УДК 32.019.51:323.28:323.2(477)

КАЛАЙДА Ю.П., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ
ORCID: https://orcid.org/0000-0002-1408-2145

ГІБРИДНІ КІБЕРАТАКИ В УМОВАХ УКРАЇНСЬКО-РОСІЙСЬКОЇ КІБЕРВІЙНИ

DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346481

Анотація. *У статті аналізуються гібридні кібератаки як ключовий елемент українсько-російської кібервійни, яка триває з 2014 року та значно посилилася після повномасштабного вторгнення Росії в Україну у 2022 році. На основі аналізу офіційних даних розглядаються типи кібератак, їх інтеграція з кінетичними операціями, їх суспільні наслідки для критичної інфраструктури та стратегічні імплікації. У статті підкреслюється роль кібероперацій у гібридній війні, де кібератаки поєднуються з інформаційними операціями, шпигунством та фізичними діями. Пропонуються стратегії кіберпротидії, зокрема, шляхом посилення кіберстійкості, розвитку кібероборони та удосконалення національного законодавства у сфері кібербезпеки. У висновках вказується необхідність посилення міжнародної співпраці для протидії таким кібератакам.*

Ключові слова*: гібридна війна, кібератаки, українсько-російський конфлікт, кібервійна, критична інфраструктура.*

Summary*. This article analyzes hybrid cyberattacks as a key element of the Ukrainian-Russian cyberwar, which has been ongoing since 2014 and has significantly intensified after Russia's full-scale invasion of Ukraine in 2022. Based on an analysis of official data, the types of cyberattacks, their integration with kinetic operations, their societal consequences for critical infrastructure, and strategic implications are examined. The article emphasizes the role of cyberoperations in hybrid warfare, where cyberattacks are combined with information operations, espionage, and physical actions. Cyber countermeasure strategies are proposed, including by enhancing cyber resilience, developing cyberdefense, and improving national legislation. The conclusions indicate the need for increased international cooperation to counter such threats.*

Keywords*: hybrid warfare, cyberattacks, Ukrainian-Russian conflict, cyberwar, critical infrastructure.*

Постановка проблеми.

Воєнні конфлікти сучасності реалізують принципи гібридної та мережецентричної війни, а притаманна їм кіберборотьба стає дедалі більш поширеним явищем через побудову високотехнологічного суспільства, його інформатизації та цифровізації [1]. Інтенсивність нанесення кібератак суттєво зростає напередодні активних конвенційних воєнних (бойових) дій, та досягає свого максимуму з їх початком, в цей період здійснюється вплив на заздалегідь виявлені вразливості у кіберінфраструктурі [2, с. 12]. Українсько-російська кібервійна є одним з найяскравіших прикладів сучасної гібридної війни, де кібернетичні операції інтегруються з традиційними військовими діями, інформаційною пропагандою та економічним тиском. В умовах цієї війни зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак [3]. Як наслідок, спектр об'єктів, що піддаються

кібервпливу, постійно розширюється, а форми та способи його нанесення – удосконалюються та урізноманітнюються [4]. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди. Посилюється тенденція щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, впливу на виборчі процеси [3]. Наймасштабнішим воєнним конфліктом сучасності, який триває і сьогодні, є російсько-українська кібервійна, яка ведеться не тільки на суходолі, в повітрі та на морі, але й у кібердомені. Сьогодні складову російсько-українського протистояння, що відбувається у кібердомені, визнано першою повноцінною кібервійною, а отже, вона є найактуальнішим джерелом досвіду ведення кіберборотьби [2, с.20].

Результати аналізу наукових публікацій. Проблеми застосування інформаційної зброї в інформаційних війнах висвітлені у працях В. Брижка [5], О. Данильяна, О. Дзьобаня, В. Пилипчука, Г. Почепцова, М. Швеця, В. Цимбалюка [5]. Шляхи запобігання кібератак в умовах воєнного стану висвітлені у роботах Я.Мануілова [6] та С.Краснікова [7].

Гібридна кібервійна в контексті українсько-російського конфлікту є предметом поглибленого аналізу багатьох вчених, серед яких слід виділити праці В.Алєйника [8] М.Білоусова, О.Дикого [9], В.Горгуленка [2] Р.Грищука та ін.

Перебіг та особливості російсько-українського інформаційної і кіберборотьби досліджували іноземні вчені – К.Бронк (Bronk C.), Дж.Колінз (Collins G.) та Д. Воллач (Wallach D.) [10].

Водночас, залишається не достатньо дослідженими існуючі тенденції та закономірності здійснення кібератак гібридного характеру під час українсько-російської кібервійни. Також не достатньо реалізованими залишаються заходи зі створення та функціонування кібервійськ у ході такої війни.

Метою статті є визначення особливостей та закономірностей гібридних кібератак в умовах українсько-російської кібервійни для розробки рекомендацій щодо необхідності удосконалення кіберборотьби в інформаційному просторі.

Виклад основного матеріалу.

Історично склалося, що поняття війни охоплює собою військове зіткнення між двома або кількома незалежними державами. Особливістю військових світових процесів останнього десятиліття стало значне зростання збройної конфліктності, локальних військових дій у порівнянні з традиційною війною. Замість традиційного поняття “війна” в сучасних умовах використовується інноваційне поняття “гібридна війна”. Одні автори розглядають таку війну для характеристики потенційних атак із застосуванням ядерної, хімічної чи бактеріологічної зброї та іншої зброї масового ураження або її компонентів, визначення динаміки бойового простору, яка передбачає адаптацію та гнучку реакцію на певні політичні події [11]. Інші вчені наполягають на тому, що “гібридна війна” - це сукупність заздалегідь підготовлених та оперативно реалізованих дій воєнного, дипломатичного, інформаційного характеру, спрямованих на досягнення стратегічних цілей [12].

Головна особливість гібридної війни полягає у тому, що під час такої війни використовуються усі доступні ресурси: матеріально-технічні, фінансові та людські.

Гібридна війна передбачає комплекс гібридних загроз різного типу: 1) традиційні; 2) нетрадиційні; 3) змішані [12]. На відміну від інших загроз комплекс гібридних загроз має кінцеву мету і спрямовується на обраний об’єкт впливу (конкретну державу-мішень). Реалізація комплексу загроз залежить від наявності джерела, здатного

забезпечити необхідні сили і засоби, а також можливостей доступу до них. Кумулятивний ефект від впливу гібридних загроз забезпечується реалізацією комплексу заходів, пов’язаних з координацією діяльності значних сил і засобів, що діють на території “країни-мішені” та за її межами. Успіх операції під час гібридної війни залежить від вмілого використання низки факторів, що зумовлюють динаміку розвитку обстановки і належну спрямованість подій. В основі стратегії гібридної війни лежить цілеспрямована робота з прогнозування та стратегічного планування [12]. Реалізація стратегії гібридної війни складає особливу загрозу для всієї системи національної безпеки держави.

У Стратегії забезпечення кібербезпеки України, серед іншого, зазначається: “Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України”. Водночас, стверджується, що “така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури” [3]. Саму тому “набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об’єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об’єктами” [3].

У свою чергу, у Доктрині інформаційної безпеки зафіксовано: “Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України” [13]. Метою цієї Доктрини є “уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни” [13].

Не дивлячись на те, що з моменту затвердження цієї Доктрини минуло майже вісім років залишаються надзвичайно актуальними зовнішні загрози національній безпеці в інформаційній сфері:

здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

інформаційне домінування держави-агресора на тимчасово окупованих територіях [13].

Найбільшою загрозою кібербезпеці України залишається гібридна агресія Російської Федерації проти України у кіберпросторі [3].

Поряд із агресією та гібридною війною існує поняття "кібервійна", яке часто застосовується науковій та публіцистичній літературі. У найбільш загальному розумінні кібервійна – це комп'ютерне протистояння у просторі Інтернету [14].

Український вчений О. Мережко визначає кібервійну як використання Інтернету й пов'язаних з ним технологічних і інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету іншої держави.

Серед характерних рис кібервійни можна виділити: 1) використання технологічних й інформаційних засобів, у т.ч. кібератак, проти комп'ютерних систем іншої держави; 2) їх застосування у кіберпросторі; 3) завдання значної шкоди суспільству, державі, юридичним та фізичним особам. Отже, однією з визначальних ознак кібервійни є кібератака, яка може мати гібридні форми.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" під кібератакою слід розуміти спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [15].

Крім визначених цим законом ознак, кібератака гібридного характеру має свої додаткові характеристики. На наш погляд, основу гібридної кібератаки утворюють комплексні дії, які поєднують: технічні кібератаки (DDoS, шкідливе ПЗ, експлуатація вразливостей); інформаційні (дезінформація, фейки, маніпуляція медіа) та психологічні операції (посилення паніки, підрив довіри до влади); фізичні дії (саботаж, диверсії, що супроводжують традиційні кібератаки). Відмінність від традиційних кібератак полягає у синергії цих компонентів для досягнення стратегічного ефекту: дестабілізації управління органами державної влади, знищення або пошкодження критичної інфраструктури, залякування та деморалізації населення.

З початку російської агресії проти України у 2014 році світ став свідком трансформації війни в гібридну форму, де кіберпростір став одним із ключових театрів воєнних дій. З цього моменту кібератаки стали серйозним інструментом дестабілізації України, спрямованим на порушення роботи урядових систем, енергетичної інфраструктури та фінансового сектору. Державна служба спеціального зв'язку та захисту інформації України зафіксувала значну кількість кібератак з боку проросійських хакерських груп після повномасштабного вторгнення. У 2015 році державними органами України фіксувалися атаки на енергетичну мережу України, які спричинили відключення електроенергії для сотень тисяч людей. Найбільш відомим прикладом стала кібератака на системи ПрАТ "Київобленерго" у грудні 2015 року, яка призвела до блекауту у частини Київської області та була пов'язана з виведенням з ладу обладнання автоматики та програмного забезпечення [16]. Загалом ця кібератака мала комплексний характер та складалась як мінімум з таких складових:

попереднє зараження мереж за допомогою підроблених листів електронної пошти з використанням методів соціальної інженерії;

захоплення управління автоматизованих систем диспетчерського управління з виконанням операцій вимикань на підстанціях;

виведення з ладу елементів IT інфраструктури (джерела безперебійного живлення, модеми, RTU, комутатори);

знищення інформації на серверах та робочих станціях (утилітою KillDisk);

атака на телефонні номери кол-центрів з метою перевантаження ліній і, відповідно, відмови в обслуговуванні знеструмлених абонентів [16].

Найбільш потужна хакерська атака на Україну з боку росії відбулася в червні 2017 року із використанням вірусу NotPetya. Зокрема, в Україні було паралізовано роботу банків, аеропортів, державних та інших установ. Збитки від атаки вірусу Petya у світі сягають 8 мільярдів доларів [17].

У сучасних наукових дослідженнях цих атак підкреслювалася: їх цільова спрямованість (кібершпигунство, кібердиверсія, кібертероризм); тенденція до їх ескалації; стійкість українських кіберзахисних систем.

Повномасштабне вторгнення 2022 року лише підтвердило, що сучасна війна не обмежується танками артилерією та авіацією — вона ведеться також у кіберпросторі, де атаки можуть бути не менш руйнівними, ніж фізичні дії.

У січні та лютому 2022 року основним вектором спрямування російської кіберборотьби був кібервплив на заздалегідь виявлені кіберрозвідкою вразливості, а саме [18]:

перша з них – кібератака раніше невідомого хакерського угруповання DEV-0586 із застосуванням ШПЗ (програми-вимагача), яку ідентифікував Центр аналізу загроз Microsoft-ту 13 січня 2022 року;

одразу після цього, 14 січня 2022 року, було здійснено кібератаку на викривлення контенту веб-ресурсів близько 70 державних інституцій України, серед яких сайти Кабінету Міністрів України, Міністерства закордонних справ України та Ради національної безпеки і оборони України;

15 лютого 2022 року – серія потужних DDoSатак на веб-ресурси Міноборони України, Міністерства закордонних справ України, Збройних Сил України, Приватбанку та Ощадбанку.

Отже, цикл описаних вище кібератак, що мали місце у січні – лютому 2022 року можна об’єднати в кібероперацію, цілями якої були дестабілізація інформаційного та кіберпростору України, відволікання зусиль основних суб’єктів забезпечення кібербезпеки держави на протидію кібератакам, компрометація онлайн-банкінгу та, в цілому, створення деякого переможного наративу ще до початку кінетичної фази конфлікту, на тлі зосередження вздовж державного кордону України стотисячного наступального угруповання військ (сил) [2, с.20].

Після повномасштабного вторгнення у лютому 2022 року кількість таких атак зросла в рази, перетворивши кіберпростір на повноцінний театр воєнних дій. Так, за офіційними даними з 2022 року кількість кібератак зросла на 300% [19].

Найчастіше об’єктами таких атак ставили об’єкти критичної інфраструктури: енергетика, транспорт та фінанси. У 2022 – 2023 рр. зафіксовано відповідно 2194 та 2543 кіберінцидентів, більшість з яких спрямована на органи державної та місцевої влади. Як ми бачимо, у 2023 році зафіксовано на 62,5% більше кіберінцидентів, ніж за результатами 2022 року [20].

У 2024 році кількість кібератак на Україну зросла ще на 69,8%, досягнувши 4315 інцидентів, у порівнянні з 2023 роком, коли було зафіксовано 2543 кіберінцидента [21].

Важливим є інформаційний компонент гібридних кібератак, спрямований на масове поширення фейків через Telegram, Twitter, фейкові новини тощо. Цей компонент активно використовується для дезінформації, поширення паніки та хаосу в соцмережах. У звіті Держспецзв"язку "Війна та кібер: три роки боротьби та уроки для глобальної безпеки" зазначається, що російські спецслужби змінили підхід – від точкових кібератак до системного компонента воєнної кампанії. Держава-агресор активно залучає приватні ІТ-компанії, хакерські угруповання та "волонтерів" до своїх кіберактивностей. Зростає частка операцій із кібершпигунства, націлених на здобуття розвідданих та підтримку бойових дій. Це частково пояснює зменшення кількості критичних інцидентів у 2023-2024 роках (367 – у 2023 та 59 – у 2024 році), попри загальне зростання кіберінцидентів (2194 – у 2022 році, 2543 – у 2023 році та 4315 – у 2024 році) [22]. Російська стратегія включає інтеграцію кібероперацій з кінетичними у випадку комбінованих атак на українські об'єкти критичної інфраструктури, що створює виклики для міжнародного права.

У 2025 році за даними українських джерел 20% глобальних кібератак з використанням гібридних методів припадає на Україну. Від початку поточного року в Україні відбувається близько 15 кібератак щодня. Основним джерелом кібератак залишається рф [23].

Як ми бачимо, сучасні гібридні кібератаки характеризуються поєднанням технічних методів (наприклад, DDoS-атаки, шкідливе ПЗ) з психологічними та інформаційними операціями, такими як поширення дезінформації та деструктивної пропаганди. Метою таких атак є не лише технічна шкода об'єктам критичної інфраструктури, але й створення обстановки страху, паніки, хаосу, підрив довіри до органів державної влади та ослаблення обороноздатності держави.

Таким чином, під час гібридних кібератак можна виділити технічні, інформаційні та інформаційно-психологічні компоненти, які часто синхронізуються з фізичними діями за певним алгоритмом (кібератака на систему управління енергосистемою → ракетний удар по електростанції → інформаційна кампанія про "нездатність влади захистити громадян").

Небезпечними є наслідки таких атак, які можна класифікувати на: економічні (збитки для критичної інфраструктури); соціальні (підрив довіри громадян до цифрових сервісів ("Дія", "Приват24"); психологічні (поширення паніки та дезінформації); військові (порушення зв'язку, логістики); політичні (численні спроби делегітимізації державної влади через інформаційні кампанії, залякування населення).

Відповіддю України, зважаючи на несформованість кібервійськ із спроможностями до здійснення кібервпливу, було створення так званої ІТ-армії, яка складається переважно з волонтерів-фахівців в галузі кібербезпеки [2]. З моменту вторгнення російської федерації на територію України з перших днів Міністерством цифрової трансформації було створено Telegram канал, покликаний масово долучати людей до атак на різні ресурси російської федерації (https://t.me/itarmyofukraine2022) [9, с.102]. Також українська сторона використовує краудсорсингові технології проти ворога на прикладі боту єВорог. Вказаний напрям є одним із новаторських у сучасному світі, так як дозволяє збирати та використовувати інформацію про пересування сил противника фактично в "реальному часі" з детальним описом кількості особового складу та відповідної техніки [9, с.103].

Попри численні кібератаки, Україна проявила кіберстійкість в умовах воєнного стану завдяки швидкій адаптації, міжнародній підтримці та власним кіберзбройним силам, формування яких ще триває. Підготовка мобілізаційного потенціалу для кіберфронту є однією із пріоритетних завдань держави [9, с.103].

Стратегія кібербезпеки України, зокрема, передбачає:

посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням;

утворення у системі Міністерства оборони України кібервійськ та забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору [3].

До речі, створення у системі Міністерства оборони України кібервійськ та набуття ними відповідних спроможностей було передбачено ще Указом Президента України від 26 серпня 2021 року № 446/2021.

Не зважаючи на те, що заходи зі створення таких військ передбачено Планом заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженим розпорядженням Кабінету Міністрів України від 7 березня 2025 р. № 204-р, Верховною Радою України досі не прийнято відповідного закону, невідкладність реалізації якого продиктовано часом.

Крім цього, багато інших питань в контексті кібероборони залишається недостатньо вирішеними. Одним з найважливіших питань є розробка національної стратегії протидії кібератакам (або внесення змін в існуючі нормативні акти), яка передбачатиме:

розвиток національних сил кібероборони;

швидке відновлення об’єктів критичної інфраструктури, пошкоджених в результаті кібератаки та ліквідація наслідків їх прояву;

проактивну кіберпротидію суб’єктами забезпечення кібербезпеки, удосконалення їх міжвідомчої взаємодії та координації;

підвищення цифрової грамотності населення, навчання та підвищення кваліфікації фахівців у сфері кібербезпеки;

використання штучного інтелекту для виявлення кібератак;

використання інших технологічних інновацій, таких як блокчейн для захисту даних та Zero Trust Architecture (модель з нульовою довірою) для мінімізації незаконного доступу, постійної верифікації даних.

На даний момент потрібно більше зосереджувати увагу на: підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування, розвиток механізмів виявлення та попередження кіберзагроз та ліквідації наслідків їх прояву, підвищення захищеності громадян та територій від наслідків надзвичайних ситуацій, спричинених інформаційно-технічним чи військовим впливом на об’єкти критичної інформаційної інфраструктури [24].

Важливо відзначити, що діяльність з кібербезпеки є справою не тільки однієї держави (групи держав), а й міжнародної спільноти, яка складається з комплексу заходів. З цього випливає потреба напрацювання державами і міжнародним співтовариством відповідної інституціональної системи забезпечення кібербезпеки, яка має бути адаптована до завдань комплексної боротьби з гібридною війною та агресією.

Досвід України доводить – ефективний кіберзахист можливий лише за умов співпраці, обміну розвідданими та синхронізації зусиль між державними та приватними структурами, а також з міжнародними партнерами [22].

В цьому контексті важливою складовою запобігання гібридних кібератак є міжнародна співпраця у частині:

зміцнення взаємодії суб'єктів забезпечення кібербезпеки з правоохоронними органами та спеціальними службами іноземних держав;

запровадження каналів обміну інформацією про кіберзагрози (threat intelligence) з країнами NATO та ЄС;

укладання міжнародних договорів у сфері боротьби з кіберзлочинами, уніфікація термінології у цій сфері;

імплементація цих договорів у національне законодавство, зокрема, імплементації Конвенції ООН про кіберзлочинність у частині криміналізації кібератак та інших кіберзлочинів;

вироблення у взаємодії з країнами НАТО та ЄС ефективного санкційного механізму проти російських APT-груп та їхніх спонсорів.

Висновки. Гібридні кібератаки демонструють еволюцію війни, де кіберпростір стає повноцінним театром воєнних дій. Гібридні кібератаки є стратегічною кіберзброю, які стали невід'ємною частиною українсько-російської кібервійни. Ця війна з початку повномасштабного вторгнення продемонструвала, що кібератаки агресора співпадають з воєнними діями, тобто захопленням або руйнуванням об'єктів критичної інфраструктури [24; 25]. Ці атаки не лише руйнують критичну інфраструктуру, а й негативно впливають на населення, підривають довіру до органів державної влади та міжнародних інституцій. Продемонструвавши свою кіберстійкість, Україна стала "тестовим полігоном" для таких атак, котрі мають глобальні імплікації. Водночас, за тривалий період кібервійни наша держава накопичила унікальний досвід кіберпротидії, який може бути корисним для формування кібероборони інших країн, які можуть стати мішенню російських кібератак. Цей досвід підкреслює необхідність впровадження комплексного підходу до забезпечення кібербезпеки з урахуванням інтеграції технічних, правових, освітніх та міжнародних зусиль у цій сфері. Подальші наукові дослідження з цієї тематики слід фокусувати на прогнозуванні кібератак гібридного характеру та розробці контрзаходів.

Використана література

1. Грищук Р.В., Канкін І.О., Охрімчук В.В. Технологічні аспекти інформаційного протиборства на сучасному етапі. *Захист інформації*. 2015. Т. 17. № 1. С. 80–86.

2. Горгуленко В.А. Кіберборотьба у воєнних конфліктах сучасності: передовий досвід, тенденції та закономірності розвитку. *Modern Information Technologies in the Sphere of Security and Defenc*e. 2024. № 2(50). С. 11-28. DOI: 10.33099/2311-7249/2024-50-2-11-28.

3. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26.08.2021 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

4. Грищук Р.В. Інформаційна та кібернетична безпека: роль та місце в умовах *гібридної війни. Кібербезпека в Україні: правові та організаційні питання :* матеріали Всеукр. наук.-практ. конф., (м. Одеса, 21 жовтня 2016 р.) Одеса : ОДУВС, 2016. С. 16–17.

5. Брижко В., Швець М., Цимбалюк В. Е-боротьба в інформаційних війнах та інформаційне право. за ред. М. Швеця. К.: ТОВ "ПанТот", 2007. 218 с.

6. Красніков С.А. Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану. *Інформація і право*. 2023. №3(46). С. 118-128.

7. Мануілов Я.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. *Інформація і право*. 2023. №1(44). С. 154-167.

8. Білоусов М.В., Алєйник В.Г. Російська гібридна війна: загрози і кібервиклики для європейської інформаційної безпеки. *Регіональні студії*. 2023. №33. С. 119-125.

URL:http://regionalstudies.uzhnu.uz.ua/archive/33/18.pdf. DOI doi.org/10.32782/2663-6170/2023.33.18

9. Дикий О.В. Кібервійна в Україні. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/9535e5f6-2d15-4630-a896-68fedf3032d1/content.

10. Bronk C., Collins G., Wallach D. The Ukrainian Information and Cyber War. *The Cyber Defense Review*. 2023. Vol. 8. № 3. P. 33–50.

11. Auditors Find DoD Hasn't Defined Cyber Warfare: URL:http://www.darkreading.com/risk-management/auditors-find-dod-hasnt-defined-cyber-warfare/d/d-id/1092427?

12. Бартош А. Гибридные войны в стратегии США и НАТО. *Независимое военное обозрение*. URL: http://nvo.ng.ru/concepts/2014-10-10/1_nato.html.

13. Доктрина інформаційної безпеки: затв. Указом Президента України від 25.02.2017 р. № 47. URL:https://www.president.gov.ua/documents/472017-21374.

14. Кібервійна URL: https://uk.wikipedia.org/wiki/Кібервійна.

15. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. №2163-VIII. *Відомості Верховної Ради України*. 2017. №45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

16. Кібератака на українську енергетику: як це було. URL: https://texty.org.ua/fragments/65835/Kiberataka_na_ukrajinsku_jenergetyku_jak_ce_bulo-65835/

17. Збитки від атаки вірусу Petya у світі сягають 8 мільярдів доларів – експерт. URL: https://www.unian.ua/science/2003241-zbitki-vid-ataki-virusu-petyaa-syagayut-8-milyardiv-dolariv-ekspert.html

18. Destructive malware targeting Ukrainian organizations [online]. (2022). Microsoft. Available URL: https://www.microsoft.com/enus/security/blog/2022/01/15/destructive-malware-targetingukrainian-organizations

19. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики. URL:https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454.

20. 2023 року кількість зареєстрованих кіберінцидентів зросла на 62,5%: звіт оперативного центру реагування на кіберінциденти ДЦКЗ. URL: https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz.

21. У 2024 році кількість кібератак на Україну зросла на 70%. URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931#:

22. Держспецзв’язку презентує звіт «Війна та кібер: три роки боротьби та уроки для глобальної безпеки». URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-prezentuye-zvit-viina-ta-kiber-tri-roki-borotbi-ta-uroki-dlya-globalnoyi-bezpeki

23. З початку 2025-го в Україні фіксується близько 15 кібератак щодня — Держспецзв'язку. URL:https://suspilne.media/1075891-z-pocatku-2025-go-v-ukraini-fiksuetsa-blizko-15-kiberatak-sodna-derzspeczvazku/.

24. Запорожець Т.В. Державна політика у сфері захисту критичної інфраструктури. Навчальний посібник. К., ДКС-Центр. 2024. 186 с.

25. Кібератаки, артилерія, пропаганда. загальний огляд вимірів російської агресії. URL:https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~