УДК 327.5:911.3]:316.776.23] (02) DOI 10.59226/2786-6920.2.2025.28-40

ВЄДЄНЄЄВ ДМИТРО ВАЛЕРІЙОВИЧ
доктор історичних наук, професор,
професор кафедри історії,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0002-8929-9875

ОРГАНІЗАЦІЙНО-ФУНКЦІОНАЛЬНІ ТА НАУКОВО-КОНЦЕПТУАЛЬНІ ОСОБЛИВОСТІ СИСТЕМ КІБЕРНЕТИЧНОГО ПРОТИБОРСТВА ПРОВІДНИХ КРАЇН СВІТУ (ПЕРША ЧВЕРТЬ XXI СТ.)

На основі праць сучасних українських і зарубіжних фахівців – дослідників проблем інформаційно-кібернетичного протиборства – розглянуто становлення систем кібернетичного протиборства провідних країн світу. Окрему увагу приділено структурі й особливостям діяльності органів кіберборотьби Китая та російської федерації. Висвітлено кібермережевий домен російсько-української війни.

Сформульовано пропозиції щодо тематики подальших досліджень і можливого застосування зарубіжного досвіду в інтересах удосконалення національної системи інформаційно-кібернетичної безпеки.

Ключові слова: *неконвенційна стратегія; інформаційне протиборство; кібернетичні війни; кібершпигунство; інформаційна безпека.*

Постановка проблеми. Сучасні теоретики військової справи та спеціальної діяльності солідарні у визнанні того, що інформаційне протиборство (ІП) незворотно стало одним із ключових компонентів військової стратегії і розвідувально-підривної діяльності. Провідні країни світу пріоритетного значення надають модернізації та розробленню нових стратегій, технологій, сил і засобів інформаційно-психологічного впливу, програмно-технічних засобів заподіяння шкоди комп'ютерним і телекомунікаційним системам. Як переконує досвід сучасних воєнних конфліктів, ІП стало однією з основних форм досягнення стратегічних цілей [1, 2, 3]. Утвердилося й поняття «кібервійни» як «організоване протиборство у цифровому просторі, принаймні однією зі сторін якого є держава, що здійснюється з політичною метою та супроводжується руйнуванням інфраструктури, заподіянням іншої моральної та матеріальної шкоди суспільству» [4].

Загрозливість зовнішніх деструктивних впливів (атак) для кібернетичної та управлінської сфер України розкривається у «Стратегії кібербезпеки України», ухваленій 6 серпня 2021 р. Цей документ наголошує на вивченні іноземного досвіду забезпечення кібербезпеки, що зумовлюється необхідністю подолання Україною відставання у цій сфері від провідних держав світу [5].

Актуальності дослідженню порушеної у статті проблеми додає важливість урахування іноземного досвіду кіберпротиборства й зовнішніх загроз інформаційно-мережевій сфері національної безпеки України у розбудові й діяльності створеного у лютому 2020 р. Командування Військ зв'язку та кібернетичної безпеки Збройних Сил України (ЗСУ), що відповідно до Закону України «Про основи національного спротиву» з 1 січня 2022 р. набули статусу окремого роду військ [6].

Перспективним предметом дослідження став кібернетичний домен російсько-української війни, що кваліфікується дослідниками як «перша кібернетична війна» проти України. Згаданий концепт, зокрема, висувався на пленарному засіданні «Вплив першої в світі кібервійни на стан національної безпеки України» у межах Всеукраїнської науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави» (березень 2024 р.) [4].

Аналіз останніх досліджень і публікацій. Вивчення особливостей актуального зарубіжного досвіду ведення протиборства в електронно-мережевій сфері нині є одним із напрямів дослідження в Україні явища кібервійни та кібербезпеки. За даними МОН України (2024 р.) 54 заклади вищої освіти проводили підготовку кадрів для сфери інформаційної безпеки, здійснювали профільні дослідження [4]. Із 2023 р. при Адміністрації Державної служби спеціального зв'язку та захисту інформації України відкрито Галузеву раду з організації та координації розроблення професійних стандартів та професійних кваліфікацій у галузі інформаційних технологій, кібербезпеки й захисту інформації. Із 2021 р. і до 2024 р. кількість професій у галузі кібербезпеки зросла з 2 до 27 [4].

Слід зазначити, що у науково-дослідному сегменті оборонно-безпекової сфери України сформувалися наукова школа й відповідні дослідницькі напрями з проблем теорії і практики кібернетичної безпеки держави. У її діяльності помітне місце відводиться вивченню зарубіжного досвіду організації структур кіберборотьби, форм і методів їх діяльності. Відповідні профільні дослідження активно ведуться у Житомирському військовому інституті імені С. П. Корольова, Військовому інституті телекомунікацій та інформатизації імені Героїв Крут, Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського». Працює центр кібербезпеки, наукова лабораторія з протидії кіберзагрозам у Навчально-науковому інституті інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України**.** Здійснюються профільні дослідження інформаційно-кібернетичної безпеки співробітниками Центру безпекових досліджень Національного інституту стратегічних досліджень. Центром наукових пошуків у галузі кіберпротиборства став Національний університет оборони України (НУОУ), у складі якого з 2023 р. працює Інститут інформаційно-комунікаційних технологій та кібероборони. Регулярно проводяться профільні наукові заходи [4, 7].

Зосереджуючись на розгляді наявних наукових розробок, доцільно згадати низку досліджень вчених силових наукових центрів, у яких зовнішні загрози кібербезпеці України вивчались у межах комплексного розгляду проблемних аспектів кібероборони, інфраструктури органів кіберзахисту України та шляхів її реформування, оцінювання місця й ролі кіберзахисту у Збройних Силах, ступеня захищеності критично важливих об'єктів від кібератак, розроблення практичних рекомендацій до проєкту «Стратегії кібероборони України» і щодо розвитку об'єднаних військ (сил) кібероборони [8–11].

Окремим напрямом досліджень стало вивчення кіберпротиборства як складника російсько-української війни, а саме розвитку структур кіберборотьби рф. Дослідниками узагальнювався досвід протистояння у кіберпросторі з початку війни, зокрема вивчалися статистичні дані здійснених кібератак, розкривалася структура обох сторін кіберпротистояння, розглядалися нові способи застосування кібервпливів та зміни у цілях кібероперацій залежно від ситуації на основному театрі воєнних дій тощо [12–21]. Відтак у межах цього наукового напряму відбувалося поглиблене дослідження особливостей системи установ кіберборотьби рф, форм і методів їхніх агресивних дій у мережевому просторі України.

Окремо варто зауважити про науково-практичну значущість серійних видань із вивчення досвіду бойового застосування військ зв'язку та кібербезпеки, підготовлених Головним командуванням Військ зв'язку та кібербезпеки ЗСУ і Головним управлінням зв'язку та кібербезпеки Генштабу ЗСУ. Аналітична робота з підготовки подібних видань зосереджувалася у Групі узагальнення досвіду управління підготовки штабу Командування військ зв'язку та кібербезпеки ЗСУ [22, 23].

Інститут інформаційно-комунікаційних технологій та кібероборони НУОУ підготував серію збірників інформаційно-аналітичних матеріалів щодо бойового досвіду кібероборони як чинника повномасштабних бойових дій (частина 3 видання охоплювала кінець 2022 – середину 2023 рр.) [24]. У виданні систематизовано корисний для профільних досліджень матеріал, зокрема стосовно характеру і статистики кібератак противника на об'єкти критичної інфраструктури України. Інститут також підготував низку збірників інформаційно-аналітичних матеріалів щодо актуального досвіду забезпечення інформаційної безпеки у період повномасштабної війни [25].

Українськими дослідниками на довгостроковій основі ведеться вивчення зарубіжного досвіду інформаційної боротьби [26]. Однак аналіз стану наукового розроблення порушеної проблеми дає змогу стверджувати про необхідність підготовки окремих досліджень із поглибленого вивчення організаційно-функціонального устрою, тенденцій розвитку й поточних завдань, форм і методів діяльності сил кіберборотьби провідних іноземних держав задля подальшого розвитку й удосконалювання діяльності органів і підрозділів кібероборони військових формувань і спеціальних служб України, а також своєчасного виявлення загроз кібернетичній сфері держави й запобігання їм.

Мета статті – розкрити організаційно-функціональні й концептуальні особливості становлення новітніх систем кібернетичного протиборства провідних країн світу для сформулювання певних рекомендацій щодо вдосконалення забезпечення системи кібербезпеки України.

Виклад основного матеріалу. В умовах «дистанційних» війн і неконвенційного протиборства серед ключових напрямів розвитку засобів інформаційно-психологічного впливу ствердилися, зокрема, такі: нарощування можливостей використання глобальної комп'ютерної мережі Інтернет і мереж стільникового зв'язку для поширення пропагандистських матеріалів; продукування спеціального програмного забезпечення для формування на базі мобільних телефонів альтернативних самоорганізованих мереж зв'язку без задіяння базових станцій в обхід офіційних провайдерів; імітація діяльності хибних груп користувачів у соціальних мережах з урахуванням мовних, культурних та географічних особливостей регіонів світу (етносів, субкультур тощо); розгортання на основі технологій Wi-Fi та Bluetooth бездротових мереж, непідконтрольних державним органам; широке використання штучного інтелекту [27, 28].

Перша чверть XXI ст. відзначилася появою у зарубіжних концептуальних і нормативно-правових документах таких сталих термінів, як «кібер-війна» (cyber war), «бойові дії у кіберпросторі» (cyber warfare), «кібератака» (cyber attack) тощо, під якими розумілося ведення військового протиборства і спеціальних операцій у кіберпросторі. Війни (підривні дії) у кіберпросторі стали новим різновидом міждержавного протиборства. Протиборство у кіберпросторі ведеться й у більш широких межах інформаційних операцій, розвідувально-підривних кампаній тощо. На думку американських фахівців, кіберпростір (cyberspace) перетворився на глобальну сферу у структурі інформаційного простору і складається із взаємопов'язаної мережі інформаційних технологічних інфраструктур, включно з глобальною інформаційною мережею Інтернет, телекомунікаційними мережами, комп'ютерними системами, вбудованими в них процесорами й контролерами.

Воєнно-політичним керівництвом провідних країн світу протиборство у кіберпросторі розглядається як один із вирішальних чинників впливу на міжнародні відносини, досягнення власних інтересів. Для цього створюються багаторівневі управлінсько-функціональні системи протиборства у кіберпросторі, відповідні національні й міждержавні (блокові) органи управління (командування, центри тощо), так звані «кібервійська» та відповідні органи у структурі спецслужб, розробляються сили й засоби кібервійн.

Саме мережа Інтернет стала центральним театром воєнних дій неконтрольованої деструктивної інформаційної експансії та полігоном для створення новітніх засобів інформаційної боротьби. Поширеними деструктивними прийомами стали інформаційні вкидання, неправдиві публікації, інформаційне «зараження», перекручування фактів, виривання з контексту, підміна понять тощо. Новітні засоби інформаційного протиборства набули мережевого характеру і паразитують на соціальних мережах, месенджерах, форумах та платформах. Сформувався високотехнологічний інструментарій кібернетичної війни [29].

Визнання кіберпростору сферою ведення бойових дій і спеціальних операцій зумовило активізацію діяльності органів безпеки та спеціальних служб у кіберпросторі. Стратегічна концепція оборони та безпеки НАТО (від 19 листопада 2010 р.) визначила завдання координації національних можливостей кіберзахисту й нарощування можливостей щодо захисту й відновлення національної інфраструктури після руйнівних кібератак. На підставі цієї концепції розробляється єдиний документ «План кібербезпеки», головним завданням якого визначено протистояння російській кіберзагрозі. Документ доповнено

також «Планом дій з використання кіберпростору як оперативного середовища» для протистояння загрозам із боку ворожих держав, терористичних та екстремістських організацій, нападам на стратегічні комунікації членів Альянсу. У грудні 2020 р. Європейський Союз репрезентував нову Стратегію кібербезпеки, що передбачає підвищення стійкості секторів критичної інфраструктури та протидії кібератакам іззовні.

У провідних країнах світу магістральним трендом є створення сукупності відомств, установ (органів) із кіберзахисту й кіберпротиборства. Сили кібероборони зазвичай отримують статус окремого виду національних збройних сил, об'єднуючи підрозділи радіоелектронної розвідки, радіоелектронної боротьби, інформаційно-психологічних операцій, криптографічного забезпечення і криптологічної підтримки, геоінформаційного забезпечення, захисту інформації в інформаційно-телекомунікаційних системах тощо. Нині понад 60 країн мають власні війська (органи) для ведення кібернетичної боротьби, що охоплює комплекс заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані інформаційно-технологічні системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів шляхом використання спеціально розроблених програмно-апаратних засобів, а також проведення системи спеціалізованих навчань. Так, у США створено Кібернетичне командування США (USCYBERCOM). Інші країни (Нідерланди, Німеччина, Іспанія, Південна Корея та Японія) так само запровадили кібернетичні командування (центри, підрозділи) [13].

Серед спеціалізованих органів кібербезпеки можна назвати Агенство з питань кібербезпеки та безпеки інфраструктури (CISA) Міністерства національної безпеки США, Національний центр кібербезпеки (NCSC) Великої Британії, Канадський центр кібербезпеки, Національний центр з кібербезпеки (Республіка Польща), Національне управління кібернетичної та інформаційної безпеки Чеської Республіки, Національний центр з кібербезпеки (Литва). У низці держав подібні органи набувають характеру окремої організаційної спільноти. Так, у Німеччині функціонують Федеральне відомство з безпеки у сфері інформаційних технологій, Війська кібернетичного й інформаційного простору Бундесверу (збройних сил), Центр кібероборони, Комп'ютерна група реагування на надзвичайні ситуації. У серпні 2020 р. до них долучилось Агентство інновацій у сфері кібербезпеки, яке спільно створили федеральні відомства оборони і внутрішніх справ [30, 31].

Світовим трендом безпекової політики стає посилення державного регулювання (зокрема неафішоване втручання спеціальних служб і правоохоронних органів) у кіберсферу, налагодження державно-приватного партнерства у сфері кібербезпеки [32]. Ще у червні 2013 р. «Washington Post» оприлюднила результати журналістського розслідування щодо засекреченої програми співробітництва безпекових структур США, передусім відомства радіоелектронної розвідки Агентства національної безпеки (АНБ), провідних приватних компаній, що працюють на світовому інформаційному ринку (Microsoft, Yahoo, Google, Facebook, PalTalk та ін.). З'ясувалося, що передбачалася передача спецслужбам даних, які стосувалися електронної пошти, будь-яких чатів (текстових і відео), завантажених користувачами фото, відеоматеріалів і взагалі будь-яких даних із серверів приватних компаній. Пізніше представники АНБ визнали існування такої програми [33].

Зростає питома вага кібероперацій в арсеналі радикальних і терористичних угруповань. Відоме палестинське угруповання ХАМАС спільно з хакерськими групами інших арабських держав лише за квітень 2021 р. збільшило у 5 разів кількість кібератак (до 150 тис. щоденно) на об'єкти Міністерства оборони, Міністерства зовнішніх справ та інші державні відомства Ізраїля. Відповідно, силове припинення кіберпідривних дій радикалів стало складником антитерористичної операції Ізраїля «Страж стін» у секторі Газа (2021 р.). Тоді було проведено міжвідомчу операцію з участю Ізраїльської національної дирекції з кіберзахисту (INCD), підрозділу «8200» (радіорозвідка та радіоелектронна боротьба), Управління військової розвідки (АМАН), кіберпідрозділів МО, Служби зовнішньої розвідки МОССАД, Загальної служби безпеки (ШАБАК). Удалося знищити понад 10 штабів кіберпідрозділів ХАМАС, начальника кібервійськ і кіберштаб ХАМАС [30].

Кіберпротиборство ствердилось як інноваційний складник новітнього воєнного мистецтва, зокрема концепції багатосферної операції (БСО). Ухвалено такі настановні документи, як «Концепція застосування у багатосферних операціях формувань СВ США від бригади і вище (2025–2045)», «Концепція багатодоменної операції», «Багатосферне бойовище: еволюція спільних дій різних видів збройних сил в XXI столітті (2025–2040)», «Сухопутні війська США в багатосферних операціях – 2028», а також дослідження Центру передового досвіду НАТО з питань кібербезпеки «Кіберпотенціал і багатодоменні операції в умовах конфлікту високої інтенсивності 2030». Багатосферна операція визначалась основною формою ведення воєнних дій, тобто погоджене між собою за часом, місцем і цілями застосування об'єднаних сил США і коаліційних угруповань союзників у наземній, повітряній, морській операціях, а також у космічному й кібернетичному просторах. В оперативно-стратегічній ланці штабів міжвідомчих угруповань передбачалося формування органу управління інформаційними процесами та діями у кіберпросторі. Проведення БСО планувалося силами міжвидових або коаліційних угруповань у всіх операційних середовищах одночасно, серед яких американські настановні документи називали протиборство у кіберпросторі (у лютому 2003 р. «Національна стратегія із забезпечення безпеки кіберпростору» запровадила орган управління кіберсилами – Об'єднане кіберкомандування ЗС США, а у 2011 р. була затверджена «Міжнародна стратегія дій США в кіберпросторі» – International Strategy for Cyberspace). Багатодоменні сили (БДС) розумілись як сухопутні угруповання, здатні у мережевоцентричний спосіб координувати свої дії з авіацією, флотом, космічними угрупованнями та кіберпідрозділами, обминаючи при цьому спільний штаб [34, 35].

Останніми роками у США формуються багатодоменні оперативні групи (MDTF – Multi-Domain Task Forces), до яких входять сухопутні, військово-повітряні, військово-морські сили з далекобійними високоточними системами озброєнь, об'єднані у наступальну платформу. На рівні армійських корпусів планується створити групи багатосферних засобів (MDEC). Так, на навчаннях «Warfighter 25-02» (листопад-грудень 2024 р.) до 1-го армійського корпусу США включили MDEC у складі підрозділів ССО, сухопутних, військово-повітряних сил, а також 11-го кібербатальйона, 12-го батальйона психологічних операцій, представників 56-ї групи інформаційних операцій [36].

У Німеччині 16–17 липня 2025 р. відбулася перша спеціалізована конференція НАТО, організована Командуванням армії США в Європі, в якій взяли участь понад 1000 осіб (політики і промисловці включно). Однією з головних тем стали багатосферні операції (multi-domain operations, MDO) з охопленням кібер- та інформаційного простору. Зокрема йшлося про проведення новоствореним 56-м командуванням багатосферних операцій у Європі відповідних навчань Dynamic Front із застосування єдиного «бойового інтернету» (kill web). Зазначалося, що операції типу MDO стають новою воєнною філософією НАТО, а війна в Україні саме й точиться у кількох вимірах, кібер- та інформаційному просторах. Так само розглядався й досвід кібероперацій і застосування штучного інтелекту [37].

Доцільно зауважити про бурхливий розвиток мережі сил кіберпротиборства у Китаї. Центральну комісію з мережевої безпеки та інформатизації компартії Китаю (координаційний орган кібербезпеки) очолює особисто голова КНР Сі Цзіньпінь. До робочих органів комісії належать: Управління у справах кіберпростору КНР (провідний орган державного регулювання й координації роботи у сфері інформаційно-кібернетичної безпеки), Центр кризового управління у сфері кібербезпеки і Центр з виявлення нездорової та незаконної інформації. «Бюро 61419» (орган кібернетичної боротьби) Сил стратегічної підтримки Народно-визвольної армії Китаю (НВАК) взаємодіє з мережею хакерських угруповань. Прикладом залучення підконтрольних хакерських груп для масштабних атак є кібернапад на військові підприємства та Космічне агентство Японії. Створюється периферійна мережа центрів кіберборотьби КНР. Зокрема, у Папуа-Новій Гвінеї китайський телекомунікаційний гігант «Huawei» побудував центр оброблення перехоплених даних державної важливості з відповідних установ Австралії. Окремо у НВАК існують Сили кібернетичної підтримки.

Бюро мережевих систем Сил стратегічної підтримки НВАК відповідає за забезпечення кібербезпеки. Йому підпорядковано спеціалізовані центри з роботи в інформаційних мережах противника та захисту власних інформаційних систем. Структура відповідає за забезпечення кібербезпеки, має підрозділи комп'ютерної розвідки й контррозвідки, з проведення електронно-вірусних атак, антивірусного захисту. До Управління зв'язку Генштабу НВАК належить Ханкоуський навчальний центр – головна навчальна база (полігон) для відпрацювання форм і способів протиборства у комп'ютерних мережах. Наприкінці липня 2025 р. у КНР офіційно оголошено про створення нового роду військ НВАК – Сил інформаційної підтримки, що перебере на себе функцію кіберборотьби, замість Сил стратегічної підтримки [37].

У Міністерстві державної безпеки Китаю (МДБ) діє 13-те управління (Центр оцінювання інформаційної безпеки КНР), відповідальне за безпеку систем інформації державних відомств (окрім збройних сил, де кібербезпекою опікуються власні структури й військова контррозвідка). Контррозвідувальні підрозділи здійснюють контроль за користувачами всесвітніх комп'ютерних мереж. До підрозділів Міністерства громадської безпеки з 2015 р. належить «мережева поліція», що має територіальні підрозділи. У цьому відомстві діє низка підрозділів, інститутів і лабораторій, де розробляються комп'ютерні віруси і «троянські» програми [30, 31].

У вересні 2025 р. у провідних країнах Заходу розгорнулася масштабна інформаційна кампанія стосовно діяльності хакерської групи Salt Typhoon, яку традиційно пов'язують із Китаєм. Агентство національної безпеки США та ФБР стверджували, що діяльність хакерів стала «найбільшою за останні роки операцією з кібершпигунства», вона зачепила понад 200 установ у 80 державах, включно з державними органами й відомими політиками. У кібершпигунстві та сприянні Salt Typhoon звинуватили китайські компанії Sichuan Juxinhe, Beijing Huanyu Tianqiong и Sichuan Zhixin Ruijie, які оголосили прикриттям діяльності МДБ КНР і НВАК [39].

Українські дослідники, характеризуючи інформаційно-когнітивне протиборство як складник триваючої російсько-української війни, звертають увагу на те, що рф використовує широкий спектр методів інформаційного впливу, серед яких: кібератаки, спрямовані на руйнування інформаційної інфраструктури та витік даних; фейкові новини й дезінформаційні кампанії; активна діяльність бот-мереж у соціальних мережах, що поширюють проросійські наративи тощо [14–18].

У російській федерації у 2014 р. створено війська інформаційних операцій збройних сил рф, а при генштабі збройних сил рф запроваджено кібернетичне командування. Планування і управління інформаційних операцій здійснює управління інформаційного протиборства («Управління 12-біс», або 12-те управління) головного управління генштабу збройних сил рф. Активно діє 85-й центр спеціального призначення (в/ч 26165) ГРУ, який вважають одним із центрів розроблення шкідливих програм (за визначенням АНБ США – «Drovorub»). Американська сторона звинувачує Головний центр спеціальних технологій ГРУ у співпраці з групою хакерів «Sandworw Team», винних у кібератаці на енергетичну систему України. Організацією психологічних операцій у кіберпросторі займається 72-й центр спеціальної служби (в/ч 54777) [30, 40, 41].

За оцінкою Міністерства оборони Великої Британії потенціал росії з ведення операцій у «сірій зоні» (на одному з традиційних театрів гібридної війни) має достатньо сил і засобів кібервійни, водночас у кілька разів зросла чисельність підрозділів російських спеціальних служб, що діють у кіберпросторі. Агентство з питань кібербезпеки та безпеки інфраструктури (CISA) Міністерства національної безпеки США спільно з Агентством національної безпеки (відомством радіоелектронної розвідки) США, ФБР та Національним центром кібербезпеки Великої Британії 7 травня 2021 р. оприлюднило рекомендації з питань кібербезпеки, тактики і прийомів служби зовнішньої розвідки росії «Операційні процедури кіберсуб'єктів, що асоціюються із СЗР». CISA залучило додатково 200 фахівців із кіберпротиборства [30, 40, 41, 42].

Згідно зі звітом компанії Microsoft щодо хакерських атак 2020–2021 рр. до вчинення 58 % атак причетна росія. При цьому більшість хакерських атак спрямовувалася проти США (46 %), Україна посідала друге місце (19 %). Велика Британія – 9 %, на Бельгію, Японію, Німеччину сукупно припали 3 % атак [43].

Від початку повномасштабної війни кіберфахівцями Служби безпеки України (СБУ) виявлено й нейтралізовано понад 3,5 тис. кібератак на електронні ресурси об'єктів критичної інфраструктури та органів державної влади. За інформацією СБУ більшість кібератак з боку рф спрямовувалися на дестабілізацію роботи: підприємств транспортної сфери – 37 %; органів центральної влади – 31 %; підприємств енергетичної сфери – 16 %; економічної сфери – 13 %; суб'єктів, що надають соціальні послуги населенню, – 3 % [12].

Доцільно зауважити про негативний синергетичний ефект, який у поєднанні з кібератаками породжує дедалі більше застосування штучного інтелекту (ШІ). На думку фахівців, подібний синтез радикально змінить характер підривних дій в інформаційному середовищі, відкриє простір для брутального спотворення реальності й витонченої маніпуляції людською свідомістю у нечуваних масштабах. На переконання дослідників, поєднання систем, побудованих на основі технології штучного інтелекту, у найближчому майбутньому може призвести до генерування псевдореальності, що виведе інформаційно-психологічні операції на якісно новий рівень, ускладнить їх виявлення [44, 45].

Зарубіжні спецслужби вивчають стан кіберактивності рф проти України у ході російсько-української війни. Уже у квітні 2022 р. кібербезпекові служби Ради ЄС, США, Великої Британії, Канади, Австралії та Нової Зеландії оприлюднили спільну доповідь «Російські державні та кримінальні загрози критичній інфраструктурі». Тоді ж команди з кіберрозвідки і кібернетичної криміналістики й реагування готували щотижневі інформативні хронологічні звіти про розвиток ситуації у кіберпросторі. Ситуацію у кіберсфері обговорили 10–11 травня 2022 р. на міжнародній конференції CYBERUK 2022 у Ньюпорті – головному щорічному заході з проблем кібербезпеки. Його учасники констатували, що «Українська держава виявила значну стійкість у збереженні комунікативної відкритості». Україна продемонструвала «приголомшливу кіберстійкість» під час конфлікту, хоча нараховувалося щонайменше вісім унікальних різновидів програм-вайперів, за допомогою яких було атаковано активи України. Проте українська сторона «успішно відреагувала, утримала й перебудувала свої системи» на тлі безперервних російських кібератак від 2014 р. [40].

Висновки й перспективи подальших досліджень. Конструювання агресивних інформаційно-кібернетичних просторів набуло таких масштабів і наслідків, що розглядається фахівцями як новий вимір геополітичного суперництва та географічної експансії. Різко знизилася захищеність національних кіберпросторів. Україна потерпає не тільки від «традиційних» кіберзлочинів, а й від кваліфікованих кібератак, що спонукає до визначення на загальнодержавному рівні концептуального бачення глобальних процесів, пов'язаних із розвитком кіберпростору, визначення місця в них нашої держави та перспектив державного буття в умовах «нового цифрового світопорядку». Постає стратегічна необхідність концептуального осмислення нової кібербезпекової реальності задля розбудови ефективної національної системи кібербезпеки.

Вивчення зарубіжного досвіду демонструє, що в забезпеченні інформаційної безпеки держави як засоби нормативного регулювання й захисту всіх сфер соціального життя важливу роль відіграють правові інститути: цивільне, адміністративне, кримінальне, спеціалізоване інформаційне право. У провідних країнах світу тривалий час формувалося національне законодавство з інформаційної політики та інформаційної безпеки, на чому ґрунтувалися відповідні державно-правові системи взаємопов'язаних державних органів, організацій, установ із провадження сукупності норм і принципів права, покликаних регулювати суспільні відносини в інформаційній сфері.

В організаційно-функціональному аспекті зарубіжний досвід доводить необхідність як системи державних відомств (органів) із визначеними профільними «наступальними» й інформаційно-безпековими функціями, так і провідного координаційного відомства у цій сфері. Корисними вбачаються висновки з аналізу розбудови загальнодержавної системи інформаційного протиборства й безпеки у КНР. Зазначена система раціонально охоплює профільні координаційно-керівні органи вищих органів державного управління (що забезпечує належну міжвідомчу мобілізацію сил і ресурсів й науково-освітні включно); відомчі профільні вертикалі управління (передусім у збройних силах, спецслужбах, у дипломатичному відомстві). По суті, створена міжвідомча система органів

інформаційного протиборства. Особлива увага приділяється контррозвідувальному, режимному й технічному захисту мереж інформації та інформаційно-когнітивної сфери суспільства загалом.

Вивчення іноземного досвіду дає змогу запропонувати певні рекомендації з удосконалення вітчизняної системи забезпечення кібербезпеки та кіберпротиборства:

– удосконалення міжвідомчої взаємодії у сфері протидії загрозам кібербезпеці на загальнодержавному рівні й у межах складових сектору безпеки і оборони України;

– активізація міжнародного співробітництва, зокрема серед партнерських спецслужб і профільних установ, із формування колективної системи кібербезпеки, відвернення кібератак;

– забезпечення випереджувального розвідувального вивчення діяльності іноземних структур із підривних дій у кіберпросторі;

– створення за рахунок агентурно-оперативних можливостей розвідувальних органів України відповідних позицій впливу в середовищі іноземних структур із підривних дій у кіберпросторі, зокрема «неурядові» хакерські структури;

– посилення роботи щодо забезпечення кібергігієни і кіберграмотності серед персоналу органів державного управління, критичної інфраструктури, фінансово-економічної сфери тощо.

Щодо подальшого вивчення досвіду зарубіжних структур (національних систем) кіберборотьби та кібербезпеки вбачається доцільним:

– поглиблено досліджувати доктринальні документи, досвід організаційно-штатної будови, форми й методи нейтралізації загроз у кіберсфері;

– окремо здіснювати аналіз механізмів використання ними «неурядових» хакерських угруповань;

– забезпечувати оперативне застосування зарубіжних інновацій у процесі професійної підготовки й підвищення кваліфікації співробітників органів інформаційно-кібернетичної безпеки й протиборства України.

Перелік джерел посилання

1. Війни інформаційної епохи: міждисциплінарний дискурс : монографія / за ред. В. А. Кротюка. Харків : Федорко М. Ю., 2021. 558 с.

2. Вєдєнєєв Д., Семенюк О. Розвиток концептуальних поглядів на інформаційне протиборство як складову неконвенційних (гібридних) війн і конфліктів (2013–2023 рр.) : монографія. Одеса : Олді+, 2024. 238 с.

3. Інформаційно-психологічна боротьба у воєнній сфері : монографія / Г. В. Пєвцов та ін. Харків : Рожко С. Г., 2017. 276 с.

4. Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів XV всеукр. наук.-практ. конф. (м. Київ, 27 берез. 2024). Київ : НА СБУ, 2024. Ч. І. Секц. 1. 288 с.

5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 06.08.2021 р. № 447/2021. URL: https://surl.li/ogmglw (дата звернення: 21.06.2025).

6. В ЗСУ формують два нові командування. *Український мілітарний портал.* URL: https://surl.li/mmkkum (дата звернення: 10.05.2025).

7. Досвід планування та бойового застосування військових частин (підрозділів) військ зв'язку та кібербезпеки Збройних Сил України. *Проблемні питання та шляхи їх вирішення*: зб. матеріалів наук.-практ. семінару кафедри комунікаційних технологій та кіберзахисту (м. Київ, 23 берез. 2023 р.). Київ : НУОУ, 2023. 160 с.

8. Терновий О. В., Шкуренко О. М., Міненко Л. М. Проблемні аспекти кібероборони: місце та роль кіберзахисту в Збройних Силах України. *Сучасні інформаційні технології у сфері безпеки і оборони.* 2023. № 1. С. 23–31.

9. Живило Є. О., Докіль В. М. Модель методики оцінювання спроможностей військ зв'язку та кібербезпеки Збройних Сил України щодо виконання завдань з відбиття воєнної агресії в кіберпросторі. *Сучасні інформаційні технології у сфері безпеки і оборони.* 2023. № 1. С. 32–40.

10. Мурасов Р., Мельник Я. Оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України. *Сучасні інформаційні технології у сфері безпеки і оборони.* 2023. № 1. С. 41–44.

11. Шиповський В. В. Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури. *Захист інформації.* 2023. Т. 25. № 1. С. 37–45.

12. Забезпечення інформаційної та кібербезпеки в умовах військової агресії РФ проти України: аналітичний огляд / Л. М. Стрельбицька, М. П. Стрельбицький, М. Л. Пальчик. Київ : НА СБУ, 2022. 56 с.

13. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування : монографія / І. В. Гора та ін.; за заг. ред. В. А. Колесника. Київ : НА СБУ, 2023. 512 с.

14. Машталір В. В., Шиповський В. В. Аналіз подій у кіберпросторі у процесі російсько-української війни 2022 року: висновки, рекомендації, засвоєні уроки. *Наука і оборона.* 2023. № 4. С.48–56.

15. Кириченко Ю. В., Сергієнко Т. І., Сластін В. О. Інформаційні війни як інструмент гібридної агресії: український досвід. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2025. № 1. С. 89–95.

16. Гребньов Г. Інформаційний аспект гібридної війни росії проти України. *Український інформаційний простір*. 2023. № 1. С. 107–118.

17. Кресіна І. О. Особливості застосування країною-агресором інформаційних технологій у гібридній війні. *Держава і право*. *Політичні науки.* 2018. Вип. 81. С. 27–41.

18. Твердохліб Ю. М. Інформаційно-психологічні операції у російсько-українській гібридній війні : дис. … канд. політ. наук. 23.00.04. Чернівці, 2019. 220 с.

19. Шерешкова І. І., Клунник М. С. Потенціал використання штучного інтелекту в інформаційно-психологічних операціях рф. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матеріалів XV всеукр. наук.-практ. конф. (м. Київ, 27 берез. 2024). Київ : НА СБУ, 2024. Ч. І. Секц. 1. С. 265–266.

20. Актуальні питання захисту національної державності в сучасних умовах : зб. матеріалів круглого столу (м. Київ, 28 лип. 2023 р.) : у 2 ч. Ч. 1 / упоряд.: А. А. Гончаренко та ін. Київ : НА СБУ, 2023. 100 с.

21. Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридної війни : тези доп. наук.-практ. конф. (м. Житомир, 24–25 жовт. 2019 р.). Житомир : ЖВІ імені С. П. Корольова, 2019. 432 с.

22. Інформаційний бюлетень вивчення бойового досвіду застосування військ зв'язку та кібербезпеки Збройних Сил України у російсько-українській війні 2022–2023 років. Київ, 2023. 52 с.

23. Інформаційний бюлетень вивчення бойового досвіду застосування військ зв'язку та кібербезпеки Збройних Сил України у російсько-українській війні 2022–2023 років. Лютий 2023 р. Київ, 2023. 79 с.

24. Бойовий досвід з питань кібероборони, отриманий під час російсько-української війни. Ч. 3. (листопад 2022 – червень 2023 року) : зб. інформ.-аналіт. матеріалів / уклад.: В. Машталір, О. Пермяков, С. Микусь, Н. Королюк. Київ : НУОУ, 2023. 218 с.

25. Бойовий досвід з питань інформаційної безпеки, отриманий під час російсько-української війни. Ч. 2 (березень 2022 – лютий 2023 року) : зб. інформ.-аналіт. матеріалів / уклад.: В. Машталір, С. Микусь, М. Авраменко, Д. Авраменко. Київ : НУОУ, 2023. 464 с.

26. Малик Я. Й., Береза О. І. Забезпечення інформаційної безпеки України у контексті світового досвіду. *Ефективність державного управління*. 2012. Вип. 32. С. 20–27.

27. Рущенко І. П., Зубар Н. В. Війни інформації. *Оборонний вісник.* 2017. № 8. С. 4–9.

28. Сніцаренко П. М. Інформаційна операція Збройних Сил України як інтегруюча форма воєнних дій в інформаційному просторі. *Наука і оборона.* 2020. № 1. С. 37–42.

29. Яскевич А. Інтернет як нове середовище сугестивного маніпулятивного впливу. *Посилення спроможностей СБ України та взаємодія зі складовими сектору безпеки і оборони* : зб. матеріалів міжвідомч. наук.-практ. конф. (м. Київ, 24 верес. 2024 р.). Київ : НА СБУ, 2024. Ч. 1. С. 265–267.

30. Інформаційна довідка щодо актуальних кіберзагроз (атак) в мережі Інтернет та дій провідних країн світу у сфері кібербезпеки за серпень 2020 року. Київ : НУОУ, 2020. 11 с.

31. Інформаційна довідка щодо актуальних кіберзагроз (атак) в мережі Інтернет та дій провідних країн світу у сфері кібербезпеки за травень 2021 року. Київ : НУОУ, 2021. 40 с.

32. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доповідь. Київ : НІСД, 2018. 81 с.

33. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.

34. Іващенко А. М., Гордійчук В. В., Андріянова Н. М. Концепція багатодоменних операцій та її застосування силами оборони. *Збірник наукових праць Центру військово-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2022. № 3. С. 62–67.

35. Вєдєнєєв Д. В., Семенюк О. Г. Нормативно-концептуальні засади визначення функцій інформаційного протиборства у багатосферних («мультидоменних») операціях збройних сил США. *Юридичний науковий електронний журнал.* 2024. № 1. С. 24–28.

36. Вєдєнєєв Д. В. Розвиток зарубіжних науково-концептуальних поглядів на «багатосферні операції». *Українське військо: сучасність та історична ретроспектива* : зб. матеріалів V міжнар. наук.-практ. конф. (м. Київ, 28 листоп. 2024 р.). Київ : НУОУ, 2024. С. 342–343.

37. Joseph Roukoz. LANDEURO 2025. URL: https://surl.li/jpqmxu (дата звернення: 14.08.2025)

38. Amber Wang. How China's new Information Support Force gears military up for PLA modernization. URL: https://surl.lu/uoohwm (дата звернення: 22.08.2025).

39. Громов М. ФБР: китайські хакери атакували близько 80 країн у межах кампанії Salt Typhoon. URL: https://surl.li/vouwch (дата звернення: 02.09.2025).

40. Гнатюк С. Кіберскладник російсько-української війни: уроки та оцінки міжнародної спільноти. Київ : НІСД, 2022. URL: https://surl.li/lxhkiz (дата звернення: 05.09.2025).

41. Вєдєнєєв Д., Сегеда С. Розвиток структури органів психологічних операцій Збройних сил Росії (2014–2021 рр.). *Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану:* тези Міжнар. наук.-практ. конф. (Хмельницький, 24 листоп. 2022 р.). Хмельницький : НА ДПСУ, 2023. С. 885–887.

42. Інформаційна довідка щодо актуальних кіберзагроз (атак) в мережі Інтернет та дій провідних країн світу у сфері кібербезпеки за грудень 2020 року. Київ : НУОУ, 2020. 40 с.

43. Слінько Т. Сучасні загрози інформаційній безпеці країни та шляхи їх подолання. *Український часопис конституційного права*. 2021. № 4. С.77–86.

44. Богом'я В. І., Гудзь А. С. Штучний інтелект: сучасний стан і перспективи застосування. *Сучасні інформаційні технології у сфері безпеки і оборони.* 2023. № 1. С.13–17.

45. Шерешкова І. І., Клунник М. С. Потенціал використання штучного інтелекту в інформаційно-психологічних операціях рф. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матеріалів XV всеукр. наук.-практ. конф. (м. Київ, 27 берез. 2024). Київ : НА СБУ, 2024. Ч. І. Секц. 1. С. 265–266.

References

1. Krotiuk V. A. (ed.) (2021). *Viiny informatsiinoi epokhy: mizhdystsyplinarnyi dyskurs* [Wars of the Information Age: An Interdisciplinary Discourse]. Kharkiv : FOP Fedorko M. Yu. [in Ukrainian].

2. Viedienieiev D., Semeniuk O. (2024). *Rozvytok kontseptualnykh pohliadiv na informatsiine protyborstvo yak skladovu nekonventsiinykh (hibrydnykh) viin i konfliktiv (2013–2023 rr.)* [Development of conceptual views on information confrontation]. Odesa : Oldi+ [in Ukrainian].

3. Pievtsov H. V., Hordiienko A. M., Zalkin S. V., Sidchenko S. O., Feklistov A. O., Hudarkovskyi K. I. (2017). *Informatsiino-psykholohichna borotba u voiennii sferi* [Information and psychological warfare in the military sphere]. Kharkiv : Rozhko S. H. [in Ukrainian].

4. NA SBU (2024). Proceedings of the 15th All-Ukrainian scientific-practical conference *"Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy"* (Kyiv, March 27, 2024) [Current problems of state information security management]. Kyiv, ch. I., sekts. 1 [in Ukrainian].

5. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 r. "Pro Stratehiiu kiberbezpeky Ukrainy" № 447/2021* [Decree of the President of Ukraine On the Resolution of the National Security and Defense Council of Ukraine dated April 14, 2021 "On the Cybersecurity Strategy of Ukraine" activity no. 447/2021]. (2021, August 6). Retrieved from: https://surl.li/ogmglw (accessed 21 June 2025) [in Ukrainian].

6. Ukrainskyi militarnyi portal (2019). *V ZSU formuiut dva novi komanduvannia.* [Two new commands are being formed in the Armed Forces of Ukraine]. Retrieved from: https://surl.li/mmkkum (accessed 10 May 2025) [in Ukrainian].

7. NUOU (2023). Proceedings of the scientific and practical seminar of the department of communication technologies and cyber security *"Dosvid planuvannia ta boiovoho zastosuvannia viiskovykh chastyn (pidrozdiliv) viiski zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy. Problemni pytannia ta shliakhy yikh vyrishennia"* (Kyiv, March 23, 2023) [Experience in planning and combat use of military units (subunits) of the Signal and Cybersecurity Forces of the Armed Forces of Ukraine]. Kyiv [in Ukrainian].

8. Ternovyi O. V., Shkurenko O. M., Minenko L. M. (2023). *Problemni aspekty kiberoborony: mistse ta rol kiberzakhystu v Zbroinykh Sylakh Ukrainy* [Problematic aspects of cyber defense: the place and role of cyber defense in the Armed Forces of Ukraine]. *Suchasni informatsiini tekhnolohii u sferi bezpeky i oborony,* no. 1, pp. 23–31 [in Ukrainian].

9. Zhyvylo Ye. O., Dokil V. M. (2023). *Model metodyky otsiniuvannia spromozhnostei viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy shchodo vykonannia zavdan z vidbyttia voiennoi ahresii v kiberprostori* [Model of the methodology for assessing the capabilities of the communications and cybersecurity troops of the Armed Forces of Ukraine in performing tasks to repel military aggression in cyberspace]. *Suchasni informatsiini tekhnolohii u sferi bezpeky i oborony,* no. 1, pp. 32–40 [in Ukrainian].

10. Murasov R., Melnyk Ya. (2023). *Otsiniuvannia zakhyshchenosti kiberprostoru obiektiv krytychnoi infrastruktury Ukrainy* [Assessment of cyberspace security of critical infrastructure facilities in Ukraine]. *Suchasni informatsiini tekhnolohii u sferi bezpeky i oborony*, no. 1, pp. 41–44 [in Ukrainian].

11. Shypovskyi V. V. (2023). *Systema pokaznykiv otsiniuvannia kiberstiikosti informatsiinykh system obiektiv krytychnoi infrastruktury* [System of indicators for assessing the cyber resilience of information systems of critical infrastructure facilities]. *Zakhyst informatsii,* no. 1 (25), pp. 37–45 [in Ukrainian].

12. Strelbytska L. M., Strelbytskyi M. P., Palchyk M. L. (2022). *Zabezpechennia informatsiinoi ta kiberbezpeky v umovakh viiskovoi ahresii RF proty Ukrainy* [Ensuring information and cybersecurity in conditions of military aggression]. Kyiv : NA SBU [in Ukrainian].

13. Hora I. V., Kolesnyk V. A., Maliuk V. V., Khodanovych V. O., Cherniak A. M., Shcherbyna L. I. (2023). *Zlochyny proty informatsiinoi bezpeky derzhavy: poniattia, vyiavlennia, dosudove rozsliduvannia* [Crimes against the information security of the state]. Kyiv : NA SBU [in Ukrainian].

14. Mashtalir V. V., Shypovskyi V. V. (2023). *Analiz podii u kiberprostori u protsesi rosiisko-ukrainskoi viiny 2022 roku: vysnovky, rekomendatsii, zasvoieni uroky* [Analysis of events in cyberspace during the russian-Ukrainian war of 2022]. *Nauka i oborona*, no. 4, pp. 48–56 [in Ukrainian].

15. Kyrychenko Yu. V., Serhiienko T. I., Slastin V. O. (2025). *Informatsiini viiny yak instrument hibrydnoi ahresii: ukrainskyi dosvid* [Information wars as a tool of hybrid aggression]. *Visnyk NTUU "KPI". Seriia: politolohiia, sotsiolohiia, pravo,* no. 1, pp. 89–95 [in Ukrainian].

16. Hrebnov H. (2023). *Informatsiinyi aspekt hibrydnoi viiny rosii proty Ukrainy* [The information aspect of russia's hybrid war against Ukrain]. *Ukrainskyi informatsiinyi prostir,* no. 1, pp. 107–118 [in Ukrainian].

17. Kresina I. O. (2018). *Osoblyvosti zastosuvannia krainoiu-ahresorom informatsiinykh tekhnolohii u hibrydnii viini* [Peculiarities of the use of information technologies by the aggressor country in hybrid warfare]. *Derzhava i pravo. Seriia: politychni nauky,* no. 81, pp. 27–41 [in Ukrainian].

18. Tverdokhlib Yu. M. (2019). *Informatsiino-psykholohichni operatsii u rosiisko-ukrainskii hibrydnii viini* [Information and psychological operations in the russian-Ukrainian hybrid war]. PhD thesis. Chernivtsi : ChNU imeni Yuriia Fedkovycha, 220 p. [in Ukrainian].

19. Shereshkova I. I., Klunnyk M. S. (2024). *Potentsial vykorystannia shtuchnoho intelektu v informatsiino-psykholohichnykh operatsiiakh rf* [The potential of using artificial intelligence in information and psychological operations in the russian federation]. Proceedings of the 15th All-Ukrainian scientific-practical conference *"Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy"*. (Kyiv, March 27, 2024). Kyiv : NA SBU, ch. I, sects. 1, pp. 265–266 [in Ukrainian].

20. Honcharenko A. A., Kucheruk M. M., Bihun V. M., Kryvenko Yu. M. (2023). Proceedings of the round table *"Aktualni pytannia zakhystu natsionalnoi derzhavnosti v suchasnykh umovakh"* (Kyiv, July 28, 2023). [Current issues of protecting national statehood in modern conditions]. Kyiv : NA SBU [in Ukrainian].

21. Zhytomyrskyi viiskovyi instytut imeni S. P. Korolova (2019). Proceedings of the scientificand practical conference *"Problemy teorii ta praktyky informatsiinoho protyborstva v umovakh vedennia hibrydnoi viiny"* (Zhytomyr, October 24-25, 2019) [Problems of the theory and practice of information confrontation in the conditions of hybrid warfare]. Zhytomyr : ZhVI [in Ukrainian].

22. NUOU (2023). *Informatsiinyi biuleten vyvchennia boiovoho dosvidu zastosuvannia viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy u rosiisko-ukrainskii viini 2022–2023 rokiv* [Information bulletin on the study of combat experience in the use of communications and cybersecurity troops of the Armed Forces of Ukraine]. Kyiv [in Ukrainian].

23. NUOU (2023). *Informatsiinyi biuleten vyvchennia boiovoho dosvidu zastosuvannia viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy u rosiisko-ukrainskii viini 2022–2023 rokiv* [Information bulletin on the study of combat experience in the use of communications and cybersecurity troops of the Armed Forces of Ukraine]. Kyiv [in Ukrainian].

24. Mashtalir V., Permiakov O., Mykus S., Koroliuk N. (2023). *Boiovyi dosvid z pytan kiberoborony, otrymanyi pid chas rosiisko-ukrainskoi viiny. Ch.3. (lystopad 2022 – cherven 2023 roku*) [Combat experience in cyber defense gained during the russian-ukrainian war].. Kyiv : NUOU [in Ukrainian].

25. Mashtalir V., Mykus S., Avramenko M., Avramenko D. (2023). *Boiovyi dosvid z pytan informatsiinoi bezpeky, otrymanyi pid chas rosiisko-ukrainskoi viiny. Ch. 2 (berezen 2022–liutyi 2023 roku)* [Combat experience in cyber defense gained during the russian-ukrainian war]. Kyiv : NUOU [in Ukrainian].

26. Malyk Ya. Yo., Bereza O. I. (2012). *Zabezpechennia informatsiinoi bezpeky Ukrainy u*

konteksti svitovoho dosvidu [Ensuring information security of Ukraine in the context of world experience]. *Efektyvnist derzhavnoho upravlinnia,* no. 32, pp. 20–27 [in Ukrainian].

27. Rushchenko I. P., Zubar N. V. (2017). *Viiny informatsii* [Information wars]. *Oboronnyi visnyk,* no. 8, pp. 4–9 [in Ukrainian].

28. Snitsarenko P. M. (2020). *Informatsiina operatsiia Zbroinykh Syl Ukrainy yak intehruiucha forma voiennykh dii v informatsiinomu prostori* [Information operation of the Armed Forces of Ukraine]. *Nauka i oborona,* no. 1, pp. 37–42 [in Ukrainian].

29. Yaskevych A. (2024). *Internet yak nove seredovyshche suhestyvnoho manipuliatyvnoho vplyvu* [The Internet as a new medium of suggestive manipulative influence.]. Proceedings of the interdepartmental scientificand practical conference *"Posylennia spromozhnostei SB Ukrainy ta vzaiemodiia zi skladovymy sektoru bezpeky i oborony".* (Kyiv, September 24, 2024). Kyiv : NA SBU, ch. 1, pp. 265–267 [in Ukrainian].

30. NUOU (2020). *Informatsiina dovidka shchodo aktualnykh kiberzahroz (atak) v merezhi Internet ta dii providnykh krain svitu u sferi kiberbezpeky za serpen 2020 roku* [Information note on current cyber threats (attacks) in the Internet network and the activities of leading countries of the world in the sphere of cybersecurity for August 2020]. Kyiv [in Ukrainian].

31. NUOU (2021). *Informatsiina dovidka shchodo aktualnykh kiberzahroz (atak) v merezhi Internet ta dii providnykh krain svitu u sferi kiberbezpeky za traven 2021 roku* [Information note on current cyber threats (attacks) in the Internet and the activities of leading countries of the world in the sphere of cybersecurity in May 2021]. Kyiv [in Ukrainian].

32. NISD (2018). *Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy* [Public-private partnership in cybersecurity]. Kyiv [in Ukrainian].

33. Dubov D. V. (2014). *Kiberprostir yak novyi vymir heopolitychnoho supernytstva* [Cyberspace as a new dimension of geopolitical rivalry]. Kyiv : NISD [in Ukrainian].

34. Ivashchenko A. M., Hordiichuk V. V., Andriianova N. M. (2022). *Kontseptsiia bahatodomennykh operatsii ta yii zastosuvannia sylamy oborony* [The concept of multi-domain operations and its application by defense forces]. *Zbirnyk naukovykh prats Tsentru viiskovo-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho,* vol. 3, pp. 62–67 [in Ukrainian].

35. Viedienieiev D. V., Semeniuk O. H. (2024). *Normatyvno-kontseptualni zasady vyznachennia funktsii informatsiinoho protyborstva u bahatosfernykh ("multydomennykh") operatsiiakh zbroinykh syl SShA* [Normative and conceptual principles for determining the functions of information confrontation]. *Yurydychnyi naukovyi elektronnyi zhurnal,* no. 1, pp. 24–28 [in Ukrainian].

36. Viedienieiev D. V. (2024). *Rozvytok zarubizhnykh naukovo-kontseptualnykh pohliadiv na "bahatosferni operatsii"* [Development of foreign scientific and conceptual views on "multi-spherical operations"]. Proceedings of the 5th International scientificand practical conference *"Ukrainske viisko: suchasnist ta istorychna retrospektyva"* (Kyiv, November 28, 2024). Kyiv : NUOU, pp. 342–343 [in Ukrainian].

37. Joseph Roukoz (2025). *LANDEURO.* Retrieved from: https://surl.li/jpqmxu (accessed 14 August 2025) [in English].

38. Amber Wang (2025). *How China's new Information Support Force gears military up for PLA modernisation*. Retrieved from: https://surl.lu/uoohwm (accessed 22 August 2025) [in English].

39. Hromov M. *FBR: kytaiski khakery atakuvaly blyzko 80 krain u mezhakh kampanii Salt Typhoon* [FBI: Chinese hackers attacked about 80 countries]. Retrieved from: https://surl.li/vouwch (accessed 2 September 2025) [in Ukrainian].

40. Hnatiuk S. (2022). *Kiberskladnyk rosiisko-ukrainskoi viiny: uroky ta otsinky mizhnarodnoi spilnoty* [The cyber component of the russian-ukrainian war]. Kyiv : NISD. Retrieved from: https://surl.li/lxhkiz (accessed 5 September 2025) [in Ukrainian].

41. Viedienieiev D., Seheda S. (2023). *Rozvytok struktury orhaniv psykholohichnykh operatsii Zbroinykh syl Rosii (2014–2021 rr.)* [Development of the structure of psychological operations bodies of the Russian Armed Forces (2014–2021)]. Proceedings of the International scientificand practical conference *"Sektor bezpeky i oborony Ukrainy na zakhysti natsional¬nykh interesiv: aktualni problemy ta zavdannia v umovakh voiennoho stanu"* (Khmelnytskyi, November 24, 2022). Khmelnytskyi : NA DPSU, pp. 885–887 [in Ukrainian].

42. NUOU (2020). *Informatsiina dovidka shchodo aktualnykh kiberzahroz (atak) v merezhi Internet ta dii providnykh krain svitu u sferi kiberbezpeky za hruden 2020 roku* [Information notes on current cyber threats (attacks) on the Internet]. Kyiv [in Ukrainian].

43. Slinko T. (2021). *Suchasni zahrozy informatsiinii bezpetsi krainy ta shliakhy yikh podolannia* [Modern threats to the country's information security and ways to overcome them]. *Ukrainskyi chasopys konstytutsiinoho prava,* no. 4, pp. 77–86 [in Ukrainian].

44. Bohomia V. I., Hudz A. S. (2023). *Shtuchnyi intelekt: suchasnyi stan i perspektyvy*

zastosuvannia [Artificial Intelligence: Current State and Prospects]. *Suchasni informatsiini tekhnolohii u sferi bezpeky i oborony,* no. 1, pp.13–17 [in Ukrainian].

45. Shereshkova I. I., Klunnyk M. S. (2024). *Potentsial vykorystannia shtuchnoho intelektu v informatsiino-psykholohichnykh operatsiiakh rf* [The potential of using artificial intelligence in information and psychological operations in the russian federation]. Proceedings of the 15th All-Ukrainian scientific-practical conference *"Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy"*. (Kyiv, March 27, 2024). Kyiv : NA SBU, ch. I, sekts. 1, pp. 265–266 [in Ukrainian].

Стаття надійшла до редакції / Received: 19.09.2025
Прорецензовано / Revised: 30.09.2025
Схвалено до друку / Accepted: 15.10.2025

VIEDIENIEIEV DMYTRO
Doctor of Historical Sciences, Professor,
Professor of the Department of History,
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
https://orcid.org/0000-0002-8929-9875

ORGANIZATIONAL-FUNCTIONAL AND SCIENTIFIC-CONCEPTUAL FEATURES OF CYBERNETIC COMBAT SYSTEMS OF THE LEADING COUNTRIES OF THE WORLD (FIRST QUARTER OF THE 21ST CENTURY)

The author's analysis of the state of scientific development of the problem raised allows us to state the need to prepare separate studies on the in-depth study of the organizational and functional structure, development trends and current tasks, forms and methods of activity of the cyber warfare forces of leading foreign states in order to take into account for the further development and improvement of the activities of the bodies and units of cyber defense of military formations and special services of Ukraine, timely detection and prevention of threats to the cyber sphere of the state.

The purpose of the article is to reveal the organizational and functional and conceptual features of the formation of the latest systems of cyber warfare of the leading countries of the world and to assess the characteristic threats that the modern stage of development of forces and means of intelligence and subversive activity in the network and virtual space poses to the national security of Ukraine.

It is proved that in the leading countries of the world the main trend is the creation of a set of departments, institutions (bodies) for cyber defense and cyber warfare. Cyber defense forces, as a rule, receive the status of a separate branch of the national armed forces by uniting units of electronic intelligence, electronic warfare, information and psychological operations, cryptographic support and cryptological support, geo-information support, information protection in information and telecommunications systems, etc. Currently, more than 60 countries have their own troops (bodies) for conducting cyber warfare – a set of measures aimed at exerting a managerial and/or destructive influence on the automated information and technological systems of the opposing side and protecting their own information and computing resources from such influence through the use of specially developed software and hardware, as well as conducting a system of specialized exercises.

In the author's opinion, in the future it seems appropriate to study in depth the doctrinal documents inherent in them, the experience of organizational and staffing structure, forms and methods of neutralizing threats in the cyberspace, the mechanism of using "non-governmental" hacker groups, the peculiarities of personnel selection, and to ensure that foreign innovations are taken into account in professional training and advanced training of employees of the information and cyber security and counterintelligence bodies of Ukraine.

Keywords: *unconventional strategy; information warfare; cyber warfare; cyber espionage; information security.*