Братіна Д.*

«КІБЕРВІЙНА» В ГЕОПОЛІТИЦІ

Кіберпростір офіційно визнали «полем бою», таким же як суходіл, море, повітряний простір або космос. Автор статті аналізує сучасні концепції «кібервійни», висвітлює проблеми кібербезпеки на міжнародному рівні та здійснює огляд основних підходів у цій сфері

Ключові слова: кібервійна, кіберпростір, кібербезпека, кіберзагрози, геополітика.

Киберпространство официально признали «полем боя», таким как суша, море, воздушное пространство или космос. Автор статьи анализирует современные концепции «кибервойны», освещает проблемы кибербезопасности на международном уровне и осуществляет обзор основних подходов в этой сфере.

Ключевые слова: кибервойна, киберпространство, кибербезопасность, киберугрозы, геополитика.

Cyber space has been officially recognized the same «battlefield» as land, sea, air or space. The author examines the current concepts of «cyberwar», highlights the challenges of cyber security on the international level and provides an overview of the main approaches in this field.

Key words: cyberwar, cyberspace, cybe security, cyberthreats, geopolitics.

В епоху інформаційної революції для досягнення цілей війни, упокорення «ворога» необов'язковою є безпосередня окупація, масове введення військ або захоплення територій. Збройні дії й величезні військові витрати зовсім необов'язкові. Більш дешевою й гнучкою є зброя «Мережі», яка маніпулює насильством і воєнними чинниками тільки в крайніх випадках. «Мережа» – це той новий четвертий простір – інформаційний простір «після трьох традиційних – суходолу, моря й повітря, у якому й розгортаються основні стратегічні операції розвідувального і військового характеру, а також здійснюється їх медійний, дипломатичний, економічний й технічний супровід (забезпечення)» [1, p. 48–50].

Основні результати війни у вигляді упокорення «ворога» досягаються шляхом впливу на широку сукупність факторів – інформаційних, соціальних, когнітивних і т.д. Зміст воєнної реформи в рамках «нової теорії війни» інформаційної епохи полягатиме, таким чином, у створення потужної й всеосяжної «Мережі», що концептуально замінить раніше існуючі моделі й концепції військової стратегії, інтегрує їх у єдину цілісну систему.

Мета даної статті – окреслити сучасні концепції «кібервійни», забезпечення кібербезпеки на міжнародному рівні та зробити огляд основних підходів у цій сфері. Аналіз сучасних поглядів на характер воєнних дій та політики держав щодо кібербезпеки дозволяє, в значній мірі, внести визначеність в геополітичну ситуацію і понизити чинник ризику.

---

* здобувач кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Науковий керівник: проф. Макаренко Є.А

Одним із поштовхів до вивчення поняття «інформаційна війна» стало введення в 1990 р. у документи Міністерства оборони США терміну «Information / Cyber war», що потім було впроваджено у наукові праці [2]. Нині накопичено значний досвід наукових досліджень в сфері державної інформаційної політики, інформаційного протиборства й інформаційно-психологічних воєн [3–10].

Інформаційні технології, будучи значною мірою продуктом перегонів озброєнь по лінії США – СРСР, змінили погляди на характер воєнних дій, завдання військового будівництва, що особливо характерно для періоду після закінчення «холодної війни». Реакція США на сучасні виклики міжнародній безпеці стосується саме превентивного контролю, спрямована на ліквідацію тих зон, які можуть бути основою для планування і здійснення терористичних атак на центри глобального впливу й влади.

Концепція «кібервійни» була достатньо випробувана в антитерористичних кампаніях в Афганістані (після 2001 р.) і в Іраку (після 2003 р.) й припускала створення нечисельних мобільних збройних сил, оснащених передовою технікою, здатних досягти всеосяжної переваги над будь-яким супротивником без застосування зброї масового ураження.

Концепція «інформаційної війни» США справді побудована на уявленнях про можливість ведення воєнних дій малими силами, які можуть бути децентралізованими і ретельно замаскованими, що істотно ускладнює виявлення і знищення зазначених бойових сил. Кібервійна – це війна без кордонів, а атаки в ній можуть вестися як з території нападаючого, так і з зовсім інших, не суміжних, територій. Хоча досі США, за офіційними даними, не проводили масштабних стратегічних кібератак, а у військових нібито немає президентської директиви, за яких обставин можна застосовувати такі атаки, хто буде їх санкціонувати і проводити, по яких цілях можна буде завдавати удари, подібні твердження можна піддати сумніву.

Останнім часом термін «кібервійна» набуває політизації та дедалі частіше використовується високопосадовцями США, в тому числі в офіційних виступах і документах [11–14]. У більшості випадків під ним розуміються або систематичні напади на інформаційну інфраструктуру, або сукупність кібератак на інформаційні мережі (об'єкти критичної інфраструктури) держави . На цьому тлі актуалізуються спроби визначити кібервійну як форму класичної війни з відповідними наслідками та можливостями для військових організацій (включно з превентивним нападом, можливістю відповіді кінетичною зброєю на кібернапад тощо). Це означає гарантовані зобов'язання міністерства оборони США щодо можливості застосуванням особливих підходів до стримування супротивників у всіх основних сферах і, зокрема, й у кіберсфері.

Особливу увагу в зв'язку з цим викликає питання про роль збройних сил у забезпеченні цивільної інформаційної безпеки. Ще наприкінці другого терміну правління адміністрація Дж. Буша-молодшого робила спроби створити єдину систему державного забезпечення інформаційної безпеки під військовим командуванням. Значна частина цієї ініціативи була засекречена, а сама спроба створити військове кіберкомандування виявилася невдалою. Адміністрації Б. Обами вдалося завершити ці ініціативи і вже у червні 2009 р. було оголошено про створення військового кіберкомандування, основною метою якого стала протидія інформаційним загрозам національній безпеці США.

Важливим кроком у формування національної системи кібербезпеки стало ухвалення у травні 2011 р. «Міжнародної стратегії розвитку кіберпростору» [11], у якій викладено не тільки основні підходи до розуміння сучасної глобальної американської політики, але й представлено нові офіційні позиції Сполучених Штатів з питань інформаційної безпеки. У Стратегії також підтверджено лідерські позиції США в інформаційному розвитку, інформаційний потенціал сприймається американським політичним керівництвом як стратегічний ресурс . Впадає в око й сама назва документу – «міжнародна стратегія», що вочевидь демонструє клю-

чові зміни у американській політиці у сфері забезпечення інформаційної безпеки, тобто її зорієнтованість на міжнародне співробітництво і глобальний масштаб діяльності.

Вперше в офіційному американському документі, присвяченому питанням кіберпростору, використовується й формулювання «колективна безпека». У розділі, присвяченому військовим питанням кібербезпеки, автори стратегії наголошують на необхідності розвивати військово-політичне співробітництво для забезпечення колективної безпеки та протидії кіберзагрозам. Інститути колективної безпеки, такі як НАТО, дозволять використовувати фактори стримування проти держав і недержавних акторів в інформаційному просторі. Показово, що подібну ідею висловлювала держсекретар США Г. Клінтон у своїй промові, присвяченій конфлікту між Google і Китаєм. На початку 2010 року вона заявила, що «країни або окремі громадяни, причетні до інформаційних атак, повинні понести суворе покарання і міжнародний осуд, Інтернет об'єднує практично весь світ, атака на Мережу однієї держави може бути атакою на всіх» [12].

Отже, «Міжнародна стратегія розвитку кіберпростору» підтверджує прагнення Сполучених Штатів адаптуватися до поліцентричної системи міжнародних відносин. У новому світі, що формується, США бачать себе як центр сили, що володіє потужним інформаційним потенціалом, який формується за рахунок плідної співпраці між державою, бізнесом та суспільством.

У липні 2011 р. було оприлюднено нову стратегію кібербезпеки США «Стратегію Міністерства оборони США у сфері кіберпростору» [13]. Напередодні представлення Стратегії заступник голови Пентагону У. Лінн заявив, що внаслідок останньої кібератаки на комп'ютерну мережу відомства у травні 2011 р. хакерам вдалося вкрасти 24 тис. документів імовірно на замовлення розвідслужб іншої держави [14].

Всесвітня мережа тепер офіційно визнана «полем бою», таким же як суша, море, повітряний простір або космос. Заступник голови Пентагону також зазначив, що наступальний потенціал в сфері кібернетичних воєн обганяє найкращі засоби оборони. Найбільш ефективною зброєю володіють поки що лише держави, а не терористичні угруповання. «Хоча встановлення джерела кібератаки може виявитися складним завданням, ризик виявлення і відповідних дій для великої країни все ж занадто великий, щоб ризикувати і проводити деструктивні атаки проти Сполучених Штатів.

Стратегія Міністерства оборони передбачає реалізацію п'ятьох стратегічних ініціатив:

1) визначення кіберпростору як самостійної галузі, поля оперативної діяльності;

2) використання тактики «активного захисту»;

3) координація дій з міністерством внутрішньої безпеки щодо стратегічно важливих та інфраструктурних мереж;

4) співробітництво у галузі кібербезпеки з партнерами і союзниками;

5) протидія кібертерористичним атакам через глобальну мережу.

За словами У. Лінна, стратегія передбачає такі джерела кіберзагроз: зовнішні загрози, вплив з боку осіб усередині США, уразливість засобів зв'язку, передачі інформації в збройних силах, які можуть підірвати її боєздатність. У Пентагоні упевнені, що інші держави «працюють над проникненням до секретних і несекретних мереж Міністерства оборони США, а деякі іноземні розвідки вже мають можливість порушувати елементи нашої інформаційної структури». Є небезпека кібератак і з боку неурядових організацій і приватних компаній.

Слід підкреслити, що напередодні офіційного представлення документу з'явилися повідомлення у ЗМІ, зокрема, The Wall Street Journal, про те, що у новій кіберстратегії США буде міститися пункт про те, що кібератака, яка призвела до людських жертв, буде прирівняна до оголошення війни. Але в офіційному тексті Стратегії та виступах представників Пентагону не було озвучено такий радикальний крок. Хоча за словами У. Лінна, США «залишають за собою право, відповідно до законів війни, відповісти на серйозні кібератаки пропорційним і спра-

ведливим чином в той час і в тому місці, які ми виберемо». Зрозуміло, що таке розпливчасте формулювання дозволить США застосувати і реальні військові кроки, для дій проти віртуального ворога. На тій підставі , що до останнього часу більшість загроз критично важливій інфраструктурі інформаційно розвинених держав (США, Великобританія, Німеччина) надходили не від поодиноких терористичних груп, що просто змінили тактику ведення своєї боротьби, а від спеціально підготовлених, інформаційно та матеріально забезпечених спеціалізованих груп, що функціонують в інтересах тих чи інших держав і є фактично продовженням їх «воєнної машини».

Військова доктрина Китаю виражена в стратегії «активної оборони», суть якої в тім, що Китай не нападе першим, поки проти нього не здійснять агресію, однак у випадку нападу відповість контрударом. При цьому в застосуванні військової чинності передбачаються гнучкість і координація такого кроку з заходами політичного, економічного й дипломатичного характеру.

Китайське керівництво як і раніше відносить Сполучені Штати до числа своїх головних супротивників і не виключає можливості збройного зіткнення з ними більшого або меншого масштабу, а тому в ході реформ наполегливо шукає шляхи так званого «асиметричного будівництва збройних сил» для того, щоб уже в найближчому майбутньому армія могла адекватно відповісти на можливі дії американців. Так, зокрема, Китай уже давно розробляє доктрину «інформаційної війни» і досить далеко просунувся в цьому напрямку.

Інформаційну війну китайські офіційні документи визначають як «перехід від механізованої війни індустріального суспільства до війни рішень і стилю керування, війні знання й війні інтелекту» [15]. У рамках цієї доктрини китайські збройні сили розвивають концепцію «Мережевих сил» – військових підрозділів чисельністю до батальйону, укомплектованих висококласними фахівцями, що володіють передовими комп'ютерними технологіями.

У доповіді ФБР (січень 2010 р.) щодо розвитку кібервійськ КНР та спричинених ними загроз національній безпеці США [16], КНР названа «найбільшою цілісною загрозою США у сфері кібертероризму» та силою, яка наразі уже володіє потенціалом, що дозволяє «знищувати життєво важливу інфраструктуру, отримувати доступ до банківських, комерційних, військових та оборонних баз даних».

За даними Доповіді, КНР має наразі армію у 180 000 хакерів, що здійснюють постійні атаки на кібермережі США (лише в 2009 році проти комп'ютерів Міністерства оборони США було здійснено 90 000 таких атак. За даними ФБР від загального числа 180 тис. кібершпигунів 30 тис. є військовими, а 150 тис. – комп'ютерними експертами з приватного сектору, місією яких є отримання доступу до військових та комерційних секретів США та внесення розладу в діяльність урядових та фінансових служб.

КНР ставить за мету створити до 2020 р. «найбільш інформатизовану» армію у світі. Основною інформаційною зброєю китайських хакерів є «шкідники» (malicious), – заражені комп'ютерні коди [17]. Вже у 2009 р. компанії, що здійснюють діяльність в енергетичній, банківській, аерокосмічній та телекомунікаційній сферах, мали суттєві проблеми із китайським «шкідливим» комп'ютерним кодом. Причому персонал компаній не своєчасно зрозумів масштаби та загрозу атак, що розпочались ще у 2008 р., і попередили ФБР про ці атаки лише на початку 2009 р.

Тим часом китайські хакери, які використали принципово нові типи вірусів, що не визначались жодним спеціальним антивірусним програмним забезпеченням, отримали доступ до найважливішої комерційної інформації включно з результатами розвідок територій, електронним листуванням топ-менеджерів компаній тощо. Останньою наразі ефективною атакою хакерів, здійсненого, за версією Міноборони США, спецпідрозділами Північної Кореї за безпосередньої підтримки хакерів з КНР, є викрадення з комп'ютерів міністерства оборони Південної Кореї оперативних планів розгортання американських військ на території півострова у випадку конфлікту з КНДР.

Звичайно, справжні масштаби кібератак набагато серйозніші. Те, що оприлюднюють медіа, є незначними витоками чутливої інформації, покликаної привернути увагу громадськості до даної проблеми, щоб організувати лобіювання в Конгресі прийняття дедалі дорожчих програм кіберзахисту. Центр стратегічних міжнародних досліджень, більш відомий як Центр З. Бжезинського (The Center for Strategic and International Studies) підготував для програмний документ в сфері інформаційної безпеки («Securing Cyberspace for the 44th Presidency» [18]), у якому робиться заява, яка сильно зближує позиції США й РФ. Інформаційна безпека розцінюється у зазначеному документі як «стратегічне питання, яке має розглядатися нарівні з питанням щодо зброї масового ураження й «глобального джихаду».

Водночас із посиланням на заяву анонімного відповідального працівника Держдепартаменту США, зроблену напередодні візиту Б. Обами до Москви, повідомлялося, що США й РФ нібито близькі до порозуміння в справі обмеження «інформаційної зброї» як зброї масового ураження [19].

Росія пропонує підписати міжнародну угоду, за якою країни світу відмовляться від закладки в комп'ютерне обладнання або програмне забезпечення різноманітних кодованих пристроїв типу «логічних бомб» які можуть бути активовані у разі виникнення війни. Росіяни пропонують також встановити міжнародний орган, відповідальний за безпеку Інтернету, на що американці заперечують, що такий орган займатиметься в Інтернеті цензурою на догоду тоталітарним політичним режимам [20].

У 2010 р. ухвалено нову Воєнну доктрину РФ [21], якою визначено, що комплексне застосування воєнної вили та сил і засобів невійськового характеру є характерною рисою сучасних воєнних конфліктів. До особливостей сучасних конфліктів Доктриною віднесено завчасне проведення заходів інформаційного протиборства з метою досягнення політичних цілей без застосування військової сили, а у подальшому – в інтересах формування сприятливої реакції світової спільноти на застосування воєнної сили. Зазначений документ також визначає одним із завдань РФ по стримуванню та попередженню воєнних конфліктів нейтралізацію можливих воєнних небезпек та воєнних загроз політичними, дипломатичними та іншими невоєнними засобами.

Отже, проведення інформаційно-психологічних операцій структурами РФ на стратегічному рівні планується здійснити задовго до початку вторгнення у формі таємної війни: забезпечити прихований контроль над інформаційними ресурсами противника, дестабілізацію внутрішньополітичного стану, активізувати діяльність опозиційних сил, досягти розвалу чи дискредитації Збройних Сил та інших силових структур, викликати недовіру народу до керівництва держави.

Прогнозується, що неможливість США забезпечити власне лідерство в сфері інформаційно-комунікаційних технологій та їхня вразливість до чисельних кібернападів у уже в короткотерміновій перспективі змусить їх піти на поступки РФ в питаннях укладання договору з міжнародної інформаційної безпеки, який прирівняє інформаційну зброю до зброї масового ураження та заборонить на рівні міжнародного права її подальше поширення. Зростаюча активність прибічників «радикального» підходу до кібератак (коли вони розуміються як «акт війни» з відповідними наслідками) дозволяє припустити, що тема кібератак і кібервійни в подальшому перебуватиме у центрі уваги дискусій світових геополітичних гравців.

Втім міжнародне співтовариство досі не напрацювало взаємопогодженого набору принципів, правил і норм, що регулювали б на міжнародному рівні інформаційну безпеку і відповідно прийнятний порядок здійснення воєнних операцій у кіберпросторі, а також можливість зберігати нейтралітет (статус невтручання у перебіг воєнних дій), як це прийнято в традиційних війнах.

Існування загроз національній безпеці України в інформаційній сфері було вперше визнано в Концепції (Основах державної політики) національної безпеки України схваленій Вер-

ховною Радою України у січні 1997 р. [22]. Наступним кроком уперед став Закон України «Про основи національної безпеки України» [23], який відповідно до пункту 17 частини першої статті 92 Конституції України (254к/96-ВР) визначив основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Відповідно до зазначеного Закону згодом були розроблені і затверджені Президентом України три принципово важливих документи: Стратегії національної безпеки України (від 12 лютого 2007 року, № 105/2007); Воєнна доктрина України (від 15 червня 2004 року, N648/2004), Доктрини інформаційної безпеки України (від 08 липня 2009 року, № 514/2009). [24 – 26]. Важливість трьох зазначених документів й, зокрема, Стратегії національної безпеки України і Воєнної доктрини України полягає передусім у тому, що вони є підґрунтям для опрацюванням у подальшому низки спеціалізованих доктрин, концепцій, стратегій і програм, якими визначаються цільові настанови та керівні принципи воєнного будівництва, а також напрями діяльності органів державної влади в конкретній обстановці з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз національним інтересам України.

Серед загроз в інформаційній сфері Стратегія національної безпеки України виокремлювала такі як:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Відповідно, основними завданнями в інформаційній сфері Стратегія визначила:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Особливої оцінки заслуговує Доктрина інформаційної безпеки України [24], яка вперше визначила загрози національній безпеці держави у воєнно-інформаційній сфері, до яких віднесла:

- порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;

• несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;

• реалізація програмно-математичних заходів з метою порушення функціонування інформаційних систем у сфері оборони України;

• перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;

• інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби.

Досить конкретними є намічені Доктриною інформаційної безпеки заходи забезпечення воєнно-інформаційної безпеки:

• проведення систематичного аналізу застосування засобів, форм та способів інформаційної боротьби у воєнній сфері, визначення напрямів забезпечення інформаційної безпеки держави;

• удосконалення законодавства з питань інформаційної безпеки, координації діяльності органів державної влади та органів військового управління під час вирішення завдань забезпечення інформаційної безпеки;

• удосконалення видів і засобів захисту інформації в інформаційно-телекомунікаційних мережах, що задіяні в управлінні військами і зброєю, від несанкціонованого доступу;

• удосконалення форм і способів протидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності держави;

• підготовка спеціалістів з питань інформаційної безпеки у воєнній сфері.

Разом з тим прийняті за останні роки закони, укази Президента України та нормативно-правові акти Кабінету Міністрів України не забезпечують в правовому і організаційному плані формування і розвиток цілісної системи державного управління та захисту інформаційних ресурсів. Лише фрагментарно і ситуаційно передбачають вирішувати згадані проблеми і проекти актів законодавства, що розробляються або перебувають на розгляді у Верховній Раді України (включно з проектами Інформаційного кодексу України та проектом Закону України «Про національні інформаційні ресурси».

Основним напрямом бойового застосування засобів ведення інформаційної війни є підвищення їх ефективності за рахунок масованого застосування різних інформаційних засобів та об'єднання їх в єдину інтегровану систему, яка буде забезпечувати мінімальний цикл управління:

• виявлення об'єктів ураження;

• пригнічування та дезорганізацію роботи систем управління військами і бойовими засобами;

• наведення власних засобів ураження на виявлені об'єкті противника.

Усе зазначене потребує об'єднання інформації, яка надходить від різних засобів ведення інформаційної війни, в єдиний банк даних.

Отже, йдеться про створення в ЗС України інтегрованої системи, в якій застосування усіх засобів ведення інформаційної війни та розподіл завдань між ними будуть здійснюватись в загальних інтересах, з єдиною метою та у реальному масштабі часу, що є основним завданням у майбутніх війнах.

У світлі глобальних інформаційних загроз сучасності Україна виглядає значно менш захищеною від їх впливу, ніж високорозвинуті країни світу. Досі в Україні жодного разу не проводились комплексні навчання з проблеми кібербезпеки (на кшталт навчань «Кіберштурм», що проводяться в США) із залученням всіх відомств, задіяних у системі забезпечення кібербезпеки держави.

При цьому слід враховувати, що Україна через своє геополітичне положення є об'єктом пильної уваги з боку розвинених країн щодо реалізації їхніх геополітичних та інших інтересів.

України, яка офіційно проголосила прагнення набути позаблокового статусу, може стати жертвою кібернападів у разі гострого зіткнення протиборчих військових сил чи блоків. В таких умовах Україна має бути готова не лише до ведення оборонних воєн, а й активно створювати власні наступальні засоби ведення війни в кіберпросторі.

Як пряму загрозу своїй незалежності Україна трактує будь-які спроби виключення її з міжнародного процесу прийняття рішень, і не може вітати новий перерозподіл сфер впливу у геостратегічному просторі, що склався наприкінці XX століття. Україна виходить з того, що однією з найважливіших гарантій її суверенного розвитку та підтримання системи колективної безпеки в європейському та трансатлантичному просторі є розвинена кооперація у політичній, економічній, гуманітарній, інформаційній та військовій сферах. Підгрунтя такого співробітництва створюють процеси глобалізації, а також посилення тенденцій взаємовпливу, необхідність узгодження позицій усіх зацікавлених сторін у ситуаціях можливого застосування військової сили з метою стримування супротивників у всіх основних сферах і, зокрема, й у кіберпросторі.

Список використаних джерел

1. Alberts D.S. Network Centric Warfare [text]: / D.S. Alberts / Washington. DC, CCRP Pub. Series, – 2000. – 284 p.
2. Жуков В. Взгляды воєнного руководства США на ведение информационной войны [текст]: / В. Жуков // Зарубежное военное обозрение. – 2001. – № 1. – С. 2-9.
3. Міжнародна інформаційна безпека: сучасні виклики та загрози / [Макаренко Є.А., Гондюл В.П., Рижков М.М. та ін.]. – К.: Центр вільної преси, 2006. – 916 с.
4. Макаренко Є.А. Міжнародні інформаційні відносини / Є.А.Макаренко. – К.: ННК, 2002. – 474с.
5. Почепцов Г. Психологические войны / Г.Почепцов – М.: Омега-Л, 2008. –528 с.
6. Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: Монографія / О.В.Литвиненко – К.: НІСД, 2003. – 239 с.
7. Соснін О.В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України / О.В.Соснін. – К.: Інститут держави і права ім. В.М.Корецького НАН України, 2003. – 572 с.
8. Ліпкан В.А.Інформаційна безпека України в умовах євроінтеграції: навч. посібник / В.А.Ліпкан, Ю.Є.Максименко, В.М.Желіховський. – К.: КНТ, 2006. – 280 с.
9. Панарин И.Н. Информационная война и дипломатия / И.Н. Панарин. – М.: Городец, 2004. –528 с.
10. Информационные вызовы национальной и международной безопасности / [И.Ю.Алексеева и др.]; Под общ. ред. А.В.Федорова, В.Н.Цыгичко. – М.: ПИР-Центр, 2001. – 328 с.
11. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. May 2011. [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
12. США считают критически важным неограниченный и безопасный доступ в интернет [Електронний ресурс]. – Режим доступу: http://iipdigital.usembassy.gov/st/russian/article/2010/01/20100119170045esnamfuak0.6832544.html#axzz1pedKA3hg.
13. Department of Defense Strategy for Operating in Cyberspace [Електронний ресурс]. – Режим доступу: www.defense.gov/news/d20110714cyber.pdf.
14. Lynn K.P. Cyber Strategy's Thrust is Defensive [Електронний ресурс] / Karen Parrish Lynn. – Режим доступу: http://www.defense.gov/news/newsarticle.aspx?id=64682.
15. Дежин Е.Н. Информационная война по взглядам китайских военных аналитиков [текст]: / Е.Н. Дежин // Военная мысль. – 1999. – № 6. – С. 73-76.

16. National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow [electronic resource]: // Access mode: http://www.globalsecurity.org/military/library/policy/dod/d20050318nms.pd f. – Title from the screen.
17. Леонов О.В. Інтернет як інструмент ведення кібернетичної війни [текст]: / О.В. Леонов // Стратегічна панорама. – 2002. – № 3. – С. 122-127.
18. Securing Cyberspace for the 44 Presidency [electronic resource]: // Access mode: http://csis.org/files/media/csis/pubs/081208_securing cyberspace_44.pdf – Title from the screen.
19. Россия убеждает США запретить кибероружие [электронный ресурс]: / Режим доступа: http://защита-информации.8и/поуо8гі-і-sobytiya/rossiya-ubezhdaet-ssha-zapretit-kiberoruzhie – Название с экрана.
20. У США и России имеются разногласия по договору о киберпространстве [электронный ресурс]: // Режим доступа: http://www.inosrm.m/worloV20090629/250205.html?id= – Название с экрана.
21. Указ Президента Российской Федерации от 5 февраля 2010 г. № 146 «О Военной доктрине Российской Федерации» [электронный ресурс]: Режим доступа: http://news.kremlin.ru/ref_notes/461 – Название с экрана.
22. Про концепцію (Основи державної політики) Національної Безпеки України 16 січня 1997 року. Постанова Верховної Ради України // Відомості Верховної Ради (ВВР), 1997, № 10, ст. 85.
23. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – С. 351.
24. Указ Президента України «Про Доктрину інформаційної безпеки України» № 514/2009 від 08.07.2009 р. // Офіційний вісник України. -2009. – №52 . – С. 1783.
25. Указ Президента України «Про Стратегію Національної безпеки України» № 105/2007 від 12.02.2007 р. // Стратегічна панорама. – № 1. – 2007. – С. 5-12.
26. Указ Президента України «Про Воєнну доктрину України» N648/2004 від 15.06.2004 р. // Офіційний вісник України.- 2004.- № 30, ч.І. – Ст. 2005.