УДК 343.9
DOI https://doi.org/10.24144/2307-3322.2025.92.4.28

ПРОТИДІЯ КІБЕРЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ: ІНСТИТУЦІЙНО-ПРЕВЕНТИВНА СПРОМОЖНІСТЬ

Рябчинська О.П.,
доктор юридичних наук, професор,
професор кафедри кримінального права
та правоохоронної діяльності
Запорізького національного університету
ORCID: 0000-0002-9012-3332

Рябчинська О.П. Протидія кіберзагрозам національній безпеці України: інституційно-превентивна спроможність.

У статті проаналізовано механізм протидії кіберзагрозам національній безпеці крізь призму формування інституційно-превентивної спроможності України. Актуальність теми зумовлена інтенсифікацією використання кіберпростору як інструменту гібридної війни, що потребує переходу від фрагментарних заходів безпеки до спеціальної превенції – активного випередження, виявлення та нейтралізації загроз на ранніх стадіях їх виникнення. Успіх такої стратегії безпосередньо залежить від злагодженої координації між державними інституціями та об'єднання їхніх ресурсів.

Особливу увагу приділено аналізу новітньої нормативно-правової бази як фундаменту розбудови превентивної спроможності суб'єктів. У роботі детально розглянуто положення Постанови Кабінету Міністрів України від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» та Порядку взаємодії, затвердженого постановою КМУ від 13 листопада 2025 року № 1471. Ці акти проаналізовано як ключові регуляторні інструменти, що забезпечують інституційну здатність правоохоронних, розвідувальних та військових органів України ефективно взаємодіяти з метою переривання злочинних посягань на ранніх етапах ініціації кібератак.

У статті структуровано багаторівневу модель координації, де інституційні ланки (Президент України, РНБО, НКЦК, КМУ) розглядаються як стратегічні центри формування превентивного потенціалу держави. Досліджено функціонування підрозділів кіберзахисту в органах державної влади (Міноборони, НБУ, Мін'юст) як елементів системи кримінологічного запобігання, що забезпечують захищеність критичних інформаційних ресурсів. Така багаторівнева модель дозволяє консолідувати адміністративні, правоохоронні та військові спроможності для забезпечення цілісності національної системи кіберзахисту. У межах цієї структури подальше інституційне та функціональне вдосконалення органів реагування на кіберзагрози у Збройних Силах України є вирішальним чинником для підвищення ефективності запобігання, своєчасного виявлення та нейтралізації викликів національній безпеці в умовах гібридної війни.

Ключові слова: національна безпека України, кібербезпека, інституційно-превентивна спроможність, рівні координації, спеціальна превенція, координація дій, Збройні Сили України, гібридна війна, запобігання кіберзагрозам.

Riabchynska O.P. Countering cyber threats to Ukraine's national security: institutional and preventive capability.

The article analyzes the mechanism of countering cyber threats to national security through the lens of developing the institutional and preventive capability of Ukraine. The relevance of the topic is driven by the intensified use of cyberspace as a tool of hybrid warfare, which necessitates a transition from fragmented security measures to special prevention – the active anticipation, detection, and neutralization of threats at the early stages of their emergence. The success of such a strategy directly depends on the seamless coordination between state institutions and the consolidation of their resources.

Particular attention is paid to the analysis of the latest regulatory framework as a foundation for building the preventive capability of stakeholders. The study examines in detail the provisions of the Cabinet of Ministers of Ukraine Resolution No. 1533 of November 26, 2025, «Certain Issues of Responding to Cyber Incidents, Cyberattacks, and Cyber Threats,» and the «Procedure for Interaction,» approved by the CMU Resolution No. 1471 of November 13, 2025. These acts are analyzed as key regulatory instruments that ensure the institutional capacity of Ukraine's law enforcement, intelligence, and military agencies to interact effectively to disrupt criminal encroachments at the early stages of cyberattack initiation.

The article structures a multi-level coordination model, where institutional links (the President of Ukraine, the NSDC, the NCCC, and the Cabinet of Ministers) are viewed as strategic centers for forming the state's preventive potential. The functioning of cyber defense units within state authorities (Ministry of Defense, National Bank, Ministry of Justice) is explored as elements of a criminological prevention system that ensures the security of critical information resources. Such a multi-level model allows for the consolidation of administrative, law enforcement, and military capabilities to ensure the integrity of the national cyber defense system. Within this framework, further institutional and functional improvement of cyber threat response bodies in the Armed Forces of Ukraine is a decisive factor for increasing the effectiveness of preventing, timely detecting, and neutralizing challenges to national security in the context of hybrid warfare.

Key words: national security of Ukraine, cybersecurity, institutional and preventive capability, levels of coordination, special prevention, coordination of actions, Armed Forces of Ukraine, hybrid warfare, prevention of cyber threats.

Актуальність теми. В сучасних правових реаліях Україна перебуває в воєнному стані, введеному Указом Президента України № 64/2022 від 24 лютого 2022 року з 24 лютого 2022 року [1] і продовженого Указом № 793/2025 від 20.10.2025 року з 5 листопада 2025 року на 90 діб [2]. Водночас висловлюється думка, що «теоретично та практично найбільш придатним для визначення характеру російської агресії проти України є поняття гібридної війни» [3, с.41]. Вона характеризується існуванням сукупності заздалегідь підготовлених та оперативно реалізованих заходів військового, дипломатичного, економічного, політичного, культурного, енергетичного та інформаційного характеру, спрямованих на досягнення стратегічних цілей, однією з ключових при цьому є підпорядкування інтересів однієї держави іншій в умовах формального збереження суверенітету [4].

Виняткову роль у гібридній війні відіграє інформаційна сфера, яку держава-агресор активно використовує для маніпулювання суспільною свідомістю, підриву довіри до влади та державних інституцій, правоохоронних органів і Збройних сил України. Її інструменти спрямовані на поширення паніки, провокування внутрішніх конфліктів і нав'язування проросійських наративів. Росія також маніпулювала й маніпулює надалі інтерпретаційними рамками в Україні: формуючи не лише інформаційне середовище як частину війни, а й те, як люди сприймають події на полі бою [5]. Паралельно вона поширює фальшиві історичні наративи, спрямовані на міжнародну аудиторію, намагаючись послабити підтримку України шляхом заперечення її права на суверенітет [6]. *Ключовим інструментом інформаційної війни в кіберпросторі сьогодні визнається штучний інтелект.* Генеративні моделі ШІ дозволяють за лічені секунди створювати тексти, відео й зображення, здатні імітувати внутрішні кризи, поширювати сфабриковані новини та провокувати соціальні конфлікти, підживлювати радикалізацію. У такому середовищі ШІ перетворюється на зброю когнітивного впливу, здатну підривати довіру до демократичних інституцій і маніпулювати масовою свідомістю [6].

*Європейські країни також чітко усвідомлюють поширення загроз в інформаційній сфері з боку рф. Зокрема, зарубіжні фахівці наголошують: «*Оборона вже не є виключно військовою: вона психологічна, соціальна, цифрова. Виклик надзвичайно серйозний, адже наступна війна вже почалася. І ведеться вона правдою та контр(дез)інформацією» [7]. Аналітики East Stratcom Task Force визначають появу великих мовних моделей (LLM) як нове поле російської інформаційної війни. Згідно з їх новим звітом, рф та пов'язані з нею структури цілеспрямовано атакують ШІ-моделі, наповнюючи інформаційний простір проросійськими матеріалами, щоб вплинути на навчальні дані та змусити чат-боти відтворювати кремлівські наративи у нібито нейтральній формі. Частка неправдивого або маніпулятивного контенту в десяти провідних чат-ботах зросла з 18% у

2024 році до 35% у 2025-му [8]. Дезінформаційні кампанії типу *Döppelganger*, які веде російська «Агенція соціального проєктування» (SDA), а також масштабне медійне висвітлення їхнього викриття показують, як інформаційний простір може бути пронизаний шляхом клонування легітимних медіа та урядових сайтів, унаслідок чого межа між вигадкою та реальністю для онлайн-аудиторій стає дедалі розмитішою [9]. Рф залишається одним з основних джерел загроз національній та міжнародній кібербезпеці. Вона активно реалізує концепцію інформаційного протиборства, що ґрунтується на поєднанні деструктивних дій у кіберпросторі з інформаційно-психологічними операціями. Механізми цієї концепції широко застосовуються у гібридній війні проти України. В Статегії кібербезпеки 2021 року гібридна агресія Російської Федерації проти України у кіберпростор визнана прямою загрозою кібербезпеці України. Її кібератаки спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності [10].

Отже, перед Україною постає стратегічне завдання: стримувати агресора не лише у традиційній військовій площині, а й ефективно протидіяти гібридній агресії – інформаційній війні та кібератакам, які рф спрямовує проти нашої держави й країн Європи. Ефективна відповідь на такі комплексні виклики потребує чіткої координації державних інституцій. Провідна роль у забезпеченні національної кібербезпеки та викритті й нейтралізації ворожого впливу належить профільним органам сектору безпеки й оборони.

Аналіз наукових публікацій. Теоретичні та практичні проблеми забезпечення інформаційної безпеки в кіберпросторі досліджували А.В. Боровик, А.Г. Вархов, В.В. Волинець, Н.З. Деревянко, В.А. Ліпкан, О.С. Ліпкан, Н.Є. Новікова, І.Ф. Тімкін, Т.Ю. Ткачук, А.В. Тарасюк та ін. Досліджуючи структурно-функциональні характеристики системи національної безпеки, науковці приділяють особливу увагу адміністративно-правовим засадам кібербезпеки. Обґрунтованим є висновок про необхідність чіткого розмежування компетенцій державних органів як ключових суб'єктів кіберзахисту, а також про важливість розвитку державно-приватного партнерства у цій сфері (Тарасюк А.В.) [11], а також те, що «формована мережа координаційних повноважень Ради національної безпеки і оборони є недосконалою та такою, що вимагає перегляду» [12, с. 156]. Необхідним є визначення місця і ролі цього органу в системі суб'єктів сектору безпеки й оборони за європейським зразком.

Наукові положення, висновки та рекомендації попередників значною мірою зберігають свою актуальність. Водночас питання комунікації та координації між суб'єктами забезпечення кібербезпеки й безпосереднього реагування на кіберзагрози та кіберінциденти потребують перегляду. Це зумовлено зміною організаційно-правових засад, зокрема переходом від Стратегії кібербезпеки України 2016 року до нової Стратегії 2021 року, а також ухваленням низки нормативних актів, що запровадили оновлений порядок взаємодії в національній системі кібербезпеки.

Мета статті полягає у дослідженні координації як самостійного повноваження суб'єктів кібербезпеки у сфері спеціальної превенції, виявлення та нейтралізації кіберзагроз національним інтересам.

Виклад основного матеріалу. Засади формування системи суб'єктів забезпечення кібербезпеки були закладені Указом Президента України від 27 січня 2016 року № 21/2016, яким уведено в дію першу Стратегію кібербезпеки України. Цей документ уперше визначив ключових учасників національної системи кібербезпеки, до яких було віднесено були включені Міністерство оборони України (далі – МО України), Державна служба спеціального зв'язку та захисту інформації (далі – Держспецз'вязку), Службу безпеки України (далі СБУ), Національну поліцію України (далі – НП України), Національний банк України (далі – НБУ) та розвідувальні органи. Як слушно зауважували фахівці, «натомість в ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» передбачає дещо інший перелік основних суб'єктів забезпечення кібербезпеки, що окремо виділяються в рамках загальної системи суб'єктів забезпечення кібербезпеки, передбаченої ст. 5 того ж Закону. До їх кола віднесено: РНБО України, Міністерство внутрішніх справ (МВС) України, МО України, Генеральний штаб ЗС України, СБ України, ДСС України, розвідувальні органи тощо» [11, с. 121]. У період реалізації Стратегії кібербезпеки України 2016 року було за-

кладено правове підґрунтя для діяльності центрального координуючого органу. Зокрема, набув чинності Указ Президента України № 242/2016 від 7 червня 2016 року (про створення Національного координаційну центру кібербезпеки – далі НКЦК) [13]. Останній суттєво розширив повноваження НКЦК щодо координації та контролю діяльності суб'єктів сектору безпеки і оборони. На думку фахівців, розширення координаційних функцій НКЦК створило передумови для взаємного дублювання повноважень Центру, СБУ та Держспецзв'язку, що актуалізувало потребу в нормативному впорядкуванні системи суб'єктів забезпечення кібербезпеки [11, с. 123].

В Стратегії кібербезпеки 2021 року звертається увага на недоліки реалізації попередньої Стратегії кібербезпеки України 2016 року, зокрема, на те, що діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства тощо [10].

Аналіз Стратегії дозволяє визначити інституційне зміцнення ключовим елементом розбудови національної системи кібербезпеки. Воно спрямовано на підвищення спроможності держави щодо стримування агресії у кіберпросторі, нейтралізації розвідувально-підривної діяльності та мінімізації загроз кіберзлочинності й кібертероризму. Розбудова національної системи кібербезпеки ґрунтується на засадах, що передбачають: чітке розмежування повноважень та відповідальності суб'єктів; оперативну актуалізацію законодавства відповідно до динаміки загроз; визначення ролей та механізмів взаємодії з акцентом на обміні інформацією. Пріоритетним є розвиток координації та інклюзивного діалогу між державним і приватним секторами, що у поєднанні з демократичним цивільним контролем забезпечує стійкість системи на національному рівні.

Отже, забезпечення дієвої координації між суб'єктами національної системи кібербезпеки та силами оборони є стратегічною ціллю формування потенціалу стримування, що дозволяє мінімізувати віктимність національної інфраструктури та превентивно нейтралізувати кіберзагрози. У широкому розумінні координація (лат. co – з, разом + ordinatus – впорядкований) – погодження, зведення до відповідності, установлення взаємозв'язку, контакту в діяльності людей, між діями, поняттями тощо [14, с. 418].

У сфері державного управління під координацією розуміють узгодження дій різних суб'єктів, яке полягає в спільному розроблені й реалізації заходів, узгоджених за місцем, часом і виконавцями, спрямованих на підвищення ефективності спільної діяльності, зміцнення законності та правопорядку [15, с. 725].

Згідно з ч.1 ст. 5 ЗУ «Про основні засади забезпечення кібербезпеки України» (далі – № 2163-VIII) суб'єктами забезпечення кібербезпеки є: Президент України, РНБО в особі НКЦК; КМУ; Міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; НБУ; оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [16]. Поряд із загальним переліком суб'єктів забезпечення кібербезпеки, спеціальний правовий статус окремих інституцій деталізується у профільному законодавстві відповідно до їхньої функціональної спеціалізації. Зокрема, в органах державної влади та місцевого самоврядування, що є власниками (розпорядниками) інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси або інформація з обмеженим доступом, утворюються спеціалізовані підрозділи кіберзахисту. Згідно зі ст. Закону, керівники таких підрозділів здійснюють безпосереднє керівництво, координацію та контроль заходів із кіберзахисту відповідних об'єктів. Окрему функціональну роль відведено Національному банку України, який забезпечує діяльність Центру кіберзахисту НБУ (включаючи команду реагування на кіберінциденти CSIRT-NBU), що здійснює галузеву координацію у фінансовій сфері.

В ч. 2 ст. 8 ЗУ № 2163-VIII основними суб'єктами національної системи кібербезпеки є такі суб'єкти її забезпечення як: Держспецзв'язку, НП України, СБУ, МОУ та генеральний штаб ЗСУ, розвідувальні органи України, НБУ, МЗС.

В ст. 9 ЗУ № 2163-VIII визначені суб'єкти національної системи реагування на кіберінциденти, кібератаки, кіберзагрози: CERT-UA – національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (національний CSIRT), діяльність якої забезпечується Держспецзв'язку; галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (далі – галузеві, регіональні CSIRT) – створюються органами державної влади або органами місцевого самоврядування (як то MIL.CERT-UA чи CSIRT-NBU); Національна поліція України, Служба безпеки України; приватні команди реагування; Національний координаційний центр кібербезпеки, в складі якого діє Об'єднана група реагування на кіберінциденти, кібератаки, кіберзагрози, до складу якої входять представники НКЦК, Держспецзв'язку, СБУ, НП України та представники інших основних суб'єктів національної системи кібербезпеки (за обґрунтованої необхідності). Поєднання широкого кола основних суб'єктів та розгалуженої системи реагування (національні, галузеві, приватні CSIRT та Об'єднана група при НКЦК) обумовлює об'єктивну потребу в координації їх діяльності. Тож, без узгодження дій між силами безпеки та оборони й технічними командами система ризикує втратити цілісність, що робить її менш спроможною досягати поставлених цілей та ефективно виконувати завдання щодо забезпечення кібербезпеки та захисту кіберпростору держави.

Провідною інституцією забезпечення цілісності національної системи кібербезпеки та її ключовим координатором виступає НКЦК, який є робочим органом РНБО України, утвореним на виконання положень Стратегії кібербезпеки України 2016 року. Правовий статус та порядок діяльності НКЦК визначені в Положенні про Національний координаційний центр кібербезпеки (далі – Положення про НКЦК), затвердженому Указом Президента України від 7 червня 2016 року № 242/2016, відповідно до якого Центр здійснює свою діяльність на підставі ст. 107 Конституції України та Закону України «Про Раду національної безпеки і оборони України» як робочий орган, що реалізує координаційні функції у сфері кібербезпеки [17]. Основними завданням центру щодо реалізації відповідних повноважень є, по-перше, здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку (пп. 1 п. 3 Положення), та, по-друге, участь у забезпеченні розроблення і впровадження суб'єктами забезпечення кібербезпеки механізмів обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків (пп.7 п.3 Положення) [13].

Для цього Центр наділений повноваженнями щодо розроблення і внесення РНБО та її Голові в установленому порядку пропозицій стосовно удосконалення нормативно-правової бази у сфері: забезпечення механізмів взаємодії суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України; узгодження і координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України; координації заходів щодо взаємоузгодженого розгортання підрозділів кібербезпеки Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних органів спеціального призначення та приведення у готовність до виконання завдань в умовах особливого періоду, в умовах воєнного, надзвичайного стану і під час виникнення кризових ситуацій, що загрожують національній безпеці України; взаємодії суб'єктів забезпечення національної безпеки із міжнародними організаціями у сфері кібербезпеки та забезпеченні захисту національних інтересів України на міжнародному рівні [10]. Для реалізації завдань Центр взаємодіє з державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями.

Важливим аспектом координаційної діяльності Кабінету Міністрів України (далі – КМУ) є повноваження щодо встановлення порядку взаємодії суб'єктів національної системи реагування на кіберінцеденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, з правоохоронними органами, контррозвідувальними органами, розвідувальними органами та суб'єктами оперативно-розшукової діяльності (п. 3 ст. 5 ЗУ «Про основні засади забезпечення кібербезпеки»). Саме відсутність чітко унормованого механізму взаємодії між різними інституціями, задіяними в сфері забезпечення національної безпеки визнавалося критичним недоліком, що негативно позначався на її ефективності. Зазначена ситуація поступово виправляється завдяки імплементації Плану реалізації Стратегії кібербезпеки України. Зокрема, було введено в дію Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570)[18]. Суттєвим кроком в оптимізації координації стало прийняття Постанови КМУ від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінцеденти, кібератаки та кіберзагрози» [19], яка замінила попередню

Постанову КМУ від 4 квітня 2023 року № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі». Цією постановою затверджено низку процедурних регламентів, зокрема: Національний план реагування на кіберінцеденти, кібератаки та кіберзагрози (далі – Національний план); Критерії віднесення інформації про характер, технічні та інші деталі кіберінцеденту, кібератаки до інформації з обмеженим доступом, перелік підстав, порядок та мету розкриття такої інформації; Порядок публічного інформування або звітування про реагування на кіберінцеденти, кібератаки, усунення їх наслідків.

Національний план визначає загальні процедури реагування на кіберінциденти, кібератаки, кіберзагрози, а також механізм координації та взаємодії між суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та суб'єктами забезпечення кібербезпеки, їх роль в рамках функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози. Дія цього документу поширюється на основних суб'єктів національної системи кібербезпеки, суб'єктів національної системи реагування, органи державної влади, державні органи, органи місцевого самоврядування, операторів критичної інфраструктури, власників або розпорядників об'єктів критичної інформаційної інфраструктури, інших суб'єктів забезпечення кібербезпеки, які відповідно до законодавства залучені до виконання завдань в рамках функціонування національної системи реагування. Також набув чинності «Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності», затверджений постановою КМУ від 13 листопада 2025 року № 1471 (далі – Порядок) [20]. Зазначений Порядок визначає механізм взаємодії між національною командою реагування на кіберінцеденти, кібератаки, кіберзагрози (CERT-UA), галузевими та регіональними командами реагування на кіберінцеденти, кібератаки, кіберзагрози (CSIRT), а також правоохоронними органами (зокрема НП України та СБУ), розвідувальними, контррозвідувальними органами та суб'єктами оперативно-розшукової діяльності. Уповноваженим суб'єктом, який визначає порядок взаємодії суб'єктів національної системи реагування на кіберінцеденти, кібератаки, кіберзагрози та обміну інформації між ними визначена Адміністрація Держспецз'вязку.

Взаємодія суб'єктів національної системи реагування на кіберінцеденти, кібератаки, кіберзагрози з правоохоронними органами, контррозвідувальними органами, розвідувальними органами та суб'єктами оперативно-розшукової діяльності здійснюється у таких формах: 1) обмін інформацією про кіберінцеденти, кібератаки, кіберзагрози; 2) проведення спільних заходів під час реагування на кіберінциденти, кібератаки, кіберзагрози; 3) надання та отримання в установленому законодавством порядку доступу до технічних та інших деталей кіберінциденту чи кібератаки (відомостей про кіберінцидент чи кібератаку) для проведення слідчих (розшукових) дій, контррозвідувальних або оперативно-розшукових заходів; 4) функціонування міжвідомчих груп із реагування на кіберінциденти, кібератаки, кіберзагрози або кризову ситуацію у сфері кібербезпеки.

Виходячи з аналізу Порядку, суб'єкти реагування (CERT-UA та CSIRT) здійснюють обмін інформацією з НКЦК, а також правоохоронними органами, зокрема СБУ, НП, ДБР, НАБУ та БЕП.

Держспецзв'язку є державним органом, на який, серед іншого, покладено функції з формування та реалізації державної політики у сфері кіберзахисту та активної протидії агресії у кіберпросторі (ст.2 ЗУ «Про Державну службу спеціального зв'язку та захисту інформації України») [21]. Також цей орган здійснює: методичне керівництво та координацію діяльності державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форм власності з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-комунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах; розробку критеріїв і порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційно-комунікаційних системах; організацію та проведення оцінки стану захищеності державних інформаційних ресурсів, надання відповідних рекомендацій.

Організаційно-координаційна діяльність Держспецзв'язку реалізується через забезпечення функціонування Державного центру кіберзахисту та CERT-UA, впровадження організаційно-технічних моделей кіберзахисту, а також здійснення заходів із запобігання, виявлення та реагування

на інциденти у кіберпросторі. Профільний закон закріплює за Держспецзв'язку функцію координації діяльності об'єктів критичної інфраструктури з питань кіберзахисту, зокрема в умовах надзвичайного або воєнного стану, та покладає на відомство обов'язок із забезпечення роботи національної системи обміну інформацією про кіберінциденти, кібератаки й кіберзагрози

Служба безпеки України здійснює координацію діяльності суб'єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям. Своєю чергою, Міністерство закордонних справ забезпечує координацію діяльності щодо співпраці з міжнародними партнерами для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці.

Виходячи з приписів статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», CERT-UA виконує функції координатора з метою узгодженого розкриття вразливостей в інформаційно-комунікаційних системах, що містять державні ресурси або інформацію з обмеженим доступом, взаємодіючи з їх власниками та операторами критичної інфраструктури. Водночас галузеві, регіональні та приватні CSIRT здійснюють обмін даними у межах національної системи обміну інформацією, координують свою діяльність та інформують CERT-UA і Ситуаційний центр забезпечення кібербезпеки СБУ про вжиті заходи реагування.

Варто зауважити, що досі не в повному обсязі реалізовано визначене Стратегією 2021 року завдання щодо формування дієвої системи кібероборони, спроможної стримувати збройну агресію в кіберпросторі та надавати відсіч агресору. Зокрема, йдеться про створення кібервійськ у складі Міністерства оборони України та налагодження на постійній основі співпраці з європейською військовою мережею CERT. Водночас слід зазначити, що один з елементів цієї системи – MIL.CERT-UA – уже функціонує в інтересах оборонного відомства та Збройних Сил України. Цей спеціалізований підрозділ реагування на комп'ютерні інциденти у системі Міністерства оборони України спрямовує свою діяльність на забезпечення належного рівня кіберзахисту, своєчасне виявлення, аналіз і реагування на кіберінцеденти в інфомаційно-комунікативних системах міністерства [22].

Натомість створення Кіберсил Збройних Сил України перебуває на початковій стадії нормативного оформлення та закріплене лише на рівні проєкту закону «Про Кіберсили Збройних Сил України». В законопроекті питання координації діяльності розглядаються як один із ключових елементів функціонування. Передбачається інтеграція Кіберсил у систему військового управління ЗСУ з підпорядкуванням Міністерству оборони України та Генеральному штабу, що має забезпечити узгодження кібероперацій із загальновійськовими, інформаційними та розвідувальними заходами, а також централізоване планування дій у разі збройної агресії в кіберпросторі. Водночас законопроєкт закладає правові засади міжвідомчої координації Кіберсил з іншими суб'єктами сектору безпеки і оборони, зокрема Службою безпеки України, Держспецзв'язку, розвідувальними органами та системою CERT/CSIRT. Така координація спрямована на обмін інформацією про кіберзагрози, уникнення дублювання повноважень і формування єдиного підходу до реагування на кіберінциденти, а також створює підґрунтя для міжнародної взаємодії з військовими кіберструктурами держав-партнерів [23].

Висновки. Діяльність основних суб'єктів національної системи кібербезпеки спрямована на нормативно-правове та організаційне забезпечення ефективної взаємодії із силами оборони для спільного виконання завдань кібероборони, а також на розбудову моделі оперативного обміну інформацією про кіберзагрози. Засади такої координації, визначені Законом України «Про основні засади забезпечення кібербезпеки України» та деталізовані у підзаконних актах, характеризуються багаторівневістю та багатовекторністю. На загальнодержавному рівні координація (стратегічна) реалізується Президентом України через РНБО та НКЦК, який здійснює узгодження дій суб'єктів сектору безпеки і оборони та функціонування національної системи реагування. Своєю чергою, Кабінет Міністрів України формує та реалізує політику у сфері такої взаємодії через нормативно-правове регулювання, затвердження програмних документів та координацію діяльності системи органів виконавчої влади. Спеціальний рівень координації (функціональної, відомчої) реалізується безпосередньо керівниками підрозділів кіберзахисту в органах державної влади, що є власниками або розпорядниками систем, де обробляються державні інформаційні ресурси чи таємна інформація (як то Міністерство оборони, Національний банк, Міністерство юстиції). Координація на цьому рівні здійснюється через такі форми, як: встановлення галузевих стандартів безпеки, проведення внутрішніх аудитів захищеності та впровадження протоколів негайно інформування про кіберінцеденти. Така багаторівнева структура дозволяє поєднувати адміністративні,

правоохоронні та військові спроможності в єдину систему. Саме в межах цієї моделі подальше інституційне та функціональне вдосконалення органів реагування на кіберзагрози безпосередньо у Збройних Силах України є логічним завершенням розбудови системи. Це забезпечить перехід від загальної координації до високоефективного запобігання, своєчасного виявлення та нейтралізації кіберзагроз національній безпеці в специфічних умовах гібридної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Указ Президента України про введення воєнного стану в Україні № 64/2022 від 24 лютого 2022 р., затверджений Законом України № 2102/IX від 24.02.2022 р. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення 10.12.2025).
2. Указ Президента України про продовження строку дії воєнного стану в Україні № 793/2025 від 20.10.2025., затверджений Законом України № 4643/IX від 21.10.2025. URL: https://zakon.rada.gov.ua/laws/show/793/2025#n2 (дата звернення 11.12.2025).
3. Яворська Г.М. Гібрідна війна як дискурсивний конструкт. *Стратегічні комунікації*. 2016. № 4 (41). С. 41-48. URL: https://ippi.org.ua/sites/default/files/yavorskaya.pdf (дата звернення 08.12.2025).
4. Магда Є.В., Водотика Т.С. Гібридна війна як явище. Енциклопедія історії України: Додатковий том. – Кн. 1: А–Я / Редкол.: В.А. Смолій (голова) та ін. НАН України. Інститут історії України. К.: В-во «Наукова думка», 2021. 773 с. URL: http://www.history.org.ua/?termin=gibrydna_vijna (дата звернення 10.12.2025).
5. Stepanenko V. Shaping critical thinking as a factor of the local security in wartime conditions. *Prawo i bezpieczenstwo*. 2024. Vol. 3, No. 2. P. 45-52. DOI: https://doi.org/10.4467/29567610PIB.24.018.20781. URL: https://ejournals.eu/czasopismo/pb-ls/artykul/shaping-critical-thinking-as-a-factor-of-the-local-security-in-wartime-conditions (дата звернення 06.12.2025).
6. Litvinova D.How the Kremlin weaponized Russian history – and has used it to justify the war in Ukraine. Associated Press, 21 February 2024. URL: https://apnews.com/article/russia-ukraine-war-history-putin-propaganda-80cb70fff9820357eddb83170695bdbb (дата звернення 06.12.2025).
7. The Cognitive Battlefield of Hybrid Warfare. URL: https://www.natofoundation.org/food/the-cognitive-battlefield-of-hybrid-warfare/ (дата звернення 06.12.2025).
8. AI Frontiers: інновації, прориви, виклики. Підготовлено експертами Громадської організації «Центр аналізу та розробки ефективних політик» (ЦАРЕП) та Національного інституту стратегічних досліджень (НІСД). Жовтень 2025 року. 40 с. URL: https://www.rnbo.gov.ua/files/2025/NATIONAL_CYBER_SCC/Digest_10_2025/NISS_CADEP_Digest_October_2025.pdf (дата звернння 08.12.2025).
9. Beatrice Catena, Ondrej Ditrych, Nad'a Kovalčíková. Smoke and mirrors: Building EU resilience against manipulation through cognitive security. 7 October 2025. URL: https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive (дата звернення 06.12.2025).
10. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення 10.12.2025).
11. Тарасюк А.В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки.*2020. Том 31 (70). Ч. 2 № 2. С.119-124. DOIhttps://doi.org/10.32838/2707-0581/2020.2-2/23URL:https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf (дата звернення 08.12.2025).
12. Боровик А.В. Адміністративно-правовий механізм взаємодії суб'єктів сектору безпеки й оборони щодо забезпечення національної безпеки: питання теорії та практики : монографія / А.В. Боровик, А.Г. Вархов, Н.З. Деревянко. Одеса: Видавництво «Юридика», 2024. 186 с.
13. Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 7 червня 2016 року № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення 11.12.2025).

14. Сучасний тлумачний словник української мови: 100 000 слів / За заг. ред. д-ра філол. наук, проф. В.В. Дубічинського. Харків : ВД «ШКОЛА». 2008. 1008 с.
15. Литвинов О.М. Координація протидії злочинності. Велика українська кримінологічна енциклопедія. У 2 т. Т. 1: А-Л / Редкол.: В.В. Сокуренко, О.М. Бандурка та ін.; наук. ред. О.М. Литвинов. Харків: Факт, 2021. С. 725–727.
16. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII**.** URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 12.12.2015).
17. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 06.12.2025).
18. Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. URL: https://zakon.rada.gov.ua/rada/show/v0570519-23#Text (дата звернення 10.12.2015).
19. Постанова Кабінету Міністрів України «Деякі питання реагування на кіберінцеденти, кібератаки та кіберзагрози» від 26 листопада 2025 року № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-п#Text (дата звернення 10.12.2015).
20. Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності», затверджений Постановою Кабінету Міністрів України від 13 листопада 2025 року № 1471. URL: https://zakon.rada.gov.ua/laws/show/1471-2025-п#n8 (дата звернення 10.12.2015).
21. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 року № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення 10.12.2015).
22. Про MIL.CERT-UA. URL: https://mil-cert.gov.ua (дата звернення 12.12.2015).
23. Проект закону України «Про Кіберсили Збройних Сил України», зареєстрований 19.12.2024 р. № 12349. URL: blob: https://itd.rada.gov.ua/455bbdff-3ab9-4672-b1cf-f747ea3523c0 (дата звернення 14.12.2015).