УДК 355.45+ 004.056.5
DOI https://doi.org/10.32782/app.v75.2025.25

В. В. Сироватко
orcid.org/0009-0008-1645-6877
аспірант кафедри політології і міжнародних відносин
Луганського національного університету імені Тараса Шевченка

КІБЕРКОМПОНЕНТ У СТРУКТУРІ НАЦІОНАЛЬНОГО ОБОРОННОГО ПОТЕНЦІАЛУ: ВИКЛИКИ ДЛЯ ДЕРЖАВНОЇ ПОЛІТИКИ

У XXI столітті глобальний безпековий простір зазнає докорінних змін, пов'язаних із переходом до інформаційно-комунікаційної епохи. У цьому контексті кіберпростір став не лише ареною міждержавної конкуренції, але й повноцінним театром воєнних дій. Відтак, сучасне трактування оборонного потенціалу держави неможливе без урахування кіберкомпоненту – складової, що охоплює як захист інформаційної інфраструктури, так і спроможність здійснювати активні дії у цифровому середовищі.

Оборонний потенціал держави є багатокомпонентним, інтегрованим явищем, що охоплює всі ключові ресурси країни – від людських і матеріальних до політичних і духовних. Під оборонним потенціалом розуміється як сукупність об'єктивно існуючих можливостей держави, так і здатність ефективно мобілізувати ці ресурси для забезпечення обороноздатності та досягнення стратегічних цілей у воєнний і мирний час.

Вітчизняні дослідники пропонують розуміти оборонний потенціал держави, як сукупність потенціалів, розділених на групи за кількома самостійними основами, а саме: за філософсько-соціологічною основою – потенційна сукупна могутність країни і воєнна могутність держави розподіляється на матеріальний (військово-матеріальний) потенціал і духовний (військово-духовний) потенціал; за загально-соціологічною основою – географічний (військово-географічний) і демографічний (військово-демографічний) потенціал; за частково-соціологічною основою (сфера суспільного життя – економічний (військово-економічний), соціальний (військово-соціальний), політичний (військово-політичний) і моральний (військово-моральний) потенціал; на основі системного, універсального функціонування – організаційний (військово-організаційний), управлінський (військово-управлінський), науковий (військово-науковий) потенціал (Пасічко, 2008).

О. Семененко, С. Салкуцан, О. Романченко, Є. Марко, А. Ремез та Л. Добровольська визначають основні структурні складові оборонного потенціалу, їх елементи та фактори впливу на оборонний потенціал, серед яких: *військові ресурси*: особовий склад; техніка та озброєння; мобілізаційні можливості; *економічна складова*: виробничі потужності, бюджетування, сільське господарство трудові мобілізаційні ресурси; *інформаційна безпека*: захист даних, контроль над інформаційними потоками; *науково-технічний потенціал:* система науково-дослідних, конструкторських та проектно-технологічних організацій; *стан розвитку військової науки:* підготовка резервного особового складу, розробка нових проектно-технічних проєктів; *соціально-моральна складова:* національні відносини, національна ідея; імідж країни (Семененко, Салкуцан, Романченко, Марко, Ремез, Добровольська, 2020).

Оборонний потенціал держави є однією з ключових складових національної безпеки. Відповідно до ст. 1 п. 9 Закону України «Про Національну безпеку України», *національна безпека* – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз»(Про національну безпеку, 2018). Як ми вже зазначали, «національна безпека» характеризує ступінь захищеності життєво важливих інтересів, прав і свобод особи, суспільства та держави від зовнішніх і внутрішніх загроз або ступінь відсутності загроз правам і свободам людини, базовим інтересам і цінностям суспільства та держави; це здатність нації задовольняти потреби, необхідні для її самозбереження, самовідтворення й самовдосконалення з мінімальним ризиком збитку для базових цінностей її нинішнього стану (Сироватко, 2024, с. 184).

Тобто, оборонний потенціал забезпечує здатність держави протидіяти зовнішнім загрозам, зберігати суверенітет, територіальну цілісність та політичну незалежність.

У системі національної безпеки оборонний потенціал виконує стратегічну функцію стримування агресора та гарантує стабільність державного розвитку в умовах зростаючої нестабільності у світі. Оборонний потенціал в системі національної безпеки можна розглядати як: силову опору безпеки, що забезпечує спроможність держави до збройного захисту, платформу для міжнародної співпраці, адже сильний оборонний потенціал дозволяє державі бути надійним партнером у міжнародних безпекових союзах; фактор стримування агресії; компонент у структурі комплексної безпеки (через взаємодію з іншими сферами безпеки (економічною, кібернетичною, інформаційною, екологічною, тощо).

Цифровізація всіх сфер суспільного життя, включно з військовою, обумовила формування нового виміру національної безпеки – кіберпростору.

Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 N 2163-VIII *кіберпростір* визначається, як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних (Про основні засади забезпечення кібербезпеки України, 2017). Унікальність кіберпростору полягає у відсутності географічних меж, асиметричності загроз і можливості дистанційного впливу на критичні об'єкти державної інфраструктури.

В умовах сучасних війн та терористичних атак, країни-учасники стають мішенню численних кібератак на їхній кіберпростір. Найчастіше під ураження потрапляють оборонний сектор (діяльність урядових установ, збройних сил, правоохоронних органів та засобів масової інформації (комунікаційні системи державної, комунальної та інших форм власності, які забезпечують обробку інформаційних ресурсів і використовуються в інтересах органів державної влади, правоохоронних структур та військових формувань); ядерна та хімічна промисловість (комунікаційні та технологічні системи критично важливих інфраструктурних об'єктів держави, до яких відносяться українські АЕС, а також низка національних хімічних підприємств);транспортні та комунікаційні мережі (системи комунікації, які використовуються для задоволення суспільних потреб, а також у процесах електронних державних послуг, електронного документообігу, електронної комерції та електронного урядування); національна та фінансова системи (комунікаційні системи фінансових установ країни, зокрема банківські мережі, які мають стратегічне значення для економічної стабільності держави) сектори виробництва, науково-технічних розробок, фінансів, охорони здоров'я та цифрових послуг та інші (Сироватко, 2025, с. 181–187).

Так, наприкінці 2017 року відбулася масштабна кібератака з використанням вірусу, який спочатку був названий Petya (пізніше – NotPetya). Тоді під атаку потрапили третина банківських установ, компанія «Нова пошта», а також уряд, низка енергетичних компаній – у тому числі регіональних, редакції великих медіахолдингів тощо. Зараження комп'ютерних систем відбувалося в напередодні Дня Конституції України. За оцінкою фахівців із кібербезпеки ні державні органи, ні бізнес не були готові до подібних атак. Зазвичай кібератаки на бізнес чи державні органи можуть мати одну із трьох цілей: вимагання грошей та шантаж; популяризація шахрая, який здійснює напад, і остання – *дестабілізація ситуації в державі* (Патрікєєва, 2018).

Стан захищеності кіберпростору держави та окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, при якому порушується їхня стабільність чи сталий розвиток, своєчасне виявлення, запобігання та відповідна нейтралізація реальних і потенційних викликів (кібервтручань, кіберзагроз, кіберзлочинів) реальним особистим, корпоративним, інституціальним і/або національним інтересам визначається як кібербезпека (Ткаченко О, Ткаченко К, 2018).

Відповідно до положень ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», під терміном «*кібербезпека*» слід розуміти захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікатив-

ного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (Про основні засади забезпечення кібербезпеки України, 2022). Тобто, кібербезпека – це сукупність організаційних, правових, технічних та інших заходів, спрямованих на захист та забезпечення конфіденційності, цілісності та доступності інформаційних систем, мереж, програм і даних. На думку Є. Колосовського та Е. Круця кібербезпека характеризується як: система спеціальних суб'єктів, які забезпечують комп'ютерну безпеку, разом із методами та засобами, які вони використовують, а також як система взаємопов'язаних організаційних, технічних та правових заходів, що впроваджуються цими суб'єктами; рівень захищеності електронних інформаційних ресурсів держави у кіберпросторі від ризиків зовнішнього впливу, а також як система виявлення та протистояння різним формам зовнішнього втручання через інформаційні системи; система елементів комп'ютерної безпеки, які взаємодіють між собою, комплектуються та розгортаються відповідно до єдиного плану з метою забезпечення безпеки інформаційно-телекомунікаційних систем; рівень захищеності важливих і життєвих інтересів людини, громадянина, а також суспільства та держави загалом, за якого можливе безперешкодне збирання, використання та зберігання інформації; здатність держави запобігати та уникати спрямованого негативного впливу (Колосовський, Круць, 2023).

До ключових викликів, що постають у цифровому середовищі обороного потенціалу можна віднести:

– *Кібершпигунство*: злочинна діяльність, яка здійснюється шляхом таємного вистежування, розшуку, збирання, викрадення та передачі інформації, що становить державну таємницю, іноземній державі, іноземній організації або їхнім представникам, якщо ці дії вчинені іноземцем або особою без громадянства із використанням кіберпростору. Об'єктом кібершпигунства є зовнішня безпека України, її суверенітет, територіальна цілісність, недоторканність, обороноздатність, державна, економічна та інформаційна безпека (Діордиця, 2020, с. 51).

– *Кібертероризм*: цифровий тероризм, відноситься до виникнення атак або загрози атак у межах стратегії тероризму в кіберпросторі з метою дестабілізації. Тобто, тероризм, який здійснюють терористичні групи, відображається просторово у віртуальному вимірі, відбуваються атаки на програмне забезпечення, апаратне забезпечення, мережі та користувачів, які є цінностями, які необхідно захищати в рамках кібербезпеки (Дінжос, Замула, 2024).

– *Кібервійна*: використання Інтернету та пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеці та суверенітету іншої держави» (Дикий, 2022), це організовані атаки на інформаційні системи з метою досягнення військово-політичних цілей.

– *Інформаційно-психологічні операції*: маніпулювання суспільною думкою, поширення дезінформації; комплекс заходів з поширення спеціально підготовленої інформації задля впливу на емоції, почуття, поведінку людей, сформувавши таким чином громадську думки у потрібному руслі. До елементів ІПсО відносяться дезінформація, пропаганда, кібератаки, перебільшення певної інформації або применшення іншої (Яка мета головних кремлівських ІПсО у війні проти України, 2023)

Кібербезпека є фундаментом національної безпеки України і складовою її оборонного потенціалу. Кібербезпека як новий вимір оборонного потенціалу держави полягає у: зміні традиційних уявлень про оборону. Якщо раніше безпека держави асоціювалася переважно з фізичними кордонами та військовими ресурсами, то нині на перший план виходить кіберпростір, який не має географічних меж; здатності держави ефективно протидіяти кібератакам, захищати інформаційні ресурси, а також вести інформаційно-психологічні операції є визначальним чинником її оборонного потенціалу у XXI столітті; розвитку національної кібербезпеки, створенні відповідних інституцій, підготовці фахівців та міжнародній співпраці у цій сфері стають невід'ємними елементами стратегії безпеки України. Державна політика України у сфері кібербезпеки формується на міжнародній нормативній базі ратифікованій Україною та внутрішніми правовими документами.

Нормативно-правова база України у сфері кібербезпеки формувалася ще до початку повномасштабної агресії Росії й нині потребує оновлення з урахуванням нових викликів. Основу

міжнародно-правового співробітництва становлять Будапештська конвенція (ратифікована Україною у 2005 році) та Директива ЄС про мережеву та інформаційну безпеку (NIS), яка, попри необов'язковість для України, виступає орієнтиром для впровадження належних практик. Національне законодавство базується на Законі України «Про основні засади забезпечення кібербезпеки України» (2017) та Національній стратегії кібербезпеки (2021), яка стала логічним продовженням стратегії 2016 року. Незважаючи на вжиті заходи, значна частина положень Будапештської конвенції досі не інтегрована у кримінальне законодавство України, що знижує ефективність протидії кіберзлочинності. У контексті євроінтеграції та сучасної безпекової ситуації актуалізується необхідність адаптації українського законодавства до стандартів ЄС, з урахуванням нових форм загроз у кіберпросторі.

Повномасштабна війна прискорила ряд політичних рішень. Так, Кабінет Міністрів України з 2023 року ухвалює низку підзаконних нормативно-правових актів, спрямованих на імплементацію положень Закону України «Про основні засади забезпечення кібербезпеки України» (2017). Значну увагу приділено вдосконаленню координації з міжнародними партнерами та підвищенню стійкості критичної інфраструктури, зокрема: Постанова КМУ № 142 (17.02.2023) передбачає представництво України в Об'єднаному центрі передових технологій з кібероборони НАТО, що посилює міжнародну взаємодію у сфері кіберзахисту; Постанова № 257 (24.03.2023) затверджує механізм незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; Постанова № 299 (04.04.2023) встановлює порядок реагування на кіберінциденти відповідно до Стратегії кібербезпеки України; Постанова № 1163-р (19.12.2023) ухвалює план заходів на 2023–2024 роки з реалізації Стратегії; Постанова № 276 (08.03.2024) передбачає створення міжвідомчої робочої групи з питань залучення міжнародної допомоги, що покликана зміцнити кіберстійкість держави шляхом координації з іноземними урядами та організаціями та інші.

Інкорпорація кіберкомпоненту в структуру національного оборонного потенціалу є не лише вимогою часу, але й ключовим чинником забезпечення суверенітету, стійкості та політичної стабільності держави в умовах гібридних загроз і масштабного цифрового протистояння та вимагає переосмислення державної політики у сфері безпеки. Кібербезпека переходить із допоміжного у стратегічний вимір національної безпеки, що потребує системного оновлення. Насамперед це стосується наступних питань: *нормативно-правового забезпечення*, яке має бути адаптованим до нових типів загроз з урахуванням досвіду війни та міжнародних стандартів; *інституційного оформлення* – створенням спеціалізованих кіберпідрозділів у силових структурах та Збройних Силах, органів координації та стратегічного планування, розширення повноважень профільних державних органів та забезпечення їх координації; *формування кадрового потенціалу*, інвестування в підготовку фахівців із кібербезпеки, розвиток профільної освіти та системи професійної перепідготовки; *фінансового та технологічного забезпечення*, що передбачає підтримку наукових розробок, інновацій та кібертехнологій в тому числі в оборонному секторі; *підвищення кіберстійкості критичної інфраструктури* – забезпечення сталості функціонування комунікаційних, енергетичних, транспортних та фінансових систем, координації між силовими структурами та впровадження інноваційних технологій захисту; *міжнародної взаємодії* через розширення участі України в міжнародних кіберкоаліціях і проєктах технічної допомоги, поглиблення обміну досвідом із союзниками. Комплексне впровадження зазначених заходів дозволить ефективно інтегрувати кіберкомпонент у систему національного оборонного потенціалу та адаптувати державну безпекову політику до викликів XXI століття.

Література

Дикий, О. В. (2024). Кібервійна в Україні. У *VII Всеукраїнській науково-практичній конференції «Інформаційне суспільство: проблеми та перспективи»* (с. 102–103).

Діжнос, І. В., & Замула, А. Ю. (2024). Кібертероризм як потенційно реалістична загроза. *UNIVERSUM*, (15), 90–103. https://archive.liga.science/index.php/universum/article/download/1517/1536/1552

Діордиця, І. В. (2020). Поняття та зміст кібершпигунства. *Наукові праці НУ «ОЮА»*, 49–55.

Закон України «Про основні засади забезпечення кібербезпеки України» від 17.08.2022 № 2163-VIII. *Відомості Верховної Ради України*. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Закон України «Про національну безпеку України» (Відомості Верховної Ради, 2018, № 31, ст. 241 зі змінами № 2952-IX від 24.02.2023). https://zakon.rada.gov.ua/laws/show/2469-19#Text

Колосовський, Є., & Круць, Е. (2023). Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*, (12), 403–405.

Пасічко, В. (2008). Обороноздатність держави: теоретичні основи системного дослідження. *Політичний менеджмент. Воєнна безпека*, (2), 135–143. https://ipiend.gov.ua/wp-content/uploads/2018/07/pasichko_oboronozdatnist.pdf

Патрікєєва, Н. (2018, 3 липня). Рік після атаки вірусу Petya: що змінилося в кібербезпеці України. *Радіо Свобода*. https://www.radiosvoboda.org/a/29336511.html

Семененко, О., Салкуцан, В., Романченко, О., Марко, Є., Добровольська, Л., & Ремез, А. (2020). Основні методологічні аспекти оцінювання взаємозв'язку оборонного та економічного потенціалу держави. *Social Development and Security, 10*(6), 161–177.

Сироватко, В. (2024). Оборонний потенціал & національна безпека. У *Національна безпека: загрози та виклики: матеріали підвищення кваліфікації* (с. 184–187). Львів – Торунь: Liha-Pres.

Сироватко, В. (2025). Кібербезпека як новий вимір оборонного потенціалу держав. У *Сучасні суспільні комунікації: міжнародний досвід та українські реалії* (с. 181–187). Лубни: Вид-во ДЗ «ЛНУ імені Тараса Шевченка».

Такаченко, О., & Ткаченко, К. (2018). Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері, 1*, 75–86. https://doi.org/10.31866/2617-796x.1.2018.147257

Яка мета головних кремлівських ІПсО у війні проти України. (2023, 25 лютого). *Центр протидії дезінформації при РНБО*. https://cpd.gov.ua/main/yaka-meta-golovnyh-kremlivskyh-ipso-u-vijni-proty-ukrayiny/

References

Dykyi, O. V. (2024). Kiberviina v Ukraini [Cyberwarfare in Ukraine]. In *VII Vseukrainska naukovo-praktychna konferentsiia "Informatsiine suspilstvo: problemy ta perspektyvy"* (pp. 102–103).

Dinzhos, I. V., & Zamula, A. Yu. (2024). Kiberteroryzm yak potentsiino realistychna zahroza [Cyberterrorism as a Potentially Realistic Threat]. *UNIVERSUM*, (15), 90–103. https://archive.liga.science/index.php/universum/article/download/1517/1536/1552

Diordytsia, I. V. (2020). Poniattia ta zmist kibershpyhunstva [The Concept and Content of Cyber Espionage]. *Naukovi pratsi NU "OYuA"*, 49–55.

Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy»[On the Basic Principles of Ensuring Cybersecurity of Ukraine] vid 17.08.2022 № 2163-VIII. *Vidomosti Verkhovnoi Rady Ukrainy*. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Zakon Ukrainy «Pro natsionalnu bezpeku Ukrainy»[On National Security of Ukraine] (Vidomosti Verkhovnoi Rady, 2018, № 31, st. 241 zi zminamy № 2952-IX vid 24.02.2023). https://zakon.rada.gov.ua/laws/show/2469-19#Text

Kolosovskyi, Ye., & Kruts, E. (2023). Suchasnyi stan kiberbezpeky Ukrainy v umovakh voiennoho periodu The Current State of Ukraine's Cybersecurity in Wartime Conditions]. *Yurydychnyi naukovyi elektronnyi zhurnal*, (12), 403–405.

Pasichko, V. (2008). Oboronozdatnist derzhavy: teoretychni osnovy systemnoho doslidzhennia [State Defense Capability: Theoretical Foundations of System Research] *Politychnyi menedzhment. Voienna bezpeka*, (2), 135–143. https://ipiend.gov.ua/wp-content/uploads/2018/07/pasichko_oboronozdatnist.pdf

Patrikieieva, N. (2018, 3 lypnia). Rik pislia ataky virusu Petya: shcho zminylosia v kiberbezpetsi Ukrainy[One Year After the Petya Virus Attack: What Has Changed in Ukraine's Cybersecurity] *Radio Svoboda*. https://www.radiosvoboda.org/a/29336511.html

Semenenko, O., Salkutsan, V., Romanchenko, O., Marko, Ye., Dobrovolska, L., & Remez, A. (2020). Osnovni metodolohichni aspekty otsiniuvannia vzaiemozviazku oboronnogo ta ekonomichnoho potentsialu derzhavy[Methodological Aspects of Assessing the Relationship Between Defense and Economic Potential] *Social Development and Security, 10*(6), 161–177.

Syrovatko, V. (2024). Oboronnyi potentsial & natsionalna bezpeka[Defense Potential & National Security] In *Natsionalna bezpeka: zahrozy ta vyklyky: materialy pidvyshchennia kvalifikatsii* (pp. 184–187). Lviv – Torun: Liha-Pres.

Syrovatko, V. (2025). Kiberbezpeka yak novyi vymir oboronnogo potentsialu derzhavy.[Cybersecurity as a New Dimension of the State's Defense Potential] In *Suchasni suspilni komunikatsii: mizhnarodnyi dosvid ta ukrainski realii* (pp. 181–187). Lubny: Vyd-vo DZ "LNU imeni Tarasa Shevchenka".

Takachenko, O., & Tkachenko, K. (2018). Kiberprostir i kiberbezpeka: problemy, perspektyvy, tekhnolohii [Cyberspace and Cybersecurity: Problems, Prospects, Technologies]. *Tsyfrova platforma: informatsiini tekhnolohii v sotsiokulturnii sferi, 1*, 75–86. https://doi.org/10.31866/2617-796x.1.2018.147257

Yaka meta holovnykh kremlivskykh IPsO u viini proty Ukrainy[What Are the Kremlin's Main Info-Psychological Ops Aimed at Ukraine?] (2023, 25 liutoho). *Tsentr protydii dezinformatsii pry RNBO*. https://cpd.gov.ua/main/yaka-meta-golovnyh-kremlivskyh-ipso-u-vijni-proty-ukrayiny/

Анотація

Сироватко В. В. **Кіберкомпонент у структурі національного оборонного потенціалу: виклики для державної політики.** – Стаття.

У статті досліджено роль кіберкомпоненту як невід'ємного елементу оборонного потенціалу держави в умовах трансформації безпекового середовища XXI століття.

Наголошено, що сучасний етап глобальної цифровізації та зростання гібридних загроз вимагає переосмислення підходів до забезпечення національної безпеки, в центрі яких опиняється кіберпростір як новий театр бойових дій.

Кіберпростір розглядається як штучне, технічно створене середовище, що об'єднує інформаційні, комунікаційні та обчислювальні мережі, в межах яких можливе здійснення стратегічних впливів без фізичного вторгнення. Його унікальність полягає у відсутності чітких географічних кордонів, асиметричному характері загроз та високій швидкості поширення шкідливого впливу.

Розглянуто структуру національного оборонного потенціалу з урахуванням класичних (військових, економічних, політичних, соціальних) і новітніх (інформаційно-комунікаційних, цифрових) складових. Показано, що кібербезпека є не лише частиною оборонного сектору, а й стратегічною категорією, що охоплює широкий спектр державних функцій: від захисту критичної інфраструктури до протидії інформаційно-психологічним впливам. Зосереджено увагу на огляді чинного законодавства України у сфері кібербезпеки, зокрема Закону України «Про основні засади забезпечення кібербезпеки України» та підзаконних актів, ухвалених після початку повномасштабної агресії.

Визначено основні типи кіберзагроз – кібершпигунство, кібертероризм, кібервійну та інформаційно-психологічні операції, що дестабілізують державу й вимагають оперативного, науково обґрунтованого реагування. Обґрунтовано необхідність інтеграції кіберкомпоненту в систему стратегічного планування оборонної політики.

Розкрито завдання держави щодо посилення інституційної спроможності, розвитку спеціалізованої освіти, наукових досліджень, міжнародної координації та формування кіберстійкої критичної інфраструктури. Автор підкреслює, що лише за умови системного підходу можлива ефективна протидія цифровим загрозам, що ставить кібербезпеку в центр сучасної парадигми національної безпеки.

Ключові слова: кібербезпека, кіберкомпонент, оборонний потенціал, національна безпека, кіберпростір, державна політика, кібероборона.

Summary

Syrovatko V. V. **Cyber component in the structure of national defense potential: challenges for public policy.** – Article.

The article explores the role of the cyber component as an integral element of the national defense potential in the context of the evolving security environment of the 21st century. It is emphasized that the current stage of global digitalization and the intensification of hybrid threats necessitate a fundamental reconsideration of approaches to national security, with cyberspace emerging as a new theatre of warfare.

Cyberspace is interpreted as an artificial, technologically constructed environment that integrates information, communication, and computational networks, within which strategic influence can be exerted without physical intrusion. Its uniqueness lies in the absence of clear geographical boundaries, the asymmetric nature of threats, and the high speed of impact dissemination.

The structure of national defense potential is analyzed with regard to both traditional (military, economic, political, social) and modern (informational, digital, cyber) components. It is demonstrated that cybersecurity is not only a functional aspect of the defense sector but also a strategic category that encompasses a broad spectrum of state functions, from the protection of critical infrastructure to countering information and psychological influence.

Particular attention is paid to the analysis of Ukraine's legal framework on cybersecurity, including the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity» and related secondary legislation adopted in response to full-scale military aggression. The article identifies key types of cyber threats–cyber espionage, cyberterrorism, cyber warfare, and information-psychological operations–which destabilize the state and demand swift, evidence-based responses.

The necessity of integrating the cyber component into the system of strategic defense planning is substantiated. The state's tasks are outlined in terms of strengthening institutional capacity, developing specialized education, fostering scientific research, promoting international coordination, and building cyber-resilient critical infrastructure. The author argues that only through a systemic and coordinated approach can effective responses to digital threats be ensured, placing cybersecurity at the core of the modern national security paradigm.

Key words: cybersecurity, cyber component, defense potential, national security, cyberspace, public policy, cyber defense.