УДК 004.056.53(100)
DOI https://doi.org/10.32850/LB2414-4207.2025.37.15

МІЖНАРОДНИЙ ДОСВІД ПРОВЕДЕННЯ КОНТРОЛЬОВАНИХ КІБЕРАТАК ПІД ЧАС ЗБРОЙНИХ КОНФЛІКТІВ

Кочман Костянтин Павлович,
orcid.org/0009-0001-3194-1220
аспірант кафедри кримінального аналізу та інформаційних технологій (Одеський державний університет внутрішніх справ, м. Одеса, Україна)

Стаття присвячена комплексному аналізу міжнародного досвіду застосування кібероперацій у сфері забезпечення національної кібербезпеки в контексті сучасних збройних конфліктів. Дослідження розкриває концептуальні підходи до використання кіберінструментів у протидії цифровим загрозам, акцентуючи увагу на трьох ключових принципах: оборона, контрнаступ та стримування. Детально проаналізовано досвід США з їхньою стратегією «захисту вперед» (defend forward), що передбачає проактивну нейтралізацію загроз через діяльність Кіберкомандування США (USCYBERCOM). Розглянуто підходи країн НАТО до колективної кібероборони, включаючи механізми активації статті 5 Північноатлантичного договору у відповідь на кібератаки, проведення масштабних кібернавчань Cyber Coalition та створення спільних платформ обміну даними. Особливу увагу приділено ізраїльській моделі кібербезпеки, що базується на інноваційному підході через Національний кібердиректорат та спеціалізований підрозділ 8200, а також унікальній системі державно-приватного партнерства.

У статті проаналізовано роль сучасних технологій – штучного інтелекту, машинного навчання та аналізу великих даних – у забезпеченні автоматизованого виявлення та нейтралізації кіберзагроз. Висвітлено проблематику інформаційної війни та кіберпропаганди як складових гібридних конфліктів. Визначено ключові виклики для України: недофінансування, кадровий дефіцит, недостатня міжвідомча координація. Запропоновано практичні рекомендації щодо адаптації міжнародного досвіду до українських реалій, включаючи розробку національної кіберстратегії, посилення нормативно-правової бази відповідно до Талліннського керівництва та норм міжнародного гуманітарного права, розвиток системи підготовки кіберфахівців. Обґрунтовано необхідність інвестицій у R&D сектор та важливість міжнародної співпраці з НАТО та ЄС для зміцнення кіберстійкості України в умовах триваючої російської агресії.

Ключові слова: кібероперація, кіберстратегія, національна безпека, штучний інтелект, міжнародне право, інформаційна безпека, кібероборона, гібридна війна.

INTERNATIONAL EXPERIENCE IN CONDUCTING CONTROLLED CYBERATTACKS DURING ARMED CONFLICTS

Kochman Konstantin Pavlovich,
orcid.org/0009-0001-3194-1220
Postgraduate Student at the Department of Criminal Analysis and Information Technologies
(Odessa State University of Internal Affairs, Odesa, Ukraine)

This article provides a comprehensive analysis of international practices in utilizing cyber operations to enhance national cybersecurity within the context of modern armed conflicts. The research explores conceptual approaches to cyber tool deployment in countering digital threats, emphasizing three fundamental principles: defense, counteroffensive, and deterrence. The study extensively examines the U.S. experience with its «defend forward» strategy, which involves proactive threat neutralization through the U.S. Cyber Command (USCYBERCOM) operations. NATO's collective cyber defense approaches are analyzed, including mechanisms for activating Article 5 of the North Atlantic Treaty in response to cyberattacks, conducting large-scale Cyber Coalition exercises, and establishing joint data-sharing platforms. Special attention is given to the Israeli cybersecurity model, based on an innovative approach through the National Cyber Directorate and the specialized Unit 8200, alongside a unique public-private partnership system.

The article analyzes the role of cutting-edge technologies – artificial intelligence, machine learning, and big data analytics – in ensuring automated detection and neutralization of cyber threats. It addresses information warfare and cyber propaganda as components of hybrid conflicts. Key challenges for Ukraine are identified: underfunding, personnel shortage, insufficient interagency coordination. Practical recommendations are proposed for adapting international experience to Ukrainian realities, including developing a national cyber strategy, strengthening the regulatory framework in accordance with the Tallinn Manual and international humanitarian law, and developing a cyber specialist training system. The necessity of R&D sector investments is substantiated, along with the importance of international cooperation with NATO and the EU to strengthen Ukraine's cyber resilience amid ongoing Russian aggression. The research contributes to understanding how cyber operations have become integral to modern military strategies and provides a roadmap for enhancing Ukraine's cyber defense capabilities through international best practices adaptation.

Key words: cyber operation, cyber strategy, national security, artificial intelligence, international law, information security, cyber defense, hybrid warfare.

Постановка проблеми та її актуальність. У сучасному світі кібероперації стали невід'ємною частиною військових стратегій держав, особливо у контексті зростання глобальних загроз у кіберпросторі. У контексті повномасштабної війни, що триває в Україні з 2022 року, кіберпростір перетворився на стратегічно важливий театр бойових дій, доповнюючи традиційні види збройного протистояння. В умовах сучасної війни кібероперації стали ключовим інструментом для атак на критичну інфраструктуру, порушення функціонування державних установ і банківської системи, впливу на енергетичний сектор та проведення інформаційних кампаній дезінформації, спрямованих на підрив стабільності суспільства. Інтеграція кібероперацій у військову стратегію України набуває вирішального значення для забезпечення національної

безпеки та підтримки обороноздатності держави. Аналіз сучасних викликів і перспектив у цій сфері є основою для формування ефективної системи кібероборони, здатної захистити критичні інформаційні ресурси країни. Інтеграція кібероперацій у стратегію забезпечує додаткові можливості для захисту національної безпеки, координації дій з союзниками та досягнення стратегічних переваг. Сучасні кіберінструменти дозволяють проводити операції зі збору інформації, перешкоджати комунікації противника, а також забезпечувати захист критичних систем управління та зв'язку. Однак ефективне використання кібероперацій потребує розробки цілісної концепції, що включає правові, організаційні та технічні аспекти їх реалізації.

Аналіз останніх досліджень і публікацій. Робота ґрунтується на аналізі законодавства України та зарубіжних країн, науково-методичної літератури, методичних посібників, наукових статей, періодичних видань та напрацювань сучасних та попередніх дослідників, серед яких: М. В. Гребенюк, І. Ляшенко, С. М. Стежко, В. В. Маштaлір тощо.

Вчені аналізують правові та практичні аспекти кібербезпеки, досвід країн у сфері кібероборони та застосування кібероперацій для забезпечення національної безпеки, зокрема в контексті України та міжнародної практики.

Метою цієї статті є аналіз значення та основних напрямів інтеграції кібероперацій у військову стратегію України, визначення ключових викликів та перспектив розвитку в цій сфері, а також обґрунтування необхідності міжвідомчої співпраці та міжнародної підтримки.

Виклад основного матеріалу. Кібероперації є комплексом дій, спрямованих на забезпечення національної безпеки через активне використання кіберпростору. Зокрема, кібероперації охоплюють заходи щодо захисту, моніторингу, проникнення, руйнування або блокування цифрових і мережевих систем противника. Ключовими компонентами кібероперацій є збирання та аналіз інформації, контроль над комунікаціями противника, вплив на об'єкти критичної інфраструктури та забезпечення безпеки власних систем управління [7].

У військовій стратегії кібероперації посідають стратегічно важливе місце завдяки їхній здатності швидко і, в більшості випадків, непомітно завдавати шкоди противнику, дестабілізувати його функціональні системи та навіть створювати переваги на полі бою без прямого використання фізичної сили. Крім того, кібероперації дозволяють здійснювати ефективний захист критичної інфраструктури, яка є вразливою до атак у сучасному цифровому середовищі. В умовах сучасної війни, де традиційні воєнні дії переплітаються з інформаційною та кібернетичною складовими, кібероперації набувають вирішального значення для досягнення стратегічних цілей.

Основні принципи застосування кібероперацій: оборона, контрнаступ, стримування. Основна мета оборонних кібероперацій полягає у захисті національних кіберсистем та інформаційних ресурсів від потенційних загроз і нападів. Це включає комплекс превентивних і реактивних заходів, що спрямовані на виявлення, запобігання та нейтралізацію атак на критичні об'єкти, такі як енергетичні мережі, транспортні системи, урядові бази даних та військові комунікації. В оборонних кіберопераціях особливу увагу приділяють моніторингу трафіку, ідентифікації потенційних загроз, а також впровадженню заходів із мінімізації наслідків у разі прориву захисних ліній. Для досягнення ефективної оборони критично важливим є постійне оновлення систем безпеки, підготовка кадрів та оперативна міжвідомча координація.

Контрнаступальні кібероперації передбачають заходи, що дозволяють нейтралізувати та ослабити противника шляхом цілеспрямованих атак на його кіберсистеми. Це може включати проникнення в мережі противника з метою знищення або порушення

роботи його критичних об'єктів, таких як військові комунікаційні системи, інформаційні центри, засоби масової інформації та інші ресурси, важливі для функціонування держави. Контрнаступ у кіберпросторі також включає активне використання методів інформаційного впливу, що допомагають деморалізувати противника, знижуючи його боєздатність та здатність до опору [4, с. 98–99].

Кібернетичне стримування є стратегією, що базується на створенні такого рівня кіберзахисту та наступальних кіберздатностей, який відлякує потенційного противника від здійснення кібератак. Цей принцип передбачає демонстрацію кібермożливостей держави та готовність до негайної відповіді на будь-які ворожі дії. Ефективне стримування передбачає наявність як оборонних, так і наступальних кіберінструментів, здатних забезпечити високий рівень безпеки та відповісти на агресію симетрично або асиметрично. Досягнення кіберстримування вимагає міжвідомчої та міжнародної співпраці, оскільки спільні зусилля держав і організацій, таких як НАТО або ЄС, значно підвищують здатність до колективного захисту та утримують агресора від нападу.

Таким чином, кібероперації є важливим елементом військової стратегії, що надає державі значний арсенал інструментів для захисту, атак та стримування у кіберпросторі, сприяючи посиленню національної безпеки та забезпечуючи стратегічні переваги на сучасному полі бою [7].

Зростання ролі кіберпростору у забезпеченні національної безпеки привело до розробки ефективних кіберстратегій і практик кібероборони у провідних державах світу. Країни НАТО, США, Ізраїль та інші держави з розвиненими кіберздатностями розробили комплексний підхід до кібероборони, який включає як технічні, так і організаційні аспекти. Їхній досвід є цінним для України, особливо в умовах підвищених кіберзагроз.

Кібероборона є важливою складовою оборонної стратегії НАТО, що визначено у «Політиці кіберзахисту» та оновленій «Концепції колективної оборони». НАТО розглядає кібератаки як потенційні підстави для колективної відповіді, зокрема в рамках статті 5 Північноатлантичного договору. Стратегії НАТО охоплюють як оборонні, так і наступальні операції у кіберпросторі, зокрема кібернавчання (наприклад, навчання Cyber Coalition), спільний кібермоніторинг і обмін інформацією між державами-членами. Важливим є також використання спільної платформи обміну даними та інструментів для забезпечення оперативної кібербезпеки. НАТО зосереджується на розвитку стійкості національних систем та критичної інфраструктури, а також сприяє підготовці спеціалістів через регулярні тренування та симуляції кіберзагроз [8].

Сполучені Штати є однією з найбільш розвинених країн у сфері кібероборони та наступальних кібероперацій. Стратегія США у кіберпросторі базується на концепції «захисту вперед» (defend forward), яка передбачає проактивний захист і стримування загроз за рахунок виявлення та нейтралізації кібератак ще до їхнього проникнення у критичні мережі США. Центральним елементом є Кіберкомандування США (USCYBERCOM), що відповідає за проведення стратегічних операцій та кіберзахист в інтересах національної безпеки. USCYBERCOM інтегрує кіберкомпоненти всіх військових підрозділів США та підтримує спільну координацію з ФБР, Агентством національної безпеки (NSA), приватним сектором та союзниками. США також активно інвестують у технології кіберзахисту, зокрема штучний інтелект, аналітику великих даних та автоматизацію захисних систем [6, с. 141].

Ізраїль є прикладом інноваційного підходу до кібероборони завдяки інтенсивному розвитку кіберінфраструктури, високій підготовці кадрів та ефективній співпраці

між державою та приватним сектором. Кібербезпека в Ізраїлі керується Національним кібердиректоратом, який координує зусилля у сфері національної безпеки, цивільного захисту та економічного кіберрозвитку. Значна частина кібероперацій здійснюється силами військових, зокрема підрозділами Армії оборони Ізраїлю, відомими як підрозділ 8200, що спеціалізується на зборі розвідданих та проведенні наступальних кібероперацій. Ізраїль також розробив комплексні системи кіберрозвідки, аналізу загроз та раннього виявлення атак, що дозволяє вчасно реагувати на можливі ризики. Інновації та співпраця з провідними технологічними компаніями сприяють розробці нових інструментів для захисту критичної інфраструктури [2, с. 47–48].

Україна може використати міжнародний досвід, зокрема США, НАТО та Ізраїлю, для розробки національної кіберстратегії, орієнтованої на захист та розвиток кіберздатностей. Адаптація концепції «захисту вперед» США дозволить стримувати загрози на ранніх етапах, а обмін даними на зразок систем НАТО сприятиме швидкій реакції на кіберзагрози. Підхід Ізраїлю щодо співпраці з приватним сектором і розвитку кібернавичок серед молоді допоможе створити кадровий резерв, а його досвід у наступальних кіберопераціях стане корисним для оборони України в умовах гібридної війни.

Важливо зазначити, що в умовах посилення кіберзагроз національне законодавство відіграє центральну роль у забезпеченні кібербезпеки та кібероборони, регулюючи діяльність органів державної влади, установ, приватного сектору та громадян у цій сфері. Українське законодавство визначає засади національної кібербезпеки та кібероборони через такі основні документи, як Закон України «Про основні засади забезпечення кібербезпеки України», ухвалений у 2017 році, а також через відповідні розпорядження, накази та стратегії.

Закон «Про основні засади забезпечення кібербезпеки України» встановлює правові основи для запобігання, виявлення та реагування на кіберзагрози, розподіляє функції і повноваження між основними суб'єктами у сфері кібербезпеки, такими як Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), Служба безпеки України (СБУ), Міністерство оборони України тощо. Законодавство передбачає створення комплексної системи кіберзахисту, що включає механізми моніторингу, координацію між органами влади, впровадження стандартів інформаційної безпеки та розвиток кіберінфраструктури [1].

Окрім цього, законодавчі акти зобов'язують державні органи та критичні інфраструктури впроваджувати стандарти кіберзахисту, розробляти та дотримуватися планів реагування на кіберінциденти, а також регулярно проводити навчання та кібернавчання. Важливим напрямом є розвиток державно-приватного партнерства, що дозволяє залучати до системи кібероборони приватні компанії та інші недержавні суб'єкти. Українське національне законодавство також активно вдосконалюється для адаптації до нових кіберзагроз, посилення міжнародного співробітництва у цій сфері та гармонізації з нормами Європейського Союзу.

Міжнародні правові норми, зокрема Статут ООН, Женевські конвенції та Талліннське керівництво, забезпечують правову основу для регулювання кібероперацій, особливо у збройних конфліктах. Стаття 2 (4) Статуту ООН забороняє агресію, яка поширюється й на кібероперації, здатні спричинити фізичну шкоду або серйозні збої в критично важливих системах. Міжнародне гуманітарне право також передбачає гуманність, пропорційність та захист цивільних об'єктів, що стосується і кіберпростору. Талліннське керівництво, хоча й не є офіційним, надає рекомендації для інтеграції кібероперацій у військові стратегії згідно з міжнародним правом, що допомагає Україні у створенні правових основ для захисту та розвитку кіберздатностей [5, с. 52].

Сучасна кібероборона дедалі більше спирається на інноваційні технології, що дозволяють підвищити ефективність протидії кіберзагрозам. Одним із провідних інструментів у цій сфері є штучний інтелект (ШІ), який забезпечує аналіз даних, прогнозування атак, виявлення та реагування на аномалії в реальному часі. Використання ШІ дозволяє здійснювати глибоке сканування мережевих активностей, оцінювати ризики та навіть автоматично усувати кіберзагрози, що знижує залежність від людського фактору й дозволяє своєчасно реагувати на потенційні інциденти.

Аналіз великих даних (Big Data) також є критичним елементом кібероборони, оскільки дає змогу обробляти величезні обсяги інформації з різних джерел, що допомагає виявляти патерни поведінки зловмисників та аномалії, які можуть свідчити про загрози. Завдяки технологіям великих даних, аналітики можуть ідентифікувати схожі кіберінциденти, розуміти їх закономірності, передбачати подібні атаки в майбутньому та адаптувати захисні заходи під специфіку нових видів загроз.

Автоматизація кіберзахисту за допомогою технологій ШІ та Big Data дозволяє здійснювати моніторинг кіберпростору в режимі реального часу, знижувати час виявлення і нейтралізації атак. Розробка інтегрованих автоматизованих систем кіберзахисту, здатних забезпечувати постійне оновлення алгоритмів захисту та адаптацію до нових загроз, є важливим напрямом розвитку сучасної кібероборони [3, с. 779–780].

Інвестиції в дослідження і розробки (R&D) є критично важливим компонентом для підтримання кібероборони на рівні сучасних викликів та забезпечення готовності до майбутніх загроз. Уряди провідних країн, а також комерційний сектор активно фінансують розробку передових технологій у сфері кібербезпеки, включаючи системи автоматизованого реагування на інциденти, криптографічні технології, мережеві засоби захисту та інтелектуальні платформи для моніторингу та аналізу кіберзагроз.

В Україні значення R&D зростає у зв'язку з потребою в удосконаленні національних кіберздатностей та підвищенні ефективності кібероборони. Збільшення фінансування на дослідження і розробки в сфері кібербезпеки дозволить Україні розвивати інноваційні технології, розширювати інструментарій протидії загрозам, адаптувати існуючі системи під нові умови та забезпечувати технологічну самодостатність. Інвестиції в R&D також стимулюють зростання науково-технічного потенціалу країни, сприяючи підготовці висококваліфікованих фахівців, які зможуть працювати над зміцненням кібербезпеки [4, с. 116].

З огляду на стрімкий розвиток технологій і зростання числа кіберзагроз, інтеграція кібероборони у військові стратегії стала однією з ключових умов забезпечення національної безпеки. Крім традиційних форм протидії загрозам, особливої уваги набуває сфера інформаційної війни, що використовує кіберпростір як майданчик для поширення дезінформації та маніпуляції громадською думкою. Розуміння методів ведення інформаційної війни та розвиток ефективних засобів для її стримування є важливими для запобігання дестабілізації суспільства та підриву довіри до державних інституцій. У цьому контексті дослідження кіберпропаганди та механізмів протидії інформаційним атакам набуває стратегічного значення для забезпечення цілісності інформаційного простору країни.

Завдяки сучасним технологіям аналізу великих даних, штучному інтелекту та автоматизованим алгоритмам, кібероперації у сфері інформаційної війни можуть бути високоточними, масштабованими і швидкодіючими. Інформаційні атаки проводяться через створення бот-мереж, використання штучного інтелекту для персоналізації дезінформаційних повідомлень, а також поширення шкідливих програм, які обмежують доступ до правдивої інформації. Інформаційна війна охоплює широкий

спектр активностей, включаючи фальшиві акаунти, «тролінг» у соціальних медіа, використання фальсифікованих відео та зображень для маніпуляції емоціями громадян, що ускладнює розрізнення між правдивою і неправдивою інформацією.

Протидія інформаційним атакам та кіберпропаганді вимагає багаторівневого підходу, що включає як технічні засоби, так і підвищення інформаційної грамотності населення. Основними заходами протидії є впровадження систем моніторингу та виявлення дезінформації, розвиток інформаційних кампаній для підвищення обізнаності населення, а також співпраця між державними органами, громадськими організаціями і приватним сектором [5, с. 54–55].

Технологічні засоби протидії інформаційним атакам включають використання штучного інтелекту та алгоритмів машинного навчання для автоматизованого виявлення підозрілих патернів поведінки у соціальних мережах, блокування бот-акаунтів та аналізу інформаційних потоків на предмет поширення дезінформації. Важливим аспектом є інтеграція платформ фактчекінгу, які дозволяють швидко перевіряти достовірність інформації та спростовувати фальшиві новини.

Іншим ефективним заходом є підвищення рівня медійної грамотності та критичного мислення серед громадян. Проведення освітніх програм, розробка інформаційних кампаній, що сприяють усвідомленню ризиків дезінформації, а також підтримка журналістів і громадських активістів сприяє створенню критичної маси освічених громадян, здатних розпізнавати кіберпропаганду. Водночас держава повинна посилювати законодавче регулювання у сфері інформаційної безпеки та кіберзахисту, розробляючи політику протидії кіберпропаганді та зміцнюючи співпрацю з міжнародними організаціями для боротьби з глобальними інформаційними загрозами [3, с. 784].

Посилення кіберзахисту та протидія інформаційним загрозам є лише частиною комплексної стратегії забезпечення національної безпеки в умовах сучасних кіберризиків. Однак для побудови надійної системи кібероборони Україна стикається з низкою серйозних викликів, які потребують вирішення на рівні державної політики та ресурсного забезпечення.

Одним із найбільших викликів є недофінансування, що обмежує можливості для розробки нових технологій, забезпечення якісного кіберзахисту державних інституцій та створення ефективних систем для протидії кіберзагрозам.

Іншою значною проблемою є кадровий дефіцит у сфері кібербезпеки. Відтік кваліфікованих фахівців до приватного сектору та за кордон спричиняє нестачу досвідчених професіоналів у державних структурах. Відсутність достатньої кількості фахівців із сучасними навичками значно ускладнює розробку та реалізацію стратегічних ініціатив у сфері кібероборони.

Також слід відзначити недостатню інтеграцію між відомствами, що займаються кібербезпекою. Відсутність чіткої координації між державними установами, відповідальними за кібероборону, призводить до дублювання зусиль, неефективного використання ресурсів та ускладнює оперативне реагування на кіберзагрози [7].

Попри значні виклики, Україна має довгострокові перспективи у розвитку кіберздатностей. Важливим аспектом є впровадження новітніх технологій, таких як штучний інтелект, автоматизація кіберзахисту та аналіз великих даних, що дозволить суттєво підвищити ефективність і швидкість виявлення загроз. Використання інноваційних рішень дозволить Україні краще адаптуватися до нових типів кіберзагроз, забезпечивши проактивну стратегію захисту.

Іншим важливим напрямом є посилення міжнародної співпраці у сфері кібербезпеки. Співпраця з країнами НАТО, Європейським Союзом та іншими партнерами

дозволить обмінюватися знаннями та передовими практиками, а також отримувати технічну підтримку та консультації з удосконалення національної кібероборони. Інтеграція в міжнародні програми та проєкти допоможе Україні використовувати накопичений світовий досвід для розвитку власних кіберздатностей та формування більш стійкої кібероборони.

Висновки. Отже, інтеграція кібероперацій у військову стратегію України є важливим напрямом у зміцненні національної безпеки та захисту від сучасних загроз, що стають дедалі інтенсивнішими в умовах повномасштабної війни. Досвід провідних країн демонструє необхідність створення гнучкої кіберстратегії, що базується на принципах активного стримування, оперативної координації між відомствами та тісної співпраці з приватним сектором. Ефективне використання кібероперацій вимагає не лише високого технологічного потенціалу, але й відповідної нормативно-правової бази, яка б враховувала міжнародні стандарти і принципи міжнародного гуманітарного права. Завдяки адаптації кращих практик і правових норм, Україна може посилити свій кіберзахист, використовуючи сучасні технології, включаючи штучний інтелект, аналіз даних та автоматизацію. Це сприятиме не лише зміцненню внутрішньої безпеки, але й поліпшенню здатності до ефективної інтеграції з міжнародними партнерами в рамках спільних кібербезпекових ініціатив.

Подальші дослідження мають зосередитись на розробці національної стратегії кібероборони з урахуванням специфіки українських загроз та вимог міжнародного права, а також на вдосконаленні механізмів кібероборони і підвищенні кіберстійкості критичної інфраструктури.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017, № 2163-VIII. URL: https://zakon. rada. gov. ua (дата звернення: 11.11.2024).

2. Гребенюк М. В., Леонов Б. Д. Досвід Ізраїлю у сфері забезпечення кібербезпеки. *Інформація і право.* 2018. № 2. С. 45–50

3. Коротченко Л., Дєгтярь О., Атаманенко М. та ін. Аналіз метододів кібервійн та кібероперацій, які використовуються провідними країнами світу та членами НАТО. *Наука і техніка сьогодні.* 2024. № 7 (35). С. 776–788. DOI: https://doi.org/10.52058 / 2786–6025–2024–7 (35).

4. Ляшенко І. О., Кириленко В. А. Кібернетичні операції – майбутня форма збройної боротьби: підручник. Харків, 2018. 176 с.

5. Машталір В. В., Шиповський В. В. Аналіз подій у кіберпросторі у процесі російсько-української війни 2022 року: висновки, рекомендації, засвоєні уроки. *Наука і оборона*. 2023. № 4. С. 48–56.

6. Стежко С. М., Шевченко Т. О., Сучасний досвід США у сфері забезпечення кібербезпеки. *Інформація і право*. 2021. №2 (37). С. 139–144. DOI: https:// doi. org/10.37750/2616–6798.2021.2 (37). 238349

7. Ткачук Н. А. Досвід США зі створення та розбудови кіберкомандування: уроки для України. *International Scientific Journal «Internauka». Ser.: Juridical Sciences.* 2024. № 1 (48): веб-сайт. DOI: https://doi.org/10.25313/2520–2308–2023–11.

8. Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation. Active Engagement, Modern Defence / NATO: веб-сайт. URL: http:// www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf. (дата звернення: 10.11.2024)

Дата надходження статті до редакції: 10.06.2025
Дата затвердження статті до друку: 02.07.2025
Дата публікації статті: 03.10.2025