Філософія, методологія, теорія та історія основ національної безпеки держави

УДК 351:316.77]:342.77

Шевчук Юрій Володимирович
аспірант кафедри публічного адміністрування
Міжрегіональної Академії управління персоналом
Shevchuk Yurii
Postgraduate Student of the Department of Public Administration
Interregional Academy of Personnel Management
ORCID: 0009-0002-6562-0326

Сліпчук Юрій Андрійович
аспірант кафедри публічного адміністрування
Міжрегіональної Академії управління персоналом
Slipchuk Yury
Postgraduate Student of the Department of Public Administration
Interregional Academy of Personnel Management
ORCID: 0009-0006-7244-1843

ВИКОРИСТАННЯ КІБЕРПРОСТОРУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ВІЙСЬКОВИМИ ОПЕРАЦІЯМИ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ ДЛЯ ДЕРЖАВНОГО УПРАВЛІННЯ

UTILIZING CYBERSPACE TO ENHANCE THE EFFECTIVENESS OF MILITARY OPERATIONS MANAGEMENT: CHALLENGES AND PROSPECTS FOR STATE MANAGEMENT

Анотація. *Вступ. У сучасних умовах ведення бойових дій використання кіберпростору стає невід'ємною складовою військових операцій. Інформаційні технології відкривають нові можливості для управління військовими силами,*

дозволяючи швидше та ефективніше приймати рішення, координувати дії підрозділів і забезпечувати надійний зв'язок на всіх рівнях командування. Однак, разом із перспективами кіберпростір також приносить низку викликів, які потребують ретельного аналізу та відповідних заходів для захисту національної безпеки.

Мета - здійснити аналіз викликів, пов'язаних з використанням кіберпростору для підвищення ефективності управління військовими операціями. Матеріали і методи. Визначення ролі державного управління у забезпеченні кібербезпеки та розвитку національних кіберспроможностей у статті вибудовується на основоположних положеннях із державного управління, економіки, досягненнях сучасної наукової думки на основі міждисциплінарного підходу. Методологічний інструментарій передбачає використання як загальнонаукових методів пізнання, так і спеціальних. Також у роботі знайшов інструментальне застосування один із ключових показників кіберпотужності країни – Національний індекс кібербезпеки (NCSI).

Результати. Національний індекс кібербезпеки оцінює готовність держав до протидії кіберзагрозам та управління кіберінцидентами. Україна отримала високу оцінку у 75,32 бала за NCSI у 2022 році, що забезпечило їй 24-те місце в глобальному рейтингу, перевищуючи середній рівень і демонструючи високий рівень кіберзахисту. Кіберпростір не тільки дозволяє інтегрувати сучасні технології, такі як штучний інтелект і великі дані, у військові процеси, але й створює нові загрози, як-от кібератаки на критичну інфраструктуру.

Національний індекс кіберпотужності (NCPI) враховує національні цілі та оцінює ефективність державних стратегій у кібербезпеці. Цей індекс дозволяє оцінювати не тільки потужність держави у кіберпросторі, але й

ефективність використання її можливостей. Важливими аспектами є здатність держави реагувати на кібератаки, розподіл ресурсів, участь приватного сектору та рівень інновацій у кібербезпеці.

Для ефективного управління військовими операціями в умовах гібридної війни необхідно створювати гібридні військово-цивільні підрозділи, здатні діяти у кіберпросторі. Це передбачає взаємодію між Збройними Силами України, організаціями публічного сектору та приватним сектором на основі існуючих законодавчих механізмів. Адміністративно-правові засади та активне залучення приватного сектору є ключовими елементами у побудові ефективної системи кібербезпеки для підвищення ефективності управління військовими операціями.

Перспективи. Для державного управління сучасний етап суспільного розвитку створює необхідність у розробці нових стратегій захисту та використання кіберможливостей. Серед країн, які досягли найвищих показників кібербезпеки, такі держави, як Греція, Бельгія та Литва, займають провідні позиції, тоді як агресори, такі як Росія та Білорусь, отримали значно нижчі оцінки, що підкреслює перевагу України у цій сфері.

Ключові слова: *кібербезпека, військові операції, кіберпростір, державне управління, національний індекс кібербезпеки, гібридна війна, кіберпотужність, державно-приватна взаємодія, кіберзагрози, інноваційні технології, "добре врядування".*

Summary. *Introduction. In modern conditions of warfare, the use of cyberspace is becoming an integral part of military operations. Information technologies open up new opportunities for managing military forces, allowing for faster and more effective decision-making, coordination of unit actions, and reliable communication at all levels of command. However, along with the prospects,*

cyberspace also brings a number of challenges that require careful analysis and appropriate measures to protect national security.

The goal is to analyze the challenges associated with the use of cyberspace to improve the effectiveness of military operations management. Materials and methods. The definition of the role of public administration in ensuring cybersecurity and the development of national cyber capabilities in the article is built on the fundamental principles of public administration, economics, and achievements of modern scientific thought based on an interdisciplinary approach. The methodological tools involve the use of both general scientific methods of cognition and special ones. The work also found instrumental application in one of the key indicators of a country's cyber power - the National Cybersecurity Index (NCSI).

Results. The National Cybersecurity Index assesses the readiness of states to counter cyber threats and manage cyber incidents. Ukraine received a high score of 75.32 points for the NCSI in 2022, which provided it with 24th place in the global ranking, exceeding the average level and demonstrating a high level of cyber protection. Cyberspace not only allows for the integration of modern technologies, such as artificial intelligence and big data, into military processes, but also creates new threats, such as cyberattacks on critical infrastructure.

The National Cyberpower Index (NCPI) takes into account national goals and assesses the effectiveness of state strategies in cybersecurity. This index allows you to assess not only the power of the state in cyberspace, but also the effectiveness of using its capabilities. Important aspects are the state's ability to respond to cyberattacks, resource allocation, private sector participation, and the level of innovation in cybersecurity.

For effective management of military operations in the context of hybrid warfare, it is necessary to create hybrid military-civilian units capable of operating in cyberspace. This involves interaction between the Armed Forces of Ukraine,

public sector organizations, and the private sector based on existing legislative mechanisms. Administrative and legal frameworks and active involvement of the private sector are key elements in building an effective cybersecurity system to improve the efficiency of military operations management.

Prospects. For public administration, the current stage of social development creates the need to develop new strategies for protecting and using cyber capabilities. Among the countries that achieved the highest cybersecurity indicators, states such as Greece, Belgium and Lithuania occupy leading positions, while aggressors such as Russia and Belarus received significantly lower scores, which emphasizes Ukraine's superiority in this area.

Key words: *cybersecurity, military operations, cyberspace, public administration, national cybersecurity index, hybrid warfare, cyberpower, public-private interaction, cyber threats, innovative technologies, "good governance".*

Постановка проблеми. У сучасних умовах ведення бойових дій використання кіберпростору стає невід'ємною складовою військових операцій. Інформаційні технології відкривають нові можливості для управління військовими силами, дозволяючи швидше та ефективніше приймати рішення, координувати дії підрозділів і забезпечувати надійний зв'язок на всіх рівнях командування. Однак, разом із перспективами кіберпростір також приносить низку викликів, які потребують ретельного аналізу та відповідних заходів для захисту національної безпеки.

З одного боку, кіберпростір надає можливість інтеграції сучасних технологій, таких як штучний інтелект, великі дані та автоматизація, у військові процеси, що дозволяє підвищити оперативну ефективність та знизити ризики людського фактору. З іншого боку, зростає загроза кібератак, які

можуть спричинити значні збитки, порушити роботу критичної інфраструктури та знизити ефективність військових операцій.

Для державного управління виникає необхідність розробки та впровадження нових стратегій, спрямованих на захист кіберпростору, підвищення кібербезпеки та використання кіберможливостей для підтримки військових операцій. Це вимагає інтеграції кібертехнологій у систему державного управління, створення спеціалізованих підрозділів для реагування на кібератаки, а також проведення регулярних навчань і тренувань для підвищення готовності військових та цивільних фахівців.

Аналіз останніх досліджень і публікацій. Українські вчені (Кондрашова Т., Кондрашов Д., Костюченко С., Лобода Ю., Магда Є., Номінатюк О., Пономарчук С., Терещук Т.) активно досліджують проблему кібербезпеки в контексті сучасних військових конфліктів. Вони аналізують складність і багатогранність гібридних війн, зокрема, як ці загрози впливають на традиційні військові стратегії та державне управління. Особлива увага приділяється адміністративно-правовим аспектам інтеграції військових і цивільних структур для побудови ефективної системи кіберзахисту [3; 5-4; 10-12].

Метою статті є аналіз основних викликів і перспектив, пов'язаних з використанням кіберпростору для підвищення ефективності управління військовими операціями, а також на визначення ролі державного управління у забезпеченні кібербезпеки та розвитку національних кіберспроможностей.

Виклад основного матеріалу. Національний індекс кібербезпеки (далі – NCSI) є глобальним показником, що оцінює готовність країн до протидії кіберзагрозам та управління кіберінцидентами. Окрім того, NCSI слугує базою даних із відкритими матеріалами та інструментами, що сприяють розвитку національного потенціалу кібербезпеки. Згідно з рейтингом 2022 року, Україна

здобула оцінку 75,32 у Національному індексі кібербезпеки, що дозволило їй зайняти 24-те місце в загальному рейтингу. Цей показник суттєво перевищує середній рівень, демонструючи високий рівень готовності країни до кіберзахисту.

Серед країн, які очолюють рейтинг, найвищі оцінки отримали Греція (96), Бельгія (93), Литва (93), Естонія (90), Чехія (92), Німеччина (90), Португалія (89), Іспанія (88), Польща (87), Фінляндія (85) та Швеція (84). Україна з оцінкою 75,32 знаходиться серед лідерів кібербезпеки в Європі, випереджаючи такі країни, як Австрія, Ірландія та Норвегія. Це свідчить про значний прогрес у сфері кібербезпеки, особливо в порівнянні з іншими регіонами.

Примітно, що агресори, такі як Російська Федерація та Білорусь, отримали значно нижчі оцінки – 71 та 53 відповідно, що підкреслює перевагу України в цьому критичному напрямку національної безпеки.

Індекс NCSI був розроблений і впроваджений Фондом академії електронного врядування Естонії. На відміну від нього, Глобальний індекс кібербезпеки (GCI), створений Міжнародним союзом електрозв'язку (МСЕ), є ініціативою, спрямованою на підвищення обізнаності щодо кібербезпеки та оцінку прихильності країн до її впровадження в різних галузях. Оцінка розвитку кібербезпеки в кожній країні проводиться за п'ятьма ключовими категоріями: правові заходи, технічні заходи, організаційні заходи, розбудова потенціалу та співробітництво.

На відміну від існуючих кіберіндексів, Національний індекс кіберпотужності (NCPI) складається з кількох компонентів і враховує національні цілі кожної країни. Цей індекс формується для держави в цілому, проте фокусується лише на тих аспектах діяльності, які перебувають під контролем уряду або інших державних інститутів.

NCPI дозволяє оцінювати ефективність державної стратегії, реакцію на правопорушення та боротьбу з ними, обороноздатність, розподіл ресурсів, участь приватного сектору, а також рівень ефективності робочої сили та інновацій у сфері кібербезпеки. Це одночасно є вимірюванням як доведеної потужності, так і потенціалу, а також ефективності використання цих можливостей урядом кожної країни, що бере участь у рейтингу [11].

NCPI визначає сім основних національних цілей, які зазвичай переслідуються владою країн для досягнення необхідного рівня кібербезпеки:

– застосування практик нагляду та моніторингу на загальнодержавному рівні за участю внутрішніх груп контролю;

– національна програма (стратегія) кібербезпеки;

– контроль та управління інформаційним середовищем;

– спеціалізована діяльність зовнішньої розвідки з питань національної кібербезпеки;

– випуск спеціалізованої продукції вітчизняного виробництва;

– здатність знищувати або відключати інформаційно-комунікаційну інфраструктуру та можливості супротивника;

– визнання та використання міжнародних стандартів та технічних норм.

Відмінність NCPI від традиційного уявлення про кіберпотужність, яка часто асоціюється лише з можливістю знищення або виведення з ладу інфраструктури супротивника через наступальні кібероперації, полягає в тому, що індекс також враховує ефективність реагування на кіберінциденти та боротьбу з ними, що суттєво впливає на загальну оцінку. Іншими важливими параметрами для формування NCPI є традиційні військові засоби, дипломатичні заходи, державна політика, кримінальна практика, бізнес-

процеси та інші ресурси, доступні країнам для досягнення визначених національних цілей.

Національний індекс кіберпотужності вимірює "всебічність" країни як кіберсуб'єкта. У цьому контексті всебічність означає збалансовану оцінку поєднання національних цілей, намірів і можливостей їх досягнення. На практиці NCPI інтегрує два інших показники – індекс кібернамірів (CII) та індекс кіберздатності (CCI), проте комплексний характер має саме NCPI.

Розробники NCPI зазначають, що вимірювання національного індексу кіберпотужності базується на актуальних базах даних, які стосуються конкретних елементів національних екосистем кібербезпеки та включають значну кількість факторів, отриманих самостійно. Також є можливість отримати за запитом будь-яку інформацію, що впливає на формування індексу для конкретної країни [4].

Національна безпека є основою стабільного розвитку суспільства. В умовах гібридної війни, спрямованої проти України, виникає необхідність перегляду традиційних підходів до забезпечення безпеки. Військові дії, що поєднують звичайні та кіберзагрози, вимагають нових методів захисту та управління. Аналіз медіа-джерел та наукових публікацій свідчить про те, що для ефективної протидії гібридним викликам необхідно створювати гібридні військові підрозділи, здатні діяти в умовах кіберпростору.

Положення Договору про Європейський Союз та Лісабонського договору (2009 р.) закладають основи для формування гібридного військово-цивільного співробітництва з метою нейтралізації кіберзагроз. Це передбачає створення:

– сфери постійного оборонного співробітництва в Європі: забезпечення безперервної координації між державами-членами для оперативної відповіді на кіберзагрози;

– постійного структурного співробітництва (PESCO) в області оборони: ініціатива, яка об'єднує 25 країн ЄС, включаючи Австрію, Бельгію, Німеччину, Францію та інші, для спільної роботи над оборонними проектами, зокрема у сфері кібербезпеки.

Програма PESCO охоплює два основні проєкти, пов'язані з кібербезпекою:

1. Платформа обміну інформацією про кіберзагрози: проєкт спрямований на створення проактивних заходів захисту та розробку загальної мережевої платформи для обміну інформацією про кіберзагрози. Відповідальною країною є Греція, яка забезпечує підтримку через Європейське агентство з мережевої та інформаційної безпеки (ENISA).

2. Команда швидкого реагування на кіберзагрози: проєкт забезпечує колективну реакцію держав-членів на кіберінциденти, підвищуючи рівень кіберстійкості. Організація та управління цими командами здійснює Литва, яка ініціювала створення кіберпідрозділів швидкого реагування.

Генеральний секретар НАТО Й. Столтенберг підкреслює важливість гібридної співпраці між НАТО та ЄС для ефективного реагування на зростаючі кіберзагрози. Співпраця базується на спільній Декларації 2016 року, яка визначає пріоритетні напрямки взаємодії у сфері кібербезпеки та кібероборони. Наприклад, у 2017 році в Естонії відбулися спільні навчання "Di-Si Cannabis Coalition" для перевірки здібностей до протидії кібератакам на національному та міжнародному рівнях.

Подальший розвиток співпраці включає участь держав, що не є членами Альянсу, таких як Японія. У 2018 році, після участі японських фахівців у навчаннях з кібербезпеки в Естонії, Японія переглянула свою національну оборонну програму та створила командний центр для управління операціями в космосі та кіберпросторі, що співпрацює з НАТО та США.

Згідно з джерелами [8; 9], компетенції бізнесу та приватного сектору є невід'ємною частиною ефективного гібридного механізму захисту об'єктів критичної інфраструктури. Приватний сектор забезпечує необхідні ресурси та експертизу для створення стійких систем захисту від кіберзагроз.

В Україні пропонується організувати функціонування та взаємодію Збройних Сил України з державними організаціями та приватним сектором на основі Закону України "Про основні засади забезпечення кібербезпеки України" [2]. Зокрема, стаття 10 цього закону визначає механізми державно-приватної взаємодії у сфері кібербезпеки, включаючи створення системи виявлення та нейтралізації кіберзагроз, підвищення цифрової грамотності громадян, обмін інформацією між державними органами та приватним сектором, а також залучення експертного потенціалу для підготовки проектів та нормативних документів у сфері кібербезпеки.

На підставі статті 10 Закону України пропонується реалізувати державно-приватну взаємодію не лише під час інформаційних операцій, але й на постійній основі для забезпечення кібербезпеки. Це передбачає співпрацю Збройних Сил України з фахівцями приватного сектору, включаючи дистанційну роботу та альтернативну військову службу для спеціалістів з кібербезпеки. Такий підхід дозволить залучити мотивованих та кваліфікованих фахівців, створити взаємодію для оперативного реагування на кіберзагрози та забезпечити економію на військовому забезпеченні.

«Стратегія кібербезпеки України» – це стратегічний документ, спрямований на захист інформаційних ресурсів, кіберінфраструктури та кіберпростору держави від кіберзагроз. Вона визначає пріоритети та заходи для забезпечення кібербезпеки, включаючи розвиток технічних та правових засобів захисту, підвищення кіберінформаційної свідомості населення та зміцнення міжнародного співробітництва в цій сфері. Останніми

нововведеннями у сфері національної безпеки є посилення уваги до інформаційно-комунікаційних технологій і важливості кібербезпеки. Зокрема новими викликами національній безпеці визнані: штучний інтелект, безпілотні літальні апарати та інші безпілотні платформи, далекобійна високоточна зброя, у т.ч. балістичні і крилаті ракети. До прикладу, Польща підтримує заходи щодо розробки та впровадження норм відповідальної поведінки держави в кіберпросторі, застосування до нього існуючих принципів міжнародного права та розробки заходів зміцнення довіри між країнами. Наразі у світі провадиться співпраця країн ЄС з союзниками по НАТО та партнерами з ЄС для запобігання гібридним загрозам і стійкості до них. З іншого боку, розвиток таких технічних напрямків, як: широкосмугові мережі стаціонарного і мобільного зв'язку (5G і наступних поколінь), квантова технологія, нанотехнологія або штучний інтелект уможливлюють створення нових оборонних і ударних можливостей.

Внаслідок інформаційної революції спостерігається формування нового парадигматичного виміру інформаційної реальності, який представлений у вигляді глобальної інформаційної інфраструктури. Дії провідних світових держав у будівництві інформаційного суспільства, їхня тенденція до інформаційного домінування та встановлення контролю над напрямками та змістом інформаційних потоків породжують нового роду протиріччя, які вирішення зараз неможливе традиційними методами управління.

У ході дослідження була проаналізована політика ЄС у сфері кібербезпеки, критичної інформаційної інфраструктури в контексті євроінтеграції та врахування європейського досвіду у забезпеченні. Водночас, впровадження системи інформаційної безпеки для кожного конкретного об'єкта критичної інформаційної інфраструктури відбувається відповідно до

технічного завдання на створення системи інформаційної безпеки, визначеного для цього об'єкта.

До прикладу, у Республіці Польща діє Національний Центр Керування, який є ключовою інституцією, призначеною для координації та керування у ситуаціях надзвичайних подій, зокрема природних катастроф або терористичних загроз. Завдяки своєму функціоналу, центр визначається як невід'ємна частина національної системи безпеки Польщі. Його завданням є не тільки ефективне управління надзвичайними ситуаціями, але й забезпечення співпраці між різними структурами, що включають громадські організації та силові відомства. Варто згадати також Національну Агенцію Кібербезпеки (Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni) роль якої наразі суттєво зросла в питаннях національної безпеки. Національна Агенція Кібербезпеки є спеціалізованим органом, призначеним для розробки та впровадження стратегій та заходів, спрямованих на захист національних інформаційних ресурсів від потенційних кіберзагроз та кібератак. Ця агенція є ключовим елементом національної системи кібербезпеки, відповідаючи за формування та реалізацію стратегічних підходів до забезпечення стійкості та надійності інформаційно-комунікаційної інфраструктури країни. Ця агенція виконує розширений спектр функцій, включаючи моніторинг кіберпростору, аналіз потенційних загроз, розробку стандартів безпеки, організацію тренувань та навчань для персоналу, а також взаємодію з міжнародними агентствами для обміну інформацією та впровадження найкращих практик у сфері кібербезпеки.

Посилення кібербезпеки вимагає дотримання міжнародних правил поведінки, стандартів і норм.

Федеральний уряд Німеччини визначає десять стратегічних сфер: захист критичних інформаційних інфраструктур, захищені IT-системи в Німеччині,

посилення IT-безпеки в державному управлінні, діяльність Національного центру кіберзахисту, діяльність Національної ради з кібербезпеки, ефективну боротьбу зі злочинністю у кіберпросторі, ефективні скоординовані дії для забезпечення кібербезпеки в Європі та світі, використання надійних і надійних інформаційних технологій, розвиток кадрів у федеральних органах влади, інноваційні інструменти реагування на кібератаки. Так, органи державної влади мають служити прикладом для наслідування безпеки даних. Вони створюють загальну, уніфіковану та безпечну мережеву інфраструктуру у федеральній адміністрації («федеральні мережі») як основу для електронної передачі даних. Ефективна IT-безпека потребує потужних структур у всіх федеральних органах влади. З цієї причини ресурси повинні бути розподілені належним чином на центральному та місцевому рівнях. Національний центр кіберзахисту (Cyber-AZ), що базується в Бонні, не є незалежним органом, а скоріше представляє спільну, міжвідомчу та міжінституційну платформу. Він був заснований у 2011 р. в рамках реалізації Стратегія кібербезпеки федерального уряду.

Вісім основних органів влади та партнерів наразі співпрацюють у рамках National Cyber-AZ: Федеральне управління служби військової контррозвідки; Федеральне управління кримінальної поліції; Федеральне відомство з безпеки інформаційних технологій; Федеральне відомство з охорони конституції; Федеральне відомство цивільного захисту та ліквідації наслідків стихійних лих; Кібернетичне та інформаційне командування Бундесверу; Федеральна поліція; Федеральна служба розвідки. Партнерами виступають: Кіберзахист Баварії, Hessen CyberCompetenceCenter (Hessen3C), Кіберпрокурори з Бамберга та Кельна, Федеральний орган фінансового нагляду. Координатор Cyber-AZ бере на себе роль модератора між залученими представниками влади, а також може ініціювати необхідні рішення. Керівна група, в якій беруть

участь усі основні органи влади та, як виняток, партнерські органи влади, приймає рішення щодо тематичних пріоритетів на своїх засіданнях та створює робочі групи. Тут мають право голосу лише основні органи влади, але не партнери.

Під час щоденного ситуаційного брифінгу контактні особи повідомляють поточні висновки своїх органів влади щодо кібернетичних питань, збагачують один одного інформацією та отримують з цього будь-які необхідні роз'яснення та дії. Це означає, що кіберпроблеми можна швидше виявляти та вирішувати, а відповідальні органи можуть узгодити скоординований підхід. Представники різних органів влади в Cyber-AZ працюють разом у різних постійних або тимчасових робочих групах і підгрупах, щоб оцінити потенціал кіберзагроз, наприклад, для окремих секторів критичної інфраструктури, на тему пов'язаних і міжвідомчих засадах і здійснювати необхідні заходи або їх реалізацію ініціювати органи влади.

Що стосується Національної ради кібербезпеки, то виявлення та усунення структурних причин криз вважається важливим превентивним інструментом кібербезпеки. З цієї причини є потреба у налагодженні та підтримці співпраці в межах федерального уряду, а також між державним і приватним секторами в межах відповідальності Уповноваженого федерального уряду з інформаційних технологій. Національна рада з кібербезпеки призначена для координації превентивних інструментів і міждисциплінарних підходів до кібербезпеки державного та приватного секторів.

Французька агенція безпеки інформаційних систем (ANSSI), створена у 2009 р., є національним органом, який відповідає за кібербезпеку. Виступаючи у французькому кіберпросторі як «рятівник», ANSSI забезпечує запобігання (у тому числі з нормативно-правової точки зору) та реагування на інциденти у

сфері IT, що зачіпають стратегічно важливі установи. Агентство також забезпечує відпрацювання управління у кризових ситуаціях на національному рівні. Міністерство збройних сил Франції виконує подвійну місію із захисту мереж, що забезпечують його діяльність, та з інтеграції цифрової протидії у військові операції. З метою підтримки діяльності міністерства у цій сфері на початку 2017 року було створено штаб кіберзахисту (COMCYBER), переданий під командування начальника штабу збройних сил.

У сучасних умовах кібербезпека є критичним компонентом національної безпеки, оскільки кібератаки можуть мати серйозні наслідки для державних інституцій, економічних систем, критичної інфраструктури та безпеки громадян. З огляду на зростаючу складність та масштабність кіберзагроз, ефективна кібербезпека потребує впровадження передових технологій для виявлення, запобігання та нейтралізації атак. Для цього необхідно не лише використовувати сучасне програмне забезпечення та апаратні засоби, а й забезпечити високий рівень кваліфікації персоналу, що працює в цій сфері. Висококваліфіковані фахівці з кібербезпеки здатні розробляти і впроваджувати комплексні стратегії захисту, аналізувати загрози в режимі реального часу та оперативно реагувати на інциденти. Однак підготовка таких спеціалістів потребує значних інвестицій у навчання та професійний розвиток. Крім того, ефективна кібербезпека вимагає постійного оновлення технологій та методів захисту, оскільки кіберзагрози швидко еволюціонують. Це потребує значних фінансових ресурсів, які не завжди доступні у необхідних обсягах. Відсутність належного фінансування може призвести до використання застарілих технологій, які не здатні забезпечити адекватний рівень захисту. У свою чергу, використання застарілих систем і технологій може знижувати здатність держави ефективно реагувати на сучасні загрози. Застарілі

технології, які були розроблені в минулі десятиліття, не можуть повною мірою забезпечити необхідний рівень безпеки та оперативності у сучасних умовах.

Виклики громадській безпеці та громадському порядку залишаться навіть в післявоєнний період, в тому числі ті, що стосуються цивільного захисту, особливої уваги буде потребувати розмінування територій та небезпека пов'язана з цим фактором, безпеки масових заходів та дорожнього руху, як а також організована економічна злочинність і злочинність, пов'язана з наркотиками, а також торгівля людьми. Через міжнародний характер тероризму та його інтенсивність, Україна теж не вільна від таких загроз. Особливо з боку групи людей, які використовують методи терору як інструмент для досягнення власних політичних, соціальних, економічних чи релігійних цілей.

Поліпшення позицій України на міжнародній арені, проте ще членство в НАТО та ЄС призводять все ж до підвищення інтересу з боку іноземних держав спецслужб нашої країни. Можливе несанкціоноване розголошення або викрадення секретної інформації та інших даних, що охороняються законом, можуть завдати шкоди національній безпеці та інтересам України. Безпечне функціонування інформаційно-комунікаційної системи України є умовою безперебійного функціонування всієї держави. Залишається проблемою забезпечення доступності, цілісності та конфіденційність даних, що обробляються в інформаційно-комунікаційних системах державного управління. Крім того, в державі не розроблені єдині заходи безпеки щодо інформаційного простору та. З точки зору безпеки, недостатній рівень знання щодо загроз у кіберпросторі, а також необхідності вирішення дилеми між особистою свободою та захистом прав індивідів та використанням заходів, спрямованих на підтримку стану безпеки.

Висновки та пропозиції. Формування гібридних військових підрозділів, здатних діяти у кіберпросторі, є необхідним кроком для Збройних Сил України. Це вимагає не лише модернізації військових стратегій, але й створення нових інтелектуальних та технологічних підходів, що враховують реалії сучасної гібридної війни. Адміністративно-правові основи військово-цивільного співробітництва, а також активне залучення приватного сектору, є ключовими елементами у побудові ефективної системи кібербезпеки з метою підвищення ефективності управління військовими операціями.

Стійкість та міцність соціальної системи пропорційна ступеню узгодженості дій органів державного управління та медіа, що забезпечує прямий та зворотний зв'язок між громадянським суспільством і державою. Агресивна інформаційна політика в умовах війни, проведена агресором, націлена на формування переконань про нестабільність та погіршення соціально-економічної обстановки. Вона активізує деструктивні політико-ідеологічні фактори, що становлять загрозу для системи національних цінностей, ідеалів та традицій, руйнуючи структури соціалізації особистості. Це також створює загрозу безпеці життєдіяльності людини, суспільства та держави. Критичні інфраструктури включають електромережі, транспортну мережу та інформаційно-комунікаційні системи. Захист цих інфраструктур є життєво важливим для безпеки держави і добробуту її громадян. Паралельно діджиталізація усіх сфер, роблять критичну інфраструктуру такою сферою, руйнування якої можливо здійснити не лише за рахунок фізичного впливу (як намагалася здійснити росія за рахунок ракетних атак), але й через інтернет-мережу (кіберзахист).

Впровадження заходів кіберзахисту надасть можливість підприємствам, установам та організаціям, що вважаються об'єктами критичної інфраструктури, забезпечити ефективний захист від кібератак, запобігти

порушенню конфіденційності, цілісності та доступності своїх інформаційних ресурсів, а також уникнути порушення стійкості функціонування об'єкта критичної інфраструктури.

В рамках ЄС досліджуване питання вперше було підняте ще у 2004 р. із запуску Європейської програми захисту критичної інфраструктури (EPCIP). Це пакет заходів, спрямованих на покращення захисту критичної інфраструктури в Європі, у всіх державах ЄС і в усіх відповідних секторах економічної діяльності. Ініціатива ЄС щодо захисту критичної інформаційної інфраструктури спрямована на посилення безпеки та стійкості життєво важливих інфраструктур інформаційних та комунікаційних технологій.

література

1. Ващенко К. О. Політологія для вчителя. К. О. Ващенко, В. О. Корнієнко. Київ: Вид. ім. М. П. Драгоманова, 2011. 406 с.

2. Про основні засади забезпечення кібербезпеки України: Закон України. (2017). URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 20.11.2024).

3. Ільяшов О.А. Війни майбутнього як об'єкт наукових досліджень. *Наука і оборона*. 2008. № 2. С. 36–40.

4. Кращі практики управління кібербезпекою. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf (дата звернення: 21.11.2024).

5. Лобода Ю.О. Поняття «гібридна війна (гібридні військові дії)»: походження та складність. *Наука і оборона*. 2020. С. 20–23.

6. Магда Є.М. Гібридна війна: сутність та структура феномену. *Міжнародні відносини: Серія. «Політичні науки».* 2014. URL:

http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/2489/2220 (дата звернення: 21.11.2024

7. Номінатюк О.А., Пономарчук С.А., Кондрашова Т.А., Кондрашов Д.М., Костюченко С.І., Терещук Т.М. Гібридна побудова системи кібербезпеки: адміністративно-правові засади військово-цивільного співробітництва. *Кібербезпека: освіта, наука, техніка.* 2023. № 3 (19). doi: 10.28925/2663-4023.2023.19.109121.

8. Правова система України в умовах воєнного стану : збірник наукових праць. За заг. ред. О. О. Кота, А. Б. Гриняка, Н. В. Міловської, М. М. Хоменка. Одеса : Видавничий дім «Гельветика», 2022. 540 с.

9. Про Стратегію кібербезпеки України : Указ Президента України. 2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 20.11.2024).

10. Україна на 24 місці в рейтингу з кібербезпеки. URL: https://ain.ua/2022/06/16/ukrayina-na-24-misczi-v-rejtyngu-z-kiberbezpeky/ (дата звернення: 20.11.2024).

11. NATO and the European Union work together to tackle growing cyber threats. *North Atlantic Treaty Organization.* 2018. URL: https://www.nato.int/cps/uk/natohq/news_161570.htm?selectedLocale=en (дата звернення: 20.11.2024).

12. Chorna O., Orlova I. S., Shyshliuk V., Pugachov M., Pugachov V. Anti-Crisis regulation of enterprises through digital management. *International Journal of Professional Business Review.* 2023. 8(5). P. 90.

13. Radchenko O., Kovach V., Semenets-Orlova I., Zaporozhets A. (Eds.). National security drivers of Ukraine: information technology, strategic communication, and legitimacy. Springer Nature, 2023.

References

1. Vashchenko, K. O. (2011). Politolohiia dlia vchytelia [Politilogy for teachers]. K. O. Vashchenko, V. O. Korniienko. Kyiv: Vyd. im. M. P. Drahomanova [in Ukrainian].

2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy [On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine]. (2017). URL: https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

3. Iliashov, O.A. (2008). Viiny maibutnoho yak obiekt naukovykh doslidzhen [Wars of the Future as an Object of Scientific Research]. *Nauka i oborona,* 2, 36–40 [in Ukrainian].

4. Krashchi praktyky upravlinnia kiberbezpekoiu [Best Practices in Cybersecurity Management]. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf [in Ukrainian].

5. Loboda, Yu.O. (2020). Poniattia «hibrydna viina (hibrydni viiskovi dii)»: pokhodzhennia ta skladnist [The Concept of "Hybrid War (Hybrid Military Actions)": Origin and Complexity]. *Nauka i oborona,* 20–23 [in Ukrainian].

6. Nominatiuk, O.A., Ponomarchuk, S.A., Kondrashova, T.A., Kondrashov, D.M., Kostiuchenko, S.I., Tereshchuk, T.M. (2023). Hibrydna pobudova systemy kiberbezpeky: administratyvnopravovi zasady viiskovo-tsyvilnoho spivrobitnytstva [Hybrid Construction of the Cybersecurity System: Administrative and Legal Foundations of Civil-Military Cooperation]. *Kiberbezpeka: osvita, nauka,* 3 (19). doi: 10.28925/2663-4023.2023.19.109121 [in Ukrainian].

7. Mahda, Ye.M. (2014). Hibrydna viina: sutnist ta struktura fenomenu [Hybrid War: The Essence and Structure of the Phenomenon]. *Mizhnarodni vidnosyny: Seriia. «Politychni nauky».* URL:

http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/2489/2220 [in Ukrainian].

8. Pravova systema Ukrainy v umovakh voiennoho stanu: zbirnyk naukovykh prats [The Legal System of Ukraine in the Conditions of Martial Law: A Collection of Scientific Papers]. Za zah. red. O. O. Kota, A. B. Hryniaka, N. V. Milovskoi, M. M. Khomenka. Odesa: Vydavnychyi dim «Helvetyka», 2022. 540 s. [in Ukrainian].

9. Pro Stratehiiu kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy [On the Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine]. (2016). URL: https://zakon5.rada.gov.ua/laws/show/96/2016 [in Ukrainian].

10. Ukraina na 24 mistsi v reitynhu z kiberbezpeky [Ukraine Ranked 24th in Cybersecurity]. URL: https://ain.ua/2022/06/16/ukrayina-na-24-misczi-v-rejtyngu-z-kiberbezpeky/ [in Ukrainian].

11. NATO and the European Union work together to tackle growing cyber threats (2018). *North Atlantic Treaty Organization.* URL: https://www.nato.int/cps/uk/natohq/news_161570.htm?selectedLocale=en.

12. Chorna, O., Orlova, I. S., Shyshliuk, V., Pugachov, M., & Pugachov, V. (2023). Anti-Crisis regulation of enterprises through digital management. *International Journal of Professional Business Review,* 8(5), 90.

13. Radchenko, O., Kovach, V., Semenets-Orlova, I., & Zaporozhets, A. (Eds.). (2023). National security drivers of Ukraine: information technology, strategic communication, and legitimacy. Springer Nature.