**DOI: 10.52363/2414-5866-2024-1-48**
**УДК: 351.861:004.056.5(477)**

***Ласуков О. Є.*** *начальник відділу інформаційних технологій, електронних комунікацій та захисту інформацій Черкаського інституту пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України*
*ORCID: 0009-0006-4780-1202*

**Lasukov O.** *head of the department of information technology, electronic communications, and information security at the cherkasy institute of fire safety named after the heroes of chernobyl, National university of civil protection of Ukraine*

# МЕХАНІЗМИ МІЖВІДОМЧОЇ КООРДИНАЦІЇ У СФЕРІ КІБЕРБЕЗПЕКИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ: ДОСВІД ВОЄННОГО СТАНУ

# MECHANISMS OF INTERAGENCY COORDINATION IN THE FIELD OF CYBER SECURITY IN THE SECURITY AND DEFENSE SECTOR OF UKRAINE: THE EXPERIENCE OF MARTIAL LAW

*Дослідження присвячене аналізу механізмів міжвідомчої координації у сфері кібербезпеки сектору безпеки і оборони України в умовах воєнного стану, запровадженого внаслідок повномасштабної російської агресії 24 лютого 2022 року. Проблема ефективної координації діяльності різних відомств та структур сектору безпеки і оборони стала першочерговою в контексті безпрецедентних кібератак на критичну інформаційну інфраструктуру держави, що супроводжують конвенційні військові дії. Метою роботи є виявлення особливостей функціонування механізмів міжвідомчої координації за воєнного стану, оцінка їх ефективності та розробка рекомендацій щодо удосконалення системи координації для забезпечення кіберстійкості держави. У роботі проаналізовано нормативно-правову базу, інституційну структуру та практичні аспекти координаційної діяльності Національного координаційного центру кібербезпеки при РНБО України, Державної служби спеціального зв'язку та захисту інформації, Служби безпеки України, розвідувальних органів та Міністерства оборони України. Дослідження виявило, що у воєнний час відбулася значна трансформація координаційних механізмів у напрямку їх централізації, скорочення часу прийняття рішень та посилення оперативної взаємодії між суб'єктами забезпечення кібербезпеки. Водночас ідентифіковано проблемні аспекти, зокрема недостатню синхронізацію дій цивільного та військового компонентів системи кібербезпеки, брак уніфікованих протоколів обміну інформацією про кіберінциденти та необхідність удосконалення механізмів*



ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

*залучення приватного сектору до забезпечення кіберстійкості критичної інфраструктури.*

***Ключові слова:*** *міжвідомча координація, кібербезпека, сектор безпеки і оборони, воєнний стан, кіберстійкість, критична інфраструктура, кіберзагрози, інформаційна безпека, управління, нормативно-правове забезпечення.*

*The study is devoted to a comprehensive analysis of interagency coordination mechanisms in the field of cybersecurity within Ukraine's security and defense sector under martial law, introduced as a result of the full-scale Russian aggression on February 24, 2022. The issue of effective coordination among various agencies and structures of the security and defense sector has become critically important in the context of unprecedented cyberattacks on the state's critical information infrastructure that accompany conventional military operations. The purpose of the research is to identify the specific features of interagency coordination mechanisms under martial law, assess their effectiveness, and develop recommendations for improving the coordination system to ensure the state's cyber resilience. The study analyzes the legal framework, institutional structure, and practical aspects of coordination activities of the National Cybersecurity Coordination Center under the National Security and Defense Council of Ukraine, the State Service of Special Communications and Information Protection, the Security Service of Ukraine, intelligence agencies, and the Ministry of Defense. The research found that during martial law, coordination mechanisms have undergone significant transformation toward greater centralization, faster decision-making, and enhanced operational interaction among cybersecurity entities. At the same time, problematic aspects were identified, including insufficient synchronization between civilian and military components of the cybersecurity system, a lack of unified protocols for cyber incident information exchange, and the need to improve mechanisms for involving the private sector in ensuring the cyber resilience of critical infrastructure.*

***Keywords:*** *interagency coordination, cybersecurity, security and defense sector, martial law, cyber resilience, critical infrastructure, cyber threats, information security, management, legal framework.*

**Постановка проблеми.** Повномасштабне вторгнення російської федерації на територію України 24 лютого 2022 року змінило безпекове середовище держави та поставило безпрецедентні виклики перед системою забезпечення кібербезпеки. Кіберпростір став повноцінним театром воєнних дій, де поряд із конвенційними операціями розгортається масштабне кіберпротистояння, що охоплює критичну інформаційну інфраструктуру, системи державного управління, об'єкти енергетики, транспорту та фінансового сектору. За даними Державної служби спеціального зв'язку та захисту інформації України, протягом першого року повномасштабної війни було зафіксовано понад 2194 кібератаки на об'єкти критичної інфраструктури, що втричі перевищує показники довоєнного періоду. Така інтенсивність кіберагресії вимагає не лише технічних засобів протидії, але й ефективної

системи координації зусиль усіх суб'єктів забезпечення кібербезпеки. Особливо важливою стає злагодженість дій між військовими та цивільними структурами, оперативність прийняття рішень та здатність системи адаптуватися до динамічних змін характеру загроз. Досвід воєнного стану продемонстрував як сильні сторони української системи кібербезпеки, наприклад її резильєнтність та здатність до швидкої мобілізації ресурсів, так і системні проблеми, пов'язані з недосконалістю координаційних механізмів, дублюванням функцій окремих суб'єктів та недостатньою інтеграцією приватного сектору в загальнодержавну систему кіберзахисту.

**Аналіз останніх досліджень і публікацій.** Проблематика міжвідомчої координації у сфері кібербезпеки досліджувалася у працях вітчизняних науковців О. Довганя [1], В. Бурячка [2], Д. Дубова [3], які заклали теоретико-методологічні основи розуміння кібербезпеки як складової національної безпеки України. Питання інституційного забезпечення кібербезпеки розглядали В. Шеломенцев [4] та М. Гуцалюк [5], акцентуючи увагу на необхідності створення ефективної системи координації між різними суб'єктами. Досвід функціонування систем кібербезпеки в умовах гібридних загроз аналізували І. Діордіца [6] та С. Вдовенко [7]. При цьому специфіка координаційних механізмів в умовах воєнного стану залишається недостатньо дослідженою, що актуалізує необхідність комплексного аналізу трансформації системи міжвідомчої координації в період повномасштабної війни та її адаптації до нових викликів і загроз.

**Формулювання цілей статті.** дослідження та узагальнення механізмів міжвідомчої координації у сфері кібербезпеки сектору безпеки і оборони України у воєнний час, а також оцінка їх ефективності та розробка пропозицій щодо удосконалення системи координації для підвищення рівня кіберстійкості держави.

**Виклад основного матеріалу дослідження.** Теоретичне осмислення механізмів міжвідомчої координації у сфері кібербезпеки базується на синтезі концепцій державного управління, теорії національної безпеки та кібернетичних підходів до забезпечення стійкості складних систем. Міжвідомча координація в контексті кібербезпеки - це система організаційно-правових, інформаційно-аналітичних та оперативно-технічних заходів. Вони спрямовані на узгодження діяльності різних суб'єктів забезпечення кібербезпеки для досягнення спільної мети - захисту національного кіберпростору від загроз різного походження. Кіберпростір характеризується транскордонністю, анонімністю акторів та швидкістю поширення загроз. Ці особливості визначають спеціальні вимоги до координаційних механізмів. Система управління повинна забезпечувати оперативність реагування, гнучкість та адаптивність.

Нормативно-правова база міжвідомчої координації у сфері кібербезпеки України формувалася поетапно. Вона відображає еволюцію розуміння кіберзагроз та їх впливу на національну безпеку. Базовим документом стала Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року №96/2016. Вона визначила основні принципи та напрями

забезпечення кібербезпеки держави [9]. Закон України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року №2163-VIII створив правову основу для функціонування національної системи кібербезпеки та визначив повноваження основних суб'єктів [10].

Важливим етапом стало прийняття нової Стратегії кібербезпеки України на 2021-2025 роки. Її затверджено Указом Президента України від 26 серпня 2021 року №447/2021. Документ врахував досвід протидії гібридним загрозам та визначив пріоритети розвитку системи кібербезпеки в умовах зростання інтенсивності кібератак [11].

Інституційна архітектура системи забезпечення кібербезпеки сектору безпеки і оборони України має багаторівневу структуру з розподіленими повноваженнями між різними суб'єктами. Центральним координаційним органом виступає Національний координаційний центр кібербезпеки (НКЦК) при Раді національної безпеки і оборони України, створений згідно Указу Президента України від 7 червня 2016 року №242/2016 [12]. НКЦК здійснює координацію діяльності суб'єктів сектору безпеки і оборони з питань кібербезпеки, аналіз стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, координацію діяльності з реагування на кіберінциденти. Державна служба спеціального зв'язку та захисту інформації України виконує функції головного органу у системі центральних органів виконавчої влади із забезпечення формування та реалізації державної політики у сферах кібербезпеки, кіберзахисту, захисту державних інформаційних ресурсів [13]. Служба безпеки України відповідає за протидію кіберзлочинності, кібертероризму та кібердиверсіям, здійснює контррозвідувальне забезпечення кіберпростору [14]. Міністерство оборони України та Генеральний штаб Збройних Сил України забезпечують кіберзахист у воєнній сфері, організовують та проводять заходи з кібероборони держави.

Механізми координації між цими суб'єктами в довоєнний період базувалися на кількох елементах. Регулярні засідання НКЦК, функціонування Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA при Держспецзв'язку, проведення спільних навчань та тренувань з кібербезпеки. Система ситуаційних центрів забезпечувала обмін інформацією про кіберінциденти та координацію заходів реагування.

Практика функціонування цієї системи виявила низку проблемних аспектів. Недостатня оперативність прийняття рішень через бюрократичні процедури узгодження. Дублювання функцій окремих суб'єктів. Брак чітких протоколів взаємодії в кризових ситуаціях. Обмеженість ресурсів для забезпечення кіберзахисту об'єктів критичної інфраструктури.

Запровадження воєнного стану відповідно до Указу Президента України від 24 лютого 2022 року №64/2022 внесло суттєві зміни в умови функціонування системи кібербезпеки. Правовий режим воєнного стану надав можливість централізації управління силами та засобами кібербезпеки. Спростилися процедури прийняття рішень, з'явилася можливість мобілізації ресурсів приватного сектору для потреб кіберзахисту.

Аналіз практики функціонування механізмів міжвідомчої координації в умовах війни дозволяє виявити ключові трансформації, що відбулися в системі забезпечення кібербезпеки. Насамперед відбулася фактична централізація оперативного управління кіберзахистом через механізми Ставки Верховного Головнокомандувача та Генерального штабу ЗСУ, що дозволило значно скоротити час від виявлення загрози до прийняття рішення про протидію. За даними CERT-UA, середній час реагування на критичні кіберінциденти скоротився з 4-6 годин у довоєнний період до 30-45 хвилин у березні-квітні 2022 року. Така оперативність досягається завдяки впровадженню режиму цілодобового чергування груп реагування, спрощенню процедур узгодження рішень та наданню розширених повноважень оперативним підрозділам.

Важливою інновацією стало створення механізмів оперативної координації з недержавними суб'єктами кібербезпеки, в тому числі волонтерськими організаціями та приватними компаніями. Формування "ІТ-армії України" як добровільного об'єднання фахівців з кібербезпеки для проведення кібероперацій проти інформаційної інфраструктури агресора продемонструвало ефективність гібридних форм координації, що поєднують державні та громадські ресурси. Координація діяльності "ІТ-армії" здійснюється через спеціалізовані канали комунікації з використанням захищених месенджерів, що забезпечує оперативність постановки завдань та отримання зворотного зв'язку про результати операцій. За оцінками Міністерства цифрової трансформації України, діяльність "ІТ-армії" дозволила завдати значних збитків інформаційній інфраструктурі агресора, порушивши роботу понад 4000 російських веб-ресурсів, включаючи критично важливі державні сервіси.

Міжнародний вимір координації вийшов на перший план в умовах воєнного стану. Україна отримала безпрецедентну технічну допомогу від партнерів, зокрема від Агентства кібербезпеки та захисту інфраструктури США (CISA), Національного центру кібербезпеки Великої Британії (NCSC), кіберцентрів країн ЄС та НАТО. Координація міжнародної допомоги здійснюється через спеціально створені механізми, включаючи Ukraine Cyber Defense Fund та платформу координації технічної допомоги під егідою ЄС. Важливим елементом стала інтеграція України до системи раннього попередження про кіберзагрози НАТО, що дозволяє отримувати оперативну інформацію про підготовку кібератак та координувати заходи протидії.

Однак аналіз виявляє низку проблемних аспектів у функціонуванні координаційних механізмів. Зберігається певна роз'єднаність між цивільним та військовим компонентами системи кібербезпеки, що ускладнює комплексне планування операцій у кіберпросторі. Відсутність єдиної системи класифікації кіберінцидентів та уніфікованих протоколів обміну інформацією між різними суб'єктами призводить до дублювання зусиль та неоптимального розподілу ресурсів. Проблемою залишається недостатня захищеність каналів комунікації між окремими елементами системи, що створює ризики компрометації оперативної інформації.

Особливої уваги потребує координація заходів із забезпечення кіберстійкості об'єктів критичної інфраструктури. Досвід кібератак на енергетичну систему України восени 2022 року продемонстрував необхідність тіснішої координації між Міністерством енергетики, операторами енергосистем та суб'єктами забезпечення кібербезпеки. Створення галузевих центрів реагування на кіберінциденти (SOC) в енергетичному секторі стало важливим кроком, однак їх інтеграція в загальнодержавну систему кібербезпеки потребує подальшого вдосконалення координаційних механізмів.

Ефективність координації значною мірою залежить від якості інформаційно-аналітичного забезпечення. Під час війни зросла роль розвідувальних органів у виявленні та попередженні кіберзагроз. Головне управління розвідки Міністерства оборони України та Служба зовнішньої розвідки активно взаємодіють з кіберпідрозділами. Метою є отримання випереджувальної інформації про плани противника в кіберпросторі.

Механізми передачі розвідувальної інформації цивільним суб'єктам кібербезпеки потребують оптимізації. Необхідно враховувати вимоги оперативності та збереження конфіденційності джерел.

Координація навчальної та тренувальної діяльності в умовах воєнного стану є важливим аспектом. Проведення масштабних кібернавчань стало проблематичним через необхідність концентрації зусиль на реальних загрозах. Але потреба в підготовці фахівців та відпрацюванні взаємодії зросла. Рішенням стало впровадження системи "навчання через дію". Реальні кіберінциденти використовуються як навчальні кейси для підвищення кваліфікації персоналу [15]. Національний університет оборони України імені Івана Черняховського спільно з Київським національним університетом імені Тараса Шевченка розробили програми експрес-підготовки фахівців з кібербезпеки для потреб сектору безпеки і оборони, що частково компенсувало кадровий дефіцит.

Фінансове забезпечення координаційної діяльності за умов військового протистояння змінилося. З одного боку, збільшилися видатки на кібербезпеку в рамках оборонного бюджету, з іншого - обмеженість ресурсів вимагає оптимізації їх розподілу. Механізми координації фінансування заходів з кібербезпеки через Міністерство фінансів України та профільні відомства потребують удосконалення для забезпечення оперативності виділення коштів на критичні потреби. Залучення міжнародної фінансової допомоги, включаючи грантів від союзників та міжнародних організацій, вимагає координації між Міністерством закордонних справ, Міністерством цифрової трансформації та суб'єктами забезпечення кібербезпеки.

**Висновки.** Дослідження механізмів міжвідомчої координації у сфері кібербезпеки сектору безпеки і оборони України в умовах війни дозволяє дійти висновку про фундаментальну трансформацію системи забезпечення кіберзахисту держави під впливом безпрецедентних викликів повномасштабної війни. Аналіз показав, що українська система кібербезпеки виявила значну адаптивність та резильєнтність, спромігшись не лише

витримати масштабні кібератаки, але й підвищити ефективність протидії кіберзагрозам через удосконалення координаційних механізмів. Ключовими факторами успіху стали централізація оперативного управління, скорочення циклу прийняття рішень, інтеграція державних та недержавних акторів кібербезпеки, а також активна міжнародна співпраця. Разом з тим дослідження виявило системні проблеми, що потребують вирішення для подальшого зміцнення кіберстійкості держави. Недостатня синхронізація дій цивільного та військового компонентів системи кібербезпеки, відсутність уніфікованих протоколів обміну інформацією, обмеженість ресурсного забезпечення та кадровий дефіцит залишаються викликами, що потребують комплексного підходу до їх подолання. Досвід воєнного стану довів критичну важливість ефективної міжвідомчої координації для забезпечення кібербезпеки держави та необхідність подальшого розвитку інституційних, організаційних та технічних механізмів координації.

Перспективними напрямами удосконалення системи є створення єдиного операційного центру кібербезпеки з інтеграцією всіх ключових суб'єктів, розробка та впровадження автоматизованих систем обміну інформацією про кіберзагрози, посилення публічно-приватного партнерства у сфері кіберзахисту критичної інфраструктури, розширення програм підготовки фахівців з кібербезпеки. Отриманий досвід функціонування системи кібербезпеки в екстремальних умовах воєнного стану має важливе значення не лише для України, але й для міжнародної спільноти, демонструючи можливості ефективної протидії кіберагресії через консолідацію зусиль всіх елементів суспільства та міжнародну солідарність.

**Список використаних джерел:**


1. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. Інформаційна безпека людини, суспільства, держави. 2015. № 3. С. 6-17.
2. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. Львів, 2018. 320 с.
3. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України. Київ: НІСД, 2011. 30 с.
4. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією. 2012. №1. С. 312-320.
5. Гуцалюк М.В. Оцінка реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик. Журнал "Інформація і право". 2(29)/2019. С. 90-99
6. Ліпкан В. О., Діордіца І.В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право. 2017. № 5. С. 174-180.
7. Вдовенко С., Даник Ю., Пермяков О. Досвід розвитку систем кібербезпеки та кібероборони провідних країн світу. Сучасні інформаційні технології у сфері безпеки та оборони. 2020. 37(1). С. 31-48.

8. Звіт Державної служби спеціального зв'язку та захисту інформації України про стан кібербезпеки за 2023 рік. URL: https://scpc.gov.ua/uk/articles/334

9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.2016 №96/2016.

10. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 №2163-VIII. Відомості Верховної Ради України. 2017. №45. Ст. 403.

11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 №447/2021.

12. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 №242/2016. Урядовий кур'єр. 2016. №107.

13. Положення про Державну службу спеціального зв'язку та захисту інформації України: Постанова Кабінету Міністрів України від 03.09.2014 №411.

14. Про Службу безпеки України: Закон України від 25.03.1992 №2229-XII. Відомості Верховної Ради України. 1992. №27. Ст. 382.

15. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки : монографія / За заг. ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.

## References:

1. Dovhan O.D. Pravovi zasady formuvannia i rozvytku systemy zabezpechennia informatsiinoi bezpeky Ukrainy. Informatsiina bezpeka liudyny, suspilstva, derzhavy. 2015. № 3. S. 6-17.

2. Buriachok V.L., Tolubko V.B., Khoroshko V.O., Toliupa S.V. Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt. Lviv, 2018. 320 s.

3. Dubov D.V. Kiberbezpeka: svitovi tendentsii ta vyklyky dlia Ukrainy. Kyiv: NISD, 2011. 30 s.

4. Shelomentsev V.P. Pravove zabezpechennia systemy kibernetychnoi bezpeky Ukrainy ta osnovni napriamy yii udoskonalennia. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu. 2012. №1. S. 312-320.

5. Hutsaliuk M.V. Otsinka realizatsii Stratehii kiberbezpeky Ukrainy z urakhuvanniam dosvidu yevropeiskykh i svitovykh praktyk. Zhurnal "Informatsiia i pravo". 2(29)/2019. S. 90-99

6. Lipkan V. O., Diorditsa I.V. Natsionalna systema kiberbezpeky yak skladova chastyna systemy zabezpechennia natsionalnoi bezpeky Ukrainy. Pidpryiemnytstvo, hospodarstvo i pravo. 2017. № 5. S. 174-180.

7. Vdovenko S., Danyk Yu., Permiakov O. Dosvid rozvytku system kiberbezpeky ta kiberoborony providnykh krain svitu. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 2020. 37(1). S. 31-48.

8. Zvit Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy pro stan kiberbezpeky za 2023 rik. URL: https://scpc.gov.ua/uk/articles/334

9. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 15.03.2016 №96/2016.

10. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 №2163-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2017. №45. St. 403.

11. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 26.08.2021 №447/2021.

12. Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky: Ukaz Prezydenta Ukrainy vid 07.06.2016 №242/2016. Uriadovyi kurier. 2016. №107.

13. Polozhennia pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy: Postanova Kabinetu Ministriv Ukrainy vid 03.09.2014 №411.

14. Pro Sluzhbu bezpeky Ukrainy: Zakon Ukrainy vid 25.03.1992 №2229-XII. Vidomosti Verkhovnoi Rady Ukrainy. 1992. №27. St. 382.

15. Danyk Yu. H., Hryshchuk R. V. Osnovy kibernetychnoi bezpeky : monohrafiia / Za zah. red. prof. Yu. H. Danyka. Zhytomyr : ZhNAEU, 2016. 636 p.



дата надходження статті: 08.05.2024
дата прийняття статті: 21.05.2024
дата публікації: 28.06.2024