УДК 355.02:004.946.5.056](100)(045)
DOI: 10.36273/2076-9555.2020.4(285).22-26

Руслан Гула,
доктор історичних наук, доцент, професор кафедри філософії
Харківського національного університету Повітряних Сил імені Івана Кожедуба,
e-mail: rslnhula1@gmai.com
ORCID: https://orcid.org/0000-0002-8177-1565
Ірина Передерій,
доктор історичних наук, доцент, завідувач кафедри українознавства, культури
та документознавства Національного університету
"Полтавська політехніка імені Юрія Кондратюка",
e-mail: iryna.perederii@gmail.com
ORCID: https://orcid.org/0000-0001-7473-5868
Олена Вітринська,
кандидат історичних наук, доцент кафедри українознавства, культури
та документознавства Національного університету
"Полтавська політехніка імені Юрія Кондратюка",
e-mail: vitrynska@gmail.com
ORCID: http://orcid.org/0000-0001-9413-1236

Концептуальні засади воєнної політики у кіберпросторі провідних держав світу та воєнно-політичних інституцій

Процеси глобалізації та модернізації зумовили формування унікального феномену "віртуальної інформаційної політики" як реалізації й захисту національних інтересів у кіберпросторі, що в умовах стрімкого поширення новітніх інформаційних технологій потребує побудови принципово нової ефективної інформаційної політики. У сучасному світі це є винятково прерогативою розвинених держав, а для інших учасників інформаційно-політичного простору існує загроза своєрідного інформаційного неоколоніалізму. Отже, об'єктивно виразна проблемна ситуація, зумовлена такими складними процесами: наявність відкритої та прихованої інформаційної агресії в сучасному інформаційно-політичному просторі, що ускладнюється глобалізацією та тенденціями до інтеграції, уніфікації світу. Це виявляється через множину форм і наслідків впливу на процес формування нової соціальної моделі — інформаційного суспільства як основного суб'єкта здійснення інформаційного протиборства.

Автори виділяють у самостійний об'єкт наукового вивчення поняття "кіберпростір", що досліджується з позицій сьогодення як комплексна категорія за нелінійного характеру розвитку цього надскладного соціально-політичного явища. Розвиток інформаційно-комунікаційних технологій у глобальному інформаційному просторі об'єктивно зумовив потребу створення системи комплексного застосування сил і засобів кібернетичних операцій у військовій сфері.

Здійснено аналіз головних тенденцій воєнної політики провідних держав світу та воєнно-політичних інституцій у кіберсфері щодо побудови ефективної системи протидії кіберзагрозам у глобальному інформаційному просторі та створення засобів ведення кібервійни. Зроблено спробу розкрити зміст і сутність кіберпростору як полігону для випробування новітніх технологій в умовах ведення інформаційної війни.

Ключові слова: *інформаційна війна; кібервійна; кібербезпека; кібератаки; кібервійська; національна безпека; блок НАТО; кіберпростір*

Постановка проблеми. Розвиток інформаційно-комунікаційних технологій у глобальному інформаційному просторі об'єктивно зумовив проблему створення системи комплексного застосування сил і засобів кібернетичних операцій у військовій сфері. Кіберпростір як "глобальна сфера", домен глобального інформаційного простору є сукупністю взаємопов'язаних інформаційних структур і технологій, що разом із сухопутним, повітряно-космічним і морським просторами стає реальним театром воєнних дій, загрози щодо якого дорівнюють загрозам від засобів масового ураження [5, с. 5].

Аналіз попередніх досліджень і публікацій. Вивченню сутності глобального інформаційного простору присвячено праці Р. Арона, З. Бжезинського, Е. Тоффлера, М. Кастельса. Серед вітчизняних авторів відповідна тематика привертала увагу дослідників В. Андрущенка, О. Базалука, О. Бахтіярова, В. Бебика, А. Гуцала, О. Зернецької, В. Іванова, Є. Макаренка, які з'ясовують питання, пов'язані з тенденціями функціонування глобального комунікативного простору, визначенням місця й ролі вітчизняних комунікативних структур і технологій у цьому процесі. Окрім того, сучасна українська наукова думка дедалі більше зближується з практикою політичного управління, зосереджує увагу на дослідженнях практично значущих інформаційних аспектів національної безпеки. У площині розв'язання проблем кібербезпеки працюють вітчизняні науковці А. Курбан, М. Требін, О. Дзьобань, О. Литвиненко, М. Ожеван, Г. Почепцов, О. Соснін, які започаткували розгляд порушеного у пропонованому дослідженні питання.

Метою статті є аналіз головних тенденцій воєнної політики провідних держав світу та воєнно-політичних інституцій у кіберсфері щодо побудови ефективної системи протидії кіберзагрозам у глобальному інформаційному просторі та створення засобів ведення кібервійни. Автори також прагнули розкрити зміст і сутність кіберпростору як полігону випробування новітніх технологій в умовах ведення інформаційної війни.

Виклад основного матеріалу дослідження. Кіберпростір поступово заповнив майже всі сфери сучасного суспільного життя. Вперше термін "кіберпростір" (ще до фактичної появи явища, за кілька років до його технічної реалізації) використав канадський письменник-фантаст американського походження В. Ґібсон у новелі "Палаючий хром" (Burning Chrome, 1982). Згодом він ширше розтлумачив це поняття у творі "Нейромант" (Neuromancer, 1984) з однойменної трилогії "Кіберпростір". На думку автора, кіберпростір (cyberspace) — це злагоджена галюцинація, котрої щодня зазнають мільярди звичайних операторів у всьому світі. Це логічна репрезентація відомостей, збережених у пам'яті та на магнітних носіях комп'ютерів людства; потоки даних, що струменять у просторі розуму; скупчення та сузір'я інформації [17].

Виходячи з дослівного розуміння терміна, що походить від словосполучення "кібернетичний простір", його слід тлумачити як простір (територію), що сформований і працює на основі принципів, методів кібернетики (науки про загальні закони створення, одержання, зберігання, передавання та опрацювання інформації) [11, с. 215—219].

Відповідно до міжнародного стандарту керівних принципів і методів кібербезпеки ISO/IES 27032, кіберпростір — це штучне середовище, що не існує в будь-якій фізичній формі й виникло внаслідок взаємодії людей, створеного ними програмного забезпечення та послуг в інтернеті за допомогою технологічних пристроїв і під'єднаних до них мереж [15, с. 62].

Нормативна база США визначає кіберпростір як сферу, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними в мережевих системах, а також пов'язану з ними фізичну інфраструктуру.

Євросоюз в офіційних документах тлумачить кіберпростір як віртуальний простір, де циркулюють електронні дані світових персональних комп'ютерів. Для Великобританії кіберпростір — це всі форми мережевої цифрової активності, що охоплюють контент і дії, котрі здійснюють через цифрові мережі. У Німеччині під кіберпростором розуміють усю інформаційну інфраструктуру, доступну через інтернет поза будь-якими територіальними кордонами [2, с. 8—9].

В Україні наразі немає стандартизованого поняття кіберпростору, але варто навести найповніші його визначення вітчизняних дослідників. Зокрема, С. Гнатюк, провівши багатокритеріальний аналіз, запропонував таку узагальнену дефініцію: кіберпростір — це віртуальний простір, отриманий унаслідок взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у тому числі інтернет) для підтримання та управління процесами перетворення інформації (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства [4, с. 118—129].

Автори підручника "Інформаційна та кібербезпека: соціотехнічний аспект" наводять визначення кіберпростору, розуміючи під ним віртуальне комунікаційне середовище, утворене системою зв'язків між користувачами та об'єктами інформаційної інфраструктури (як-от електронний інформаційний ресурс, системи та мережі всіх форм власності), керовані автоматизованими системами управління, що використовуються не лише для перетворення та трансляції інформації, що в них циркулює, з метою забезпечення інформаційних потреб суспільства, а й для впливу на аналогічні об'єкти протиборчої сторони [2, с. 10].

Про важливість захисту національної військової інформаційної інфраструктури свідчать такі статистичні дані. Інформаційно-комунікативна система Міністерства оборони (МО) США складається з 15 тис. комп'ютерних мереж і понад 7 млн комп'ютерів; на інформаційні ресурси Пентагону (в тому числі й внутрішню мережу SPIRNET) здійснюється 360 млн кібератак на рік, а на Глобальну інформаційну мережу (Global Information Grid) МО США — майже 3 млн кібератак на добу. Військові фахівці вважають, що наразі загроза початку "комп'ютерних воєн" ("кібервоєн") стає очевидною реальністю й потребує постійної уваги. За оцінками фахівців, у цій війні переможеною може виявитися навіть та держава, військовий потенціал якої значно перевершує могутність супротивника [3].

Поступово світова спільнота усвідомлює, що кіберпростір перетворюється на поле боротьби, для якого слід розробити відповідну стратегію національної та міжнародної безпеки. Американський фахівець із питань кібербезпеки К. Гірс ще 2008 р. закликав стратегів усвідомити, що "частина кожного політичного чи військового конфлікту реалізовуватиметься в інтернеті" [16]. Віцепрезидент американського Інституту вивчення тероризму та політичного насильства, колишній аналітик МО США П. Пробст зауважив, що за доби інформаційного суспільства в міжнародному середовищі "держави дедалі більше залежать від високих технологій. Комплексні національні системи потенційно небезпечні, оскільки охоплюють життєво важливі вузли, удари по яких здатні призвести до незворотних руйнівних наслідків. Така атака може бути здійснена через комп'ютери або з використанням вибухівки, або шляхом виведення з ладу кабелів, що спричинить ланцюг аварій із наступним колапсом усіх контрольних систем трубопроводу чи аеропорту" [7]. Співробітник вашингтонського Центру міжнародних і стратегічних досліджень У. Лакер наголошує, що "втручання комп'ютерних хакерів може зробити всю державу не здатною до нормального функціонування. Звідси зростання занепокоєння щодо можливостей інформаційного тероризму та кібервійни… Достатньо 20 кваліфікованих хакерів та одного мільярда доларів, щоб знищити Америку" [18, с. 35].

Актуалізація потреби убезпечення держави у сфері кіберпростору від загрози несанкціонованого кібервторгнення зумовила сплеск дискусій про визнання на міжнародному рівні кібератаки "актом війни". 30 січня 2010 р. сенатор США від Республіканської партії С. Колінз зазначила, що США розглядають питання про ставлення до кібератак як до

оголошення війни, а 12 травня 2010 р. помічник заступника міністра оборони США з політичних питань Дж. Міллер заявив, що США готові завдати воєнного удару у відповідь на кібератаки в комп'ютерних мережах. Отже, реальність і масштабність інформаційних загроз національній безпеці держав у сучасному глобальному інформаційно-комунікаційному середовищі зумовили створення спеціалізованих підрозділів у правоохоронних органах і збройних силах країн, так званих кібервійськ. На нашу думку, *кібервійська* — це спеціальні військові формування у складі збройних сил, що за функціональним призначення забезпечують комплексний захист інформаційно-комунікаційної інфраструктури національної безпеки держави від несанкціонованого втручання з боку державних, недержавних і транснаціональних кіберугрупувань, доступ до комп'ютерних мереж ймовірного супротивника та використання їх у власних інтересах через застосування новітніх ІТ-технологій силами професійних комунікаторів і фахівців із ведення інформаційної війни.

У структурі збройних сил країн створюють спеціальні підрозділи кібератак і кіберзахисту. Згідно з даними відкритих джерел та офіційними заявами, такі підрозділи сформовано у США (U. S. Cyber Command), Великобританії (Cyber Security Operations Centre при уряді Великобританії), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cybersecurity Operations Centre), Індії та інших державах. У 2014 р. уперше було повідомлено про власні кібервійська у РФ. На цей час, за даними розвідки США, над формуванням кібервійськ працюють майже у 30 країнах світу. У 2008 р. створено Спільний центр кібероборони НАТО у Таллінні (Естонія).

Основними засобами кібервійськ (так звана *кіберзброя)* є: електронні технології та засоби поширення електромагнітних випромінювань інформаційно-комунікаційної інфраструктури, інші матеріальні інфраструктури, що пов'язані із соціотехнічним простором і здатні створювати, модифікувати, зберігати й передавати інформацію (керувати її потоками), а також впливати на стан фізичних інфраструктур супротивника.

Скоординовані дії в інформаційній війні, масштабне застосування інформаційно-комунікаційних технологій у кіберпросторі вперше було здійснено під час підготовки та проведення військової операції "Союзницька сила" проти Югославії 24.03. — 10.06.1999. Уперше у практиці НАТО, за пів року до операції був створений спеціальний комітет, що координував дії союзників в інформаційному просторі в умовах проведення військової операції. Вперше було організовано широку інформаційну підтримку операції НАТО в інтернеті. У мережі розмістили майже 300 тис. сайтів, що певною мірою стосувалися проблеми Косово та військової операції Альянсу в Югославії. Більшість ресурсів розробили американські фахівці з комп'ютерних технологій, значно посиливши ефективність пропагандистської компанії. Також були визначені об'єкти потенційної інформаційної загрози — національні засоби масової інформації, система воєнно-політичного управління та зв'язку, що стали пріоритетними цілями для повітряно-вогневого придушення.

Одночасно загострилася боротьба за інформацію у цифрових системах. Хакери неодноразово проникали через інтернет у локальні обчислювальні мережі командувань і штабів об'єднаних збройних сил НАТО. Масові запити серверів в окремі періоди паралізували роботу електронної пошти, що можна вважати першою ефективною акцією із застосуванням інформаційної зброї [13, с. 247—249]. Дії югославських хакерів спровокували появу в теорії та практиці інформаційного протиборства поняття "кібератака".

Першим системним протиборством у кіберпросторі під час бойових дій слід вважати проведення інформаційно-психологічних операцій у грудні 2008 р. між Армією оборони Ізраїлю та рухом ХАМАС. Ізраїльтяни активно використовували спеціальні інтернет-портали для пропаганди потенціалу ізраїльської високоточної зброї, блокування радіо- й телесигналів у Секторі Газа та вогневе знищення телекомунікацій арабів. Члени ХАМАС за допомогою хакерських спільнот Марокко та Саудівської Аравії вже в січні 2009 р. зламали систему безпеки 10 тис. ізраїльських сайтів, що містили інформацію про події на Близькому Сході. Основною метою кібератак стала фальсифікація контенту електронних сторінок і переадресація трафіку низки ізраїльських інформаційних служб на вигадані електронні адреси.

Улітку 2009 р. хакери Азербайджану й Туреччини здійснили серію кібератак на вірменський сегмент інтернету, внаслідок чого було блоковано роботу урядових установ Республіки Вірменії [12, с. 11]. На початку липня 2009 р. хвиля кібератак, імовірно з території КНДР, тимчасово паралізувала роботу вебсайтів окремих державних установ Південної Кореї та США. Сталося це в період здійснення КНДР послідовної серії пусків балістичних ракет, посилення загальної дипломатичної напруженості через її ядерну програму й загрози введення відповідних санкцій із боку США й ООН. За даними газети "Вашингтон Пост" від 31.08.2013, упродовж 2011 р. проведено 231 комп'ютерну атаку, три чверті з яких було спрямовано на інформаційно-комунікаційні системи Росії, Ірану, КНР і КНДР. Основною метою кібератак було зараження вірусами комп'ютерних систем ядерних програм [1, с. 104]. 27 червня 2013 р. голова Об'єднаного комітету начальників штабів Збройних сил США адмірал М. Демпсі зазначив, що впродовж 2011—2013 рр. інтенсивність кібератак на інформаційно-комунікаційну структуру США зросла у 17 разів.

З метою мінімізації кіберзагроз від 2014 до 2017 р. адміністрація США планувала витратити на кібербезпеку 23 млрд дол. і збільшити штат відповідних структурних підрозділів до 4 тис. осіб [14, с. 105]. Реалії навіть перевершили ці плани, оскільки на 01.01.2017, за даними кампанії Zecurion, щорічні витрати США на кібербезпеку становили 7 млрд дол. на рік, а чисельність кібербійців — 9 тис. осіб [10].

Активну позицію з протидії кіберзагрозам обстоює й провідна міжнародна безпекова організація —

НАТО (Cooperative Cyber Defence Centre of Excellence). Інтенсифікація процесів створення кібервійськ країнами НАТО логічно висуває на перший план питання координації зусиль у межах цього військово-політичного блоку.

У червні 2010 р. група експертів під керівництвом М. Олбрайт запропонувала трактувати масштабні кібератаки як такі, що підпадають під п'яту статтю Північноатлантичного договору та вважаються атаками на всіх членів Альянсу [6, с. 4]. Отже, за даними агентства Reuters, "новий військовий командний центр НАТО з протидії комп'ютерним хакерам повинен бути повністю укомплектований до 2023 р.". До роботи у центрі планується залучити 70 експертів, які надаватимуть інформацію військовій розвідці про хакерів злочинних груп ворожих держав.

У липні 2016 р. на саміті НАТО у Варшаві кіберпростір визнано сферою операцій, аналогічною традиційним сферам військової взаємодії. У лютому 2017 р. ухвалено оновлений План кібероборони з визначенням орієнтирів опанування кіберпростору як нової сфери операцій. 8 листопада 2017 р. під час засідання НАТО на рівні міністрів оборони прийнято рішення про створення Центру кібероперацій [8].

Посилена увага до організації кібербезпеки та створення засобів ведення кібервійни ставить перед урядами держав завдання перегляду внутрішньої політики в кіберсфері та концепцій воєнної політики. Такі тенденції зумовлені зростанням випадків використання розвідувальними службами та спеціалізованими військовими підрозділами держави можливостей і технічних потужностей транснаціональних кримінальних груп, що спеціалізуються на сфері кіберзлочинності. Це спричиняє зміни в політиці провідних держав світу щодо застосування нормативно-правових механізмів обмеження й цензури як однієї з форм реалізації внутрішньої інформаційної політики. Отже, НАТО офіційно визнала кіберпростір новим рубежем, котрий слід захищати на одному рівні із сухопутним, повітряним і морським [9].

Висновки. У сучасній геополітичній ситуації для України життєво необхідним є усвідомлення урядом держави та суспільством надзвичайної важливості вивчення сутності та специфіки інформаційних воєн і створення дієвої системи національної безпеки, визнання історичної потреби захисту територіальної цілісності та недоторканності власного географічного й інформаційного просторів. Інформаційні війни стали аксіомою в сучасних міжнародних відносинах і дають змогу доволі ефективно, із залученням незначних фінансових і людських ресурсів, досягати цілей в усіх сферах суспільно-політичного життя. Ці війни ведуть з активним використанням інформаційної зброї, а стан захищеності інформаційного простору держави визначається рівнем її інформаційної безпеки.

Ураховуючи ступінь входження України до глобальних інформаційних систем, питання вивчення багатоаспектної проблеми кібербезпеки держави є *перспективним.* На наше переконання, слід зосередитися на проблемах удосконалення механізму взаємодії органів державного, військового управління та місцевого самоврядування щодо побудови єдиної системи кіберзахисту.

Список використаної літератури

1. *Американские* кибератаки // Зарубежное военное обозрение. — 2013. — № 9. — С. 104.
2. *Бурячок В. Л.* Інформаційна та кібербезпека: соціотехнічний аспект : підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа] ; за заг. ред. д-ра техн. наук, проф. В. Б. Толубка. — Київ : ДУТ, 2015. — 288 с.
3. *В информационной* войне превосходство в военной мощи не гарантирует от поражения. — Режим доступа: http://www.arms-expo.ru/049051124053053051052.html. — Загл. с экрана. — Дата обращения: 3.01.2020.
4. *Гнатюк С.* Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк // Безпека інформації. — 2013. — Т. 19. — № 2. — С. 118—129. — Режим доступу: http://www.nbuv.gov.ua/UJRN/bezin_2013_19_2_8. — Назва з екрана. — Дата звернення: 3.01.2020.
5. *Давыдов Д.* Информационные операции как средство достижения целей военно-политического руководства США / Д. Давыдов // Зарубежное военное обозрение. — 2013. — № 10. — С. 3—10.
6. *Дубов Д. В.* Кібербезпека: світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. — Київ : Вид-во НІСД, 2011. — 30 с.
7. *Еляков А.* Проблемы безопасности в современном мире. Компьютерный терроризм / А. Еляков // Мировая экономика и международные отношения. — Москва : Наука, 2008. — № 10. — С. 102—105. — Режим доступа: http://naukarus.com/kompyuternyy-terrorizm. — Загл. с экрана. — Дата обращения: 25.02.2020.
8. *Карасев П.* Кибервойска Европы и НАТО / П. Карасев // Expert Online. — 2019.20.02. — Режим доступа: http://expert.ru/2018/03/13/kibervojska-evropyi-i-nato/. — Загл. с экрана. — Дата обращения: 3.01.2020.
9. *Киберкомандование* НАТО полностью закончит формироваться в 2023 году // УКРИНФОРМ. — 16.10.2018. — Режим доступа: https://www.ukrinform.ru/rubric-technology/2559824-nato-sformiruet-sobstvennye-kibervojska-v-2023-godu.html. — Загл. с экрана. — Дата обращения: 3.01.2020.
10. *Лещев В.* Названы самые боеспособные страны в киберпространстве / В. Лещев // LIFE.RU. 10 января 2017. — Режим доступа: https://life.ru/p/957102. — Загл. с экрана. — Дата обращения: 25.02.2020.
11. *Манжай О. В.* Використання кіберпростору в оперативно-розшуковій діяльності / О. В. Манжай // Право і Безпека. — 2009. — № 4. — С. 215—219.
12. *Мелин А.* Особенности применения киберсредств в межгосударственных военных и внутренних конфликтах / А. Мелин // Зарубежное военное обозрение. — 2013. — № 3. — С. 11—17.
13. *Морозов Ю. В.* Балканы сегодня и завтра: военно-политические аспекты миротворчества / Ю. В. Морозов. — Москва, 2001. — С. 247—249.

14. *Председатель* КНШ ВС США о защите военных компьютерных сетей // Зарубежное военное обозрение. — 2013. — № 8. — С. 105.
15. *Присяжнюк М. М.* Особливості забезпечення кібербезпеки / М. М. Присяжнюк, Є. І. Цифра // Реєстрація, зберігання і обробка даних. — 2017. — Т. 19. — № 2. — С. 61—68. — Режим доступу: http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-arfare/article/115929/. — Назва з екрана. — Дата звернення: 3.03.2020.
16. *Geers K.* Cyberspace and the Changing nature of warfare. — Mode of access: http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-arfare/article/115929/. — Title from the screen. — Accessed: 3.03.2020.
17. *Gibson W.* Neuromancer / W. Gibson. — London : HarperCollins, 1994. — 271 p.
18. *Laqueur W.* Postmodern Terrorism / W. Laqueur // Foreign Affairs. — 1996. — № 75. — P. 35.

Ruslan Hula, Iryna Perederii, Olena Vitrynska

Military policy in cyberspace of leading world countries and military-political institutions concept

The globalization and modernization processes form a unique phenomenon of virtual information policy as a means for protecting the national interests in cyberspace. It is a task that requires a new and effective information policy as the latest information technologies appear to challenge the current order of things. In contemporary world, creating such a policy is a prerogative of developed states as the other players feel themselves under a continual threat of information colonialism. It appears to be an objective universal issue, caused by a number of complex processes, such as the presence of open or hidden information aggression in the modern information and political space, complicated by globalization that tends towards integration and unification of the world. This manifests itself in a variety of forms and consequences of information confrontation that affects the forming of a new social model the main subject of which is the information society.

The authors separate the concept of cyberspace as a particular object of scientific study. It is examined as a non-linear complex category for a complex socio-political phenomenon. The development of information and communication technologies in the global information space has objectively conditioned the necessity to establish the system of integral cyber power and means application in military actions.

The main objective of the paper is to analyze the main tendencies in military policy of the developed countries and military-political institutions in cyberspace with respect to constructing of an effective system of counteraction to cyber threats in the global information space and the means of cyber warfare. The authors also endeavour to provide the definition of the content and essence of cyberspace as a testing area for the latest technologies within the context of information war.

Keywords: *informative war; cyberwar; cybersafety; cyberattacks; cybertroos; national safety; block of NATO; cyberspace*

References

1. Amerikanskie kiberataki (2013). *Zarubezhnoe voennoe obozrenie*, 9, p. 104.
2. Buryachok V. L., Tolubko V. B., Horoshko V. O., Tolyupa S. V. (2015). *Informacijna ta kiberbezpeka: sociotehnichnij aspekt*. Kyiv: DUT.
3. *V informacionnoj vojne prevoshodstvo v voennoj moshi ne garantiruet ot porazheniya* (2020). Available at: http://www.arms-expo.ru/049051124053053051052.html.
4. Gnatyuk S. (2013). Kiberterorizm: istoriya rozvitku, suchasni tendenciyi ta kontrzahodi. *Bezpeka informaciyi*, 19 (2), pp. 118—129. Available at: http://www.nbuv.gov.ua/UJRN/bezin_2013_19_2_8.
5. Davydov D. (2013). Informacionnye operacii kak sredstvo dostizheniya celej voenno-politicheskogo rukovodstva SShA. *Zarubezhnoe voennoe obozrenie*, 10, pp. 3—10.
6. Dubov D. V. (2011). *Kiberbezpeka: svitovi tendenciyi ta vikliki dlya Ukrayini*. Kyiv: Vid-vo NISD.
7. Elyakov A. (2008). Problemy bezopasnosti v sovremennom mire. Kompyuternyj terrorizm. *Mirovaya ekonomika i mezhdunarodnye otnosheniya*, 10, pp. 102—105. Available at: http://naukarus.com/kompyuternyy-terrorizm.
8. Karasev P. (2019). Kibervojska Evropy i NATO. *Expert Online*. Available at: http://expert.ru/2018/03/13/kibervojska-evropyi-i-nato/.
9. *Kiberkomandovanie NATO polnostyu zakonchit formirovatsya v 2023 godu*. (2020). Available at: https://www.ukrinform.ru/rubric-technology/2559824-nato-sformiruet-sobstvennye-kibervojska-v-2023-godu.html.
10. Leshev V. (2020). *Nazvany samye boesposobnye strany v kiberprostranstve*. Available at: https://life.ru/p/957102.
11. Manzhaj O. V. (2009). Vikoristannya kiberprostoru v operativno-rozshukovij diyalnosti. *Pravo i Bezpeka*, 4, pp. 215—219.
12. Medin A. (2013). Osobennosti primeneniya kibersredstv v mezhgosudarstvennyh voennyh i vnutrennih konfliktah. *Zarubezhnoe voennoe obozrenie*, 3, pp. 11—17.
13. Morozov Yu. (2001). V. *Balkany segodnya i zavtra: voenno-politicheskie aspekty mirotvorchestva*. Moskva.
14. Predsedatel KNSh VS SShA o zashite voennyh kompyuternyh setej. *Zarubezhnoe voennoe obozrenie*, 8, p. 105.
15. Prisyazhnyuk M. M., Cifra Ye. I. (2017). Osoblivosti zabezpechennya kiberbezpeki. *Reyestraciya, zberigannya i obrobka danih*, 19 (2), pp. 61—68. Available at: http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-arfare/article/115929/.
16. Geers K. (2020). Cyberspace and the Changing nature of warfare. Available at: http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-arfare/article/115929/.
17. Gibson W. (1994). *Neuromancer*. London: HarperCollins.
18. Laqueur W. (1996). Postmodern Terrorism. *Foreign Affairs*, 75, p. 35.

Надійшла до редакції 19 березня 2020 року