони України. Національний координаційний центр кібербезпеки буде представлений у CCDCOE фахівцем Держспецзв'язку. URL: https://www.rnbo.gov.ua (дата звернення: 22.11.2025).

REFERENCES

1. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. Pravova osnova diialnosti Tsentru operatsii bezpeky (vkliuchaie polozhennia Zakonu Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy») [State Service of Special Communications and Information Protection of Ukraine. Legal basis of the Security Operations Centre (includes reference to the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine"]. *scpc.gov.ua.* Retrieved from https://scpc.gov.ua [in Ukrainian].
2. Rada natsionalnoi bezpeky i oborony Ukrainy. (27.08.2021). Prezydent Ukrainy zatverdyv novu Stratehiiu kiberbezpeky Ukrainy (Ukaz № 447/2021) [National Security and Defence Council of Ukraine. The President of Ukraine approved a new Cybersecurity Strategy of Ukraine (Decree №447/2021 from August 27, 2021]. *www.rnbo.gov.ua.* Retrieved from https://www.rnbo.gov.ua [in Ukrainian].
3. Davydiuk, A., & Potii, O. (2024). *National Cybersecurity Governance: Ukraine*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. *ccdcoe.org.* Retrieved from https://ccdcoe.org/library/publications/national-cybersecurity-governance-ukraine [in English].
4. Svintsytskyi, A. V. (2022). Systema orhaniv kiberbezpeky v Ukraini [The system of cybersecurity bodies in Ukraine]. *Cuestiones Políticas*, *40(72),* 49–66. Retrieved from https://www.redalyc.org/journal/5717/57177064004/html [in Ukrainian].
5. Rada natsionalnoi bezpeky i oborony Ukrainy. (04.03.2021). Pershe koordynatsiine zasidannia Natsionalnoho koordynatsiinoho tsentru kiberbezpeky pry RNBO Ukrainy [National Security and Defence Council of Ukraine. The first coordination meeting of the National Cybersecurity Coordination Center under the NSDC of Ukraine from March 4, 2021]. *www.rnbo.gov.ua*. Retrieved from https://www.rnbo.gov.ua [in Ukrainian].
6. Rada natsionalnoi bezpeky i oborony Ukrainy. Natsionalnyi koordynatsiinyi tsentr kiberbezpeky maie postiinu Obiednanu komandu reahuvannia na kiberintsydenty/kiberataky [National Security and Defence Council of Ukraine. The National Coordination Center for Cybersecurity has a permanent Joint Response Team for Cyber Incidents/Cyber Attacks]. *www.rnbo.gov.ua.* Retrieved from https://www.rnbo.gov.ua [in Ukrainian].
7. NATO. (2024, July 30). Kiberoborona [Cyber defence]. *www.nato.int.* Retrieved from https://www.nato.int/cps/en/natolive/topics_78170.htm [in Ukrainian].
8. NATO. (2016). *Cyber defence – Factsheet*. NATO Public Diplomacy Division. *www.nato.int.* Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160718_1607-factsheet-cyber-defence-en.pdf [in English].
9. NATO. (2021). Briusselske komiunike Samitu NATO [Brussels Summit Communiqué]. *www.nato.int.* Retrieved from https://www.nato.int/cps/en/natohq/news_185000.htm [in Ukrainian].
10. Tsentr peredovoho dosvidu NATO z kiberoborony (CCDCOE). Pro nas [NATO Cooperative Cyber Defence Centre of Excellence. About us]. *ccdcoe.org.* Retrieved from https://ccdcoe.org/about-us [in Ukrainian].
11. Stratehichne komanduvannia NATO z transformatsii. (29.08.2023). Tsentry peredovoho dosvidu NATO – Cooperative Cyber Defence CCD COE [NATO Allied Command Transformation. NATO Centres of Excellence – Cooperative Cyber Defence CCD COE from August 29, 2023]. *www.act.nato.int.* Retrieved from https://www.act.nato.int/article/nato-centres-of-excellence-cooperative-cyber-defence-ccd-coe [in Ukrainian].

12. Syly oborony Estonii. (20.02.2025). NATO Cooperative Cyber Defence Centre of Excellence [Estonian Defence Forces. NATO Cooperative Cyber Defence Centre of Excellence from February 20, 2025]. *mil.ee*. Retrieved from https://mil.ee/en/defence-forces/ccdcoe [in Ukrainian].
13. Tsentr peredovoho dosvidu NATO z kiberoborony (CCDCOE). Locked Shields [NATO Cooperative Cyber Defence Centre of Excellence. Locked Shields]. *ccdcoe.org.* Retrieved from https://ccdcoe.org/exercises/locked-shields [in Ukrainian].
14. Rada natsionalnoi bezpeky i oborony Ukrainy. (2024). Ukraina vizme uchast u kibernavchanniakh Locked Shields CCDCOE [National Security and Defence Council of Ukraine. Ukraine to participate in NATO CCDCOE Locked Shields cyber defense exercise]. *www.rnbo.gov.ua.* Retrieved from https://www.rnbo.gov.ua [in Ukrainian].
15. PRISM UA. (2023). YeS, NATO i Ukraina: Dream Team chy Trykutnyk? Kyiv: Rada zovnishnoi polityky «Ukrainska pryzma» [PRISM UA. *EU, NATO and Ukraine: Dream Team or a Triangle?* Kyiv: Foreign Policy Council "Ukrainian Prism"]. *prismua.org*. Retrieved from https://prismua.org/eu-nato-ukraine [in Ukrainian].
16. Akademiia elektronnoho vriaduvannia (e-Governance Academy). National Cyber Security Index – Ukraine [e-Governance Academy. National Cyber Security Index – Ukraine]. *ncsi.ega.ee*. Retrieved from https://ncsi.ega.ee/country/ua [in Ukrainian].
17. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (10.03.2025). Robota nad posylenniam kiberstiikosti derzhavy: zatverdzheno Plan dii na 2025 rik z realizatsii Stratehii kiberbezpeky [State Service of Special Communications and Information Protection of Ukraine. Working to strengthen the state's cyber resilience and protection against cyber threats: Action plan for 2025 to implement the Cybersecurity Strategy approved from March 10, 2025]. *cip.gov.ua.* Retrieved from https://cip.gov.ua/en/news/action-plan-for-2025-to-implement-cybersecurity-strategy-approved [in Ukrainian].
18. Rada natsionalnoi bezpeky i oborony Ukrainy. Natsionalnyi koordynatsiinyi tsentr kiberbezpeky bude predstavlenyi u CCDCOE fakhivtsem Derzhspetszviazku [National Security and Defence Council of Ukraine. The National Coordination Center for Cybersecurity will be represented at the CCDCOE by a specialist from the State Service for Special Communications]. *www.rnbo.gov.ua*. Retrieved from https://www.rnbo.gov.ua [in Ukrainian].

Історія статті / Article history:
Подано до редакції / Submitted to the editorial office (24.11.2025);
Прийнято до друку / Accepted for publication (28.12.2025);
Опубліковано / Published (06.04.2026).