DOI 10.52363/2414-5866-2025-1-31
УДК 316.334.3 ; 316.334.4

Неводчікова І.М., *аспірант, НУЦЗУ, м. Черкаси,*
ORCID: 0009-0008-5998-8822,
Помаза-Пономаренко А.Л., *д.держ.упр., с.д., НУЦЗУ, м. Черкаси,*
ORCID: 0000-0001-5666-9350

Nevodchikova I., *postgraduate student of National University of Civil Defence of Ukraine, Cherkasy,*
Pomaza-Ponomarenko A., *Doctor bin Public Administration, Senior Researcher, Head of the research laboratory for studying management problems in the sphere of civil protection of National University of Civil Defence of Ukraine, Cherkasy*

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ПУБЛІЧНОГО УПРАВЛІННЯ СЕКТОРОМ БЕЗПЕКИ Й ОБОРОНИ УКРАЇНИ В УМОВАХ РОЗВИТКУ КРИЗОВИХ СИТУАЦІЙ

FEATURES OF THE FUNCTIONING OF PUBLIC MANAGEMENT IN THE SECURITY AND DEFENSE SECTOR OF UKRAINE IN THE CONDITIONS OF DEVELOPMENT OF CRISIS SITUATIONS

Досліджено сутність і форми публічно-приватного партнерства. Його охарактеризовано як сучасний державноуправлінський інструмент, покликаний забезпечити належне функціонування сфер суспільної життєдіяльності. Оцінено стан і проаналізовано проблеми реалізації проєктів публічно-приватного партнерства в Україні, на теренах якої впроваджується низка реформ. Серед них реформі децентралізації влади віднесено особливу роль, адже нею передбачено зменшення ресурсного навантаження на державні органи й активізацію приватних і самоврядних інституцій для підвищення рівня функціонування сфер суспільної життєдіяльності. Виявлено перспективи розвитку чинної правової бази у сфері регулювання публічно-приватного партнерства в Україні, а також систематизовано сценарії розвитку публічно-приватного партнерства.

Ключові слова*: публічне управління, система публічного управління, національна безпека, сектор безпеки й оборони, кризові ситуації.*

The essence and forms of public-private partnership are studied. It is characterized as a modern state management tool designed to ensure the proper functioning of the spheres of public life. The state is assessed and the problems of implementing pub-

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)
Creative Commons Attribution 4.0 International (CC BY 4.0)

lic-private partnership projects in Ukraine, in which a number of reforms are being implemented, are analyzed. Among them, the reform of decentralization of power is given a special role, since it provides for a reduction in the resource burden on state bodies and the activation of private and self-government institutions to increase the level of functioning of the spheres of public life. Prospects for the development of the current legal framework in the field of regulating public-private partnership in Ukraine are identified, and scenarios for the development of public-private partnership are also systematized.

Key words: *public administration, public administration system, public policy, public-private partnership, forms of public-private partnership, projects, decentralization reform, concession, leasing.*

Постановка актуальності. Проблема обґрунтування та прийняття дієвих управлінських рішень у структурах державної влади набуває особливої ваги в умовах сучасних викликів, що постають перед Україною, зокрема задля забезпечення її суверенітету, територіальної цілісності та безпеки. Саме тому наявність технологічно-інституційного середовища, яке сприяє якісному аналізу інформації та оперативному ухваленню ефективних рішень, є критично важливою як для керівників центральних органів влади, так і для місцевих адміністрацій, особливо у кризових ситуаціях. В Україні наразі триває процес створення потужної інтегрованої мережі ситуаційних центрів (далі – СЦ), де Міністерство оборони України (далі – МОУ) є однією із ключових ланок. У цьому контексті планується формування таких центрів на єдиній цифровій платформі, здатній функціонувати в режимі реального часу, у тому числі передбачено розгортання резервних СЦ та мобільних центрів управління. На практиці введені в експлуатацію ситуаційні центри використовують спеціалізоване програмне забезпечення для інформаційно-аналітичної підтримки, моніторингу, прогнозування, прийняття рішень, аудиту та забезпечення безпеки.

Усі ці процеси повинні реалізуватися в межах об'єднаного цифрового середовища, захищеного від кіберзагроз і несанкціонованих втручань. Необхідність створення чіткої організаційної структури в складі СЦ Міністерства оборони України стає одним із головних завдань у цьому напрямку. Основна функція зазначеної структури полягає в оперативному реагуванні на кіберзагрози й забезпеченні стабільної технічної підтримки програмно-апаратного комплексу платформи. Отже, комплексна організація цих завдань потребує подальших наукових досліджень і координації зусиль для ефективної реалізації поставлених стратегічних цілей.

Аналіз останніх досліджень і публікацій. Процес формування механізмів прийняття управлінських рішень, у т. ч. в умовах криз у державному управлінні, досліджували В. Бакуменко, А. Васильєв, Ю. Гладун, О. Карпенко, О. Ляшевська, Н. Подвірна, О. Труш та ін.

Безпекова проблематика стала предметом ґрунтовного наукового дослідження вчених С. Бєлая, О. Бондаренка, І. Волкова, В. Горбуліна, Ю. Древаля, С. Домбровської, Є. Живіло, О. Кравчука, С. Крука, О. Крюкова, Н. Нижник, В. Новікова, В. Олуйка, О. Пархоменко-Куцевіл, С. Пороки, Г. Ситника, В. Скуратівського, В. Степанова, О. Суходолі, В. Торічного, Т. Ярового та ін. [4; 5; 7].

Наукові роботи вищевказаних авторів становлять важливу теоретико-методологічну базу для осмислення й аналізу механізмів держави у сфері гарантування безпеки крізь призму розвитку кризових ситуацій, а також для подальшого обґрунтування шляхів удосконалення даних механізмів.

Постановка завдання. Мета статті полягає у визначенні особливостей функціонування публічного управління сектором безпеки й оборони України в умовах розвитку кризових ситуацій.

Виклад основного матеріалу дослідження. Досвід світових країн демонструє, що застосування систем центрів управління в кризових ситуаціях стрімко набуває масштабного поширення [4; 7]. Одним з ключових факторів, які визначають ефективність роботи таких центрів, є рівень інформаційного забезпечення. У контексті динамічних процесів прийняття державно управлінських рішень та реагування на кризові події всередині мережі державних СЦ, включаючи головний СЦ, з'являється гостра необхідність у задіянні всіх доступних інформаційних ресурсів країни.

Як відомо, у межах Міністерства оборони України та Збройних сил України нараховується приблизно 20 інформаційно-аналітичних систем, які перебувають у використанні на системній основі або проходять тестову експлуатацію. Ця кількість має постійну тенденцію до зростання. Беручи до уваги первинні наукові джерела, аналітичні матеріали й прогнози, можна з упевненістю стверджувати, що державні інформаційні ресурси постійно стикаються із реальними та потенційними загрозами в кіберпросторі. У зв'язку із цим забезпечення стабільної та безперебійної роботи інформаційно-аналітичних систем СЦ Міністерства оборони України набуває критичного значення.

У цьому контексті можна визначити, що особливу увагу слід приділяти перевірці таких систем на вразливість, адаптації їх конфігурації відповідно до змінних умов, моніторингу ефективності відповідно до встановлених регламентів. Паралельно фахівці ІТ-підрозділів єдиної мережі СЦ України активно шукають рішення для впровадження системного підходу до використання хмарних технологій. Це включає організацію доступу до розподілених інформаційних ресурсів, створення уніфікованого програмного забезпечення для оптимізації формування та супроводу динамічних реєстрів електронних ресурсів у національному сегменті кіберпростору [4; 7].

У сучасних складних умовах воєнно-політичного протистояння, коли Україна захищає свою територіальну цілісність і суверенітет, постала необхідність подальшого вдосконалення системи організації ситуаційних центрів як ефективного інструменту стратегічної комунікації. У цьому процесі враховується досвід передових держав світу. Сучасний світ вимагає динамічного реагування на виклики, які пов'язані з підвищенням ролі інформації та знань у суспільному житті, зростанням рівня інформатизації, стрімким розвитком інформаційних технологій та глобального інформаційного простору. Це створює нові виклики для управлінців, які все частіше стикаються з дефіцитом часу для прийняття рішень [5].

Усі ці фактори є підґрунтям для реформування різних сфер суспільного життя, зокрема системи державного (публічного) управління. Перебуваючи у жорстких воєнно-політичних реаліях, МО України спрямовує зусилля на перетворення Збройних Сил України (далі – ЗСУ) та інших елементів сектору безпеки й оборони, щоб забезпечити їхню готовність адекватно діяти за умов криз. У рамках цього процесу у 2021 році, згідно з Директивою Головнокомандувача ЗСУ, було створено Ситуаційний центр ЗСУ. Його структура адаптується відповідно до завдань чи загроз, а система ситуаційного управління є гнучкою й розробляється за кількома варіантами.

МО України також активізувало створення та забезпечення функціонування ситуаційних центрів у власній системі. Ця ініціатива узгоджена з рішенням Ради національної безпеки й оборони України від червня 2021 року щодо модернізації мережі ситуаційних центрів і цифрової трансформації сфери національної безпеки та оборони. Рішення схвалене Указом Президента України та іншими нормативними актами. На основі цих документів у грудні 2021 року було створено робочу групу для реалізації проєкту створення та забезпечення діяльності ситуаційних центрів у системі МО України [1; 6]. Завданнями групи була підготовка пропозицій та інформаційних матеріалів щодо:

1) розробки шляхів створення ситуаційних центрів;

2) всебічного аналізу загроз для визначення ключових напрямів реагування;

3) прогнозування можливих кризових ситуацій із подальшою розробкою управлінських рішень та рекомендацій для протидії негативним впливам;

4) координації дій ситуаційних центрів МО України із відповідними центрами ЗСУ щодо реагування на виклики;

5) оцінювання перспектив інтеграції систем центрів у єдину мережу в умовах цифрової трансформації;

6) розроблення положення про структуру та функціонування ситуаційних центрів в МО України;

7) можливості створення резервного ситуаційного центру або центрів на мобільній базі;

8) забезпечення центрів уніфікованим програмним і апаратним обладнанням для взаємодії з аналогічними структурами (урядовими, державними органами, пунктами управління ЗСУ) та аналітичної підтримки при ухваленні управлінських рішень.

Така ініціатива є фундаментальною для посилення здатності країни ефективно протидіяти сучасним загрозам і забезпечувати безпеку держави в умовах нового інформаційного середовища.

У рамках реалізації завдань, зазначених у [2; 8; 10], передбачено виконання комплексу заходів для забезпечення кібернетичної та інформаційної безпеки. Заплановані дії включають таке:

– установлення «портфеля» інформаційних, програмних і апаратних ресурсів програмно-апаратного комплексу, оцінка їх критичності для структури та/або її функціонування, а також аналіз можливих наслідків порушення конфіденційності, цілісності, доступності інформації, недоступності функцій інформаційних систем, чи збоїв у роботі їх компонентів;

– розробка політики управління ризиками у сфері кібернетичної та інформаційної безпеки, створення методології їх оцінювання та обробки;

– проведення аналізу платформи для оновлення даних про функціонування програмно-апаратного комплексу, технологічні процеси обробки інформації, визначення критичних ресурсів та компонентів комплексу для забезпечення кібербезпеки;

– оновлення переліку загроз й оцінка ризиків інформаційної безпеки у випадку виявлення змін в технології обробки даних, інтеграції нових програмних чи апаратних компонентів, або зміни списку критичних інформаційних ресурсів та компонентів платформи;

– розробка чи оновлення технічного завдання на створення комплексної системи захисту інформаційних ресурсів, а також оновлення документації в разі виявлення нових ризиків чи загроз;

– подальше уточнення та коригування проектної, технічної та іншої документації щодо комплексної системи захисту інформації ІТС з описом реалізованих організаційних та технічних заходів безпеки;

– становлення чітких правил розмежування, надання, зміни чи скасування прав доступу користувачам і адміністраторам до функцій платформи, а також забезпечення контролю (аудиту) використання цих прав;

– організація управління автентифікаційними атрибутами (надання, скасування, контроль) для користувачів і адміністраторів, включно із зовнішніми носіями даних для доступу до функцій платформи;

– забезпечення стабільної роботи ІТ-платформи в реальному часі, зокрема виконання резервного копіювання даних і елементів платформи, збе-

реження резервних копій, відновлення даних і заміни вихідних з ладу компонентів.

На основі вищезазначених заходів необхідно приділити увагу аналізу інцидентів кібербезпеки та модифікаціям існуючих загроз, які можуть вплинути на стабільність функціонування системи централізації в структурах Міністерства оборони України. Такі ризики можуть різнитися за ступенем небезпеки, що дозволяє класифікувати кіберінциденти та визначати пріоритетність реагування. Категоризація кіберінцидентів залежить від причин їх виникнення і є ключовою для прийняття рішень щодо необхідності оперативного реагування.

Отже, наукове обґрунтування перспектив створення організаційної структури у складі СЦ МО України із завданнями реагування на кіберзагрози, що виникають в інформаційно-аналітичних системах, упровадження нових систем та інформаційних технологій, об'єднання та використання на одній платформі існуючих розрізнених інформаційних систем і технічної підтримки функціонування програмно-апаратного комплексу (платформи) набирає критичного характеру та є доволі виваженим. Враховуючи зазначене, необхідно зробити наголос на необхідності створення та введенні у штатний розпис організаційної структури у складі СЦ МО України з завданнями реагування на виникаючі кіберзагрози. Формування та розвиток у складі СЦ МО України необхідних військових організаційних структур для дій у кіберпросторі, їх комплектування, підготовка та всебічне забезпечення дозволить:

1) визначити завдання для ЗС України у частині здійснення оборони кіберпростору (участі у заходах з кібероборони держави);

2) визначити основні функції та повноваження МО України та ЗС України у керівництві заходами з кібероборони України та кібервійськами;

3) забезпечити оперативними інформаційно-аналітичними матеріалами в ході застосування упершій хвилі відсічі і стримування збройної агресії проти України кібервійськ з проведенням дій (операцій) у кіберпросторі та стримуванні подальшої ескалації воєнного конфлікту [9];

4) забезпечити підтримання спроможностей сил системи МО України та ЗС України щодо завдання противнику у кіберпросторі політичних, економічних, воєнних та інших втрат, з огляду на це, він буде змушений відмовитися від ескалації збройної агресії проти України;

5) надати стратегічну мобільність у веденні асиметричних, мережецентричних, багатосферних і непрямих дій у кіберпросторі, які нівелюватимуть чисельну та технологічну перевагу противника в інформаційному просторі та кіберпросторі [3];

6) створити комплексну систему захисту інформації та кібербезпеки в ІТС СЦ МО України та ЗС України в інтересах зміцнення безпекового середовища держави;

7) проводити розробку та тестування технічних рішень за експертної підтримки держав-членів НАТО та партнерів в ІТС СЦ МО України та ЗС України;

8) практично залучити фахівців (спеціалістів) з кібербезпеки до участі у навчаннях НАТО з кібербезпеки, багатонаціональних навчаннях;

9) здійснити державно-приватне партнерство у сфері кібероборони, у т. ч. залучення висококваліфікованих цивільних фахівців приватних структур, ресурсів ІТ-компаній до виконання завдань з кібероборони держави в умовах постійного деструктивного кібервпливу.

Висновки. З огляду на змістовний аналіз матеріалу та ключові пріоритети державної політики у сферах національної безпеки й оборони, а також враховуючи потребу у створенні й функціонуванні системи СЦ ЗСУ та СЦ МО України, може бути обґрунтовано необхідність формування спеціалізованої організаційної структури в рамках МО України. Основним завданням цієї структури стане реагування на інформаційні та кіберзагрози воєнного характеру. Її діяльність здійснюватиметься під загальною координацією Національного координаційного центру кібербезпеки у тісній співпраці з іншими суб'єктами, які займаються забезпеченням кібербезпеки держави.

Список використаних джерел:

1. В Міноборони України буде створено ситуаційний центр. URL: https://opk.com. ua/%D0%B2-%D0%BC%D1%96%D0%BD%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D0%B1%D1%83%D0%B4%D0%B5-%D1%81%D1%82%D0%B2%D0%BE%D1%80%D0%B5% D0%BD%D0%BE-%D1%81%D0%B8/

2. Відомості про виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. Офіційний вісник України. 2019. № 50. ст. 1697.

3. Всеохоплююча оборона України: стан, проблеми та заходи щодо зміцнення кібероборони держави і створення кібервійськ. URL: https://opk.com.ua/%D0%B2%D1%81%D0%B5% D0%BE%D1%85%D0%BE%D0%BF%D0%BB%D1%8E%D1%8E%D1%87% D0%B0-%D0%BE% D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B0-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D1%81%D1%82%D0%B0%D0%BD-%D0%BF%D1%80/.

4. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г.Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія. Харків: НУЦЗУ, 2024. 244 с.

5. Живило Є.О. Формування та запровадження ситуаційного управління сектором безпеки та оборони держави – основа ефективної системи державного управління. Публічне управління XXI століття: погляд у майбутнє : збірник тез XXI Міжнародного наукового конгресу. Харків : Вид-во ХарРІ НАДУ "Магістр", 2021. URL: %D0%A1%D0%B8%D1%82%D1%83 %D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9%20%D1%86%D0%B5%D1% 82%D1%80_%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F/zbirnik_kongress_2021.pdf (дата звернення: 22.09.2022). DOI: https://doi.org/10.34213/mnkongr.2021.

6. Зеленський увів у дію рішення РНБО щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери нацбезпеки. URL: //https://ua.interfax.com.ua/news/ general/751001.html

7. Новіков В.О. Information and hybrid wars in the current environment: public-administrative aspect // *Public administration and state security aspects.* 2023. Vol. 2. P. 43–51.

8. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету міністрів України від 19.06.2019 р. № 518. URL: https://zakon.rada. gov.ua/laws/show/518-2019-%D0%BF#Text.

9. Про рішення Ради національної безпеки і оборони України від 20.08.2021 р. "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 17.09.2021 р. № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121.

10. Технічні вимоги на створення спеціалізованого програмного забезпечення "Державний реєстр об'єктів критичної інформаційної інфраструктури". Департамент кіберзахисту Адміністрації Держспецзв'язку. Київ, 2021, 31 с.

References:

1. A situation center will be created at the Ministry of Defense of Ukraine. URL: https://opk.com. ua/%D0%B2-%D0%BC%D1%96%D0%BD%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D0%B1%D1%83%D0%B4%D0%B5-%D1%81%D1%82%D0%B2%D0%BE%D1%80%D0%B5% D0%BD%D0%BE-%D1%81%D0%B8/

2. Information on the implementation of the General requirements for cyber protection of critical infrastructure facilities: Resolution of the Cabinet of

Ministers of Ukraine dated 19.06.2019. No. 518. Official Gazette of Ukraine. 2019. No. 50. p. 1697.

3. Comprehensive defense of Ukraine: status, problems and measures to strengthen the state's cyber defense and create cyber troops. URL: https://opk.com.ua/%D0%B2%D1%81%D0%B5% D0%BE%D1%85%D0%BE%D0%BF%D0%BB%D1%8E%D1%8E%D1%87% D0%B0-%D0%BE% D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B0-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D1%81%D1%82%D0%B0%D0%BD-%D0%BF%D1%80/.

4. Dombrovska S.M., Pomaza-Ponomarenko A.L., Kryukov O.I., Poroka S.G. Information threats and communication infrastructure in the state sector: monograph. Kharkiv: NUCZU, 2024. 244 p.

5. Zhivylo E.O. Formation and implementation of situational management of the security and defense sector of the state - the basis of an effective system of public administration. Public administration of the 21st century: a look into the future: collection of abstracts of the 21st International Scientific Congress. Kharkiv: Publishing house of KharRI NAPU "Master", 2021. URL: %D0%A1%D0%B8%D1%82%D1%83 %D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9%20%D1%86%D0%B5%D1% 82%D1%80_%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F/zbirnik_kongress_2021.pdf. DOI: https://doi.org/10.34213/mnkongr.2021.

6. Zelenskyy put into effect the NSDC decision on improving the network of situational centers and digital transformation of the national security sphere. URL: //https://ua.interfax.com.ua/news/ general/751001.html.

7. Novikov V.O. Information and hybrid wars in the current environment: public-administrative aspect // Public administration and state security aspects. 2023. Vol. 2. P. 43–51.

8. On approval of the General requirements for cyber protection of critical infrastructure facilities: Resolution of the Cabinet of Ministers of Ukraine dated 06/19/2019 No. 518. URL: https://zakon.rada. gov.ua/laws/show/518-2019-%D0%BF#Text.

9. On the decision of the National Security and Defense Council of Ukraine dated 08/20/2021 "On the Strategic Defense Bulletin of Ukraine": Decree of the President of Ukraine dated September 17, 2021 No. 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121.

10. Technical requirements for the creation of specialized software "State Register of Critical Information Infrastructure Objects". Cyber Defense Department of the State Special Communications Administration. Kyiv, 2021, 31 p.

дата надходження статті: 30.04.2025
дата прийняття статті: 16.05.2025
дата публікації: 25.06.2025