УДК 355.4

Є. О. Архипова,
к. філос. н., доцент кафедри теорії та практики управління, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ

ТЕОРЕТИЧНА СУТНІСТЬ ТА ПРАКТИКА ВИКОРИСТАННЯ АСИМЕТРИЧНОЇ ВІДПОВІДІ В УМОВАХ ГІБРИДНОЇ АГРЕСІЇ

Ye. Arkhypova,
PhD in Philosophy, Associate Professor of the Department of Theory and Practice of Management,
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv

THE THEORETICAL ESSENCE AND EXPERIENCE OF ASYMMETRIC RESPONSE IN TERMS OF HYBRID AGGRESSION

У статті розкрито сутнісні характеристики асиметричної відповіді, за допомогою якої слабша сторона може одержати перемогу у боротьбі з сильнішим супротивником. Наведені історичні та сучасні приклади асиметричних відповідей в рамках гібридної війни та асиметричних стратегій, зокрема відповідь Радянського Союзу на програму протидії "Стратегічній оборонній ініціативі" Р. Рейгана та елементи асиметричної відповіді у військово-політичній стратегії сучасної Японії.

Показано, що асиметрична відповідь в умовах гібридної війни передбачає використання як військових, так і невійськових методів: політичних, інформаційних, дипломатичних, економічних та пропагандистських. Серед невійськових методів можна, зокрема, назвати залякування протилежної сторони, провокування її на неспівмірні економічні витрати, спонукання на односторонні поступки.

Окрему увагу зосереджено на таких видах асиметричної відповіді, як інформаційна та кібернетична. Проведено розмежування термінів інформаційний та кібернетичний (простір, зброя, атака тощо). Розкрито особливості використання сучасних мас-медіа в гібридній війні. Проаналізовано досвід використання кіберпростору та кіберзброї в сучасних конфліктах. Досліджено перспективи використання кіберпростору в умовах україно-російського протистояння. Підкреслено, що кібернетичний вектор для нашої держави є одним із найперспективніших векторів асиметричної відповіді агресору.

The paper disclosed the essential characteristics of an asymmetric response, through which the weaker side may obtain a victory in the fight against a stronger opponent. Presented the historical and contemporary examples of asymmetric responses in the framework of hybrid warfare and asymmetric strategies, in particular the response of the Soviet Union to the program of counteraction to the Strategic Defense Initiative of R. Reagan and asymmetric response elements in the military and political strategy of modern Japan.

It is shown that the asymmetric response in terms of hybrid warfare involves the use of both military and non-military methods: political, informational, diplomatic, economic and propaganda. Among non-military methods may be called, in particular, intimidating the other side, provoking it to incommensurable economic cost, prompting unilateral concessions.

Special attention is focused on these types of asymmetric responses as information and cyber-response. Given a distinction between the terms "information" and "cybernetic" (space, weapons, attack, etc.). It is shown the features of the use of modern media in the hybrid war. It is analyzed the experience of use the cyberspace and cyberweapon in modern conflicts. investigated the prospects use of cyberspace in terms of Ukraine-Russia conflict. Emphasized that cyber vector for our country is one of the most promising vectors of asymmetric response to aggressor.

Ключові слова: асиметрична відповідь, гібридна війна, кібернетична зброя, кібернетична відповідь, протистояння, збройний конфлікт.

Key words: asymmetric response, hybrid warfare, cyber weapons, cyber response, opposition, armed conflict.

ПОСТАНОВКА ПРОБЛЕМИ

У сучасних умовах, коли триває протистояння із більш потужною країною (в плані матеріальних, фінансових та людських ресурсів), наша країна повинна застосовувати методи, які дозволяють більш слабким державам успішно протидіяти агресивній поведінці інших, могутніших країн. Мова йде про взяття на озброєння стратегії асиметричної відповіді, яка

дозволяє слабшій стороні отримати перевагу над більш сильною стороною конфлікту. Тактика асиметричної відповіді застосовується для виснаження та завдання суттєвої шкоди сильнішій стороні, при цьому можуть використовуватися всі можливі інструменти впливу не лише у тій площині, в якій діє супротивник.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Події останніх років спричинили посилення уваги науковців та практиків до проблематики гібридної війни. Так, окремі аспекти гібридних воєн, гібридних конфліктів, асиметричних методів боротьби висвітлювали такі вчені, як М. Айшервуд, Р. Барнсбі, В. Власюк, А. Демидов, Ю. Климчук, Є. Магда, Дж. МакКуен, П. Мансур, Л. Савін, А. Соловйов, Ф. Хоффман, Ш. Рівс. Тим не менше, питання асиметричної відповіді досі залишається малодослідженим.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Незважаючи на те, що термін "асиметрична відповідь" увійшов до наукового вжитку порівняно нещодавно, самій ідеї стосовно того, що успіх тієї чи іншої битви не обов'язково визначається розміром та потужністю війська, вже дві з половиною тисячі років. Так, військовий стратег Сунь-Цзи (IV ст. до н.е.) вважав, що для перемоги над чисельнішим військом достатньо уразити його за найбільш критичними напрямами. Елементами асиметричної стратегії можна вважати і давні методи ведення війни, згадані Н. Попеску: отруєння криниць та дача хабара за відкриття брами замку [13].

Окремі елементи асиметричного підходу активно використовувалися Німеччиною в XIX-му — першій половині XX ст. у протистоянні з Великобританією та США, оскільки бюджет Німеччини, який суттєво поступався бюджетам цих країн, не дозволяв діяти традиційними засобами [10].

Стратегія "асиметричного підходу" реалізовувалася і Радянським Союзом в рамках програми протидії "Стратегічній оборонній ініціативі" Рональда Рейгана, який у березні 1983 року запропонував створити систему космічного базування, що була б спроможна "перехоплювати і знищувати стратегічні балістичні ракети перш, ніж вони досягнуть нашої території або території наших союзників". Рішення застосувати концепцію асиметричної відповіді було прийнято керівництвом країни після довгих вагань, оскільки традиційною поведінкою для тогочасного Радянського Союзу було сповідування принципу рівнозначної відповіді.

Сутність асиметричної відповіді, наданої на "Стратегічну оборонну ініціативу" США, зводилася перш за все до того, щоб ... при розгортанні США багатоешелонної протиракетної оборони забезпечити можливість радянським ракетно-ядерним засобам нанести неприйнятного збитку агресору, тим самим змусивши його відмовитися від випереджального (превентивного) удару" [8, с. 9—10]. Для цього довелося розглянути масу можливих сценаріїв, долучаючи для їх моделювання широке коло спеціалістів різного профілю та електронно-обчислювальну техніку.

Технічно асиметрична відповідь передбачала підвищення стійкості стратегічних ядерних сил по відношенню до удару на випередження супротивника, збільшення здатності стратегічних ядерних сил із подолання протиракетної оборони іншої сторони і розвиток засобів ураження і нейтралізації протиракетної оборони США, особливо її космічних компонентів [8, с. 50]. В рамках асиметричної стратегії передбачався широкий комплекс заходів щодо підвищення бойової стійкості радянських стратегічних ядерних сил і їх здатності долати багатоешелоновану протиракетну оборону. Були виявлені особливо вразливі компоненти потенційної протиракетної оборони США, які могли виводитися з ладу засобами радіоелектронної боротьби. Особливо це стосувалося виведених в космос лазерів та інших "платформ". Зокрема пропонувалося побудувати наземні лазери, здатні вражати супутники. Точність наведення цих лазерів мала б дозволяти тримати промінь на космічному об'єкті тривалий час, що значно зменшувало потребу в енергії [6].

Ще на етапі розробки асиметричної відповіді Радянського Союзу на програму "Стратегічної оборонної ініціативи" було визначено, що побудова ефективної відповіді можлива за умови поєднання дій у воєнному напрямі з діями, спрямованими на створення політико-психологічного тиску на американську сторону. Першочерговими засобами такого впливу стали публічні виступи перед своєю і особливо зарубіжною аудиторією, для чого довелося переконати владу зняти секретність з деяких вчених. Зокрема, першим "виїзним" вченим став академік Ю.Б. Харитон, головний конструктор і науковий керівник проекту створення ядерної і термоядерної зброї, який реалізовувався в ядерному науковому центрі "Арзамас-16".

Відзначимо, що події навколо американської стратегічної оборонної ініціативи та радянської відповіді на неї стали одним з найбільш цікавих прикладів комплексної асиметричної стратегії політико-військового плану, що включає дипломатичну, політико-пропагандистську діяльність, розробку та реалізацію конкретних програм розвитку систем озброєнь і створення під них науково-технічної бази. Але не лише Росія використовувала в цьому конфлікті асиметричні засоби. Так, відомий російський політолог, учений-американіст Г.А. Арбатов стверджував, що в 1983—1984 роках немолоде покоління пізньорадянської лідерів не до кінця розуміло, чого хоче Р. Рейган і всерйоз "злякалося Стратегічної оборонної ініціативи". Згодом ці побоювання обернулися низкою односторонніх вчинків, на які пішло радянське керівництво М.С. Горбачова при укладанні договорів про скорочення озброєнь [10].

Звернемося до більш сучасних прикладів асиметричної відповіді. Прагнення КНР встановити регіональну гегемонію в Східній і Південно-Східній Азії змусила Японію перейти до нової стратегії створення "Asia's democratic security diamond". Ця стратегія, реалізація якої розпочата кабінетом міністрів Японії в кінці 2012 року, передбачала укріплення зав'язків Японії як із традиційними союзниками (США, Австралія), так і з нови-

ми партнерами (Індія та країни Південно-Східної Азії). Передбачалося, що це "рятівне коло" навколо Японії створить у Пекіна відчуття стримування, а отже змусити його відмовитися від агресивної політики, що у поєднанні з новою військовою оборонною концепцією "Maritime supremacy and air superiority" Японії та розроблюваною під неї технічною базою має забезпечити мирне співіснування країни вранішнього сонця зі своїми сусідами [2].

Росія заявляє про створення нових видів озброєння [7], яке грунтується на нових фізичних принципах, яке має стати "бюджетною" асиметричною відповіддю на зовнішні загрози, в тому числі в контексті концепції глобального удару та глобальної протиракетної оборони.

У серпні 2016 року в Перській затоці чотири катери ВМС Ірану, активно маневруючи, на високій швидкості наблизилися до американського ескадреного міноносця, тим самим, як заявив представник Міністерства оборони США, створивши небезпечну ситуацію через можливість прийняття активних захисних заходів із боку есмінця. Тим не менше, спеціалісти відзначають, що інцидент стався у тій частині Перської затоки, яка повністю прострілюється іранськими протикорабельними ракетами, тому застосування зброї есмінцем багато в чому нагадувало б поведінку самовбивці, а тому було маловирогідним. Враховуючи наявність у складі ВМС Ірану швидкісних водних скутерів з водіями-гранатометальниками, дії маневрових катерів у Перській затоці можна розцінювати як елемент асиметричної відповіді у боротьбі з великим та сильним супротивником [4].

Як бачимо, асиметрична відповідь в умовах гібридної війни передбачає використання не лише військових методів. Своє застосування отримують й інші, невійськові методи: від залякування протилежної сторони до провокування її на неспівмірні економічні витрати і спонукання на односторонні поступки. Військові заходи активно доповнюються політичними, дипломатичними, економічними та пропагандистськими методами.

Сьогодні до переліку методів асиметричної боротьби можна із впевненістю додати методи інформаційного супротиву та кібернетичні засоби, що використовуються в кіберпросторі.

У сучасному україно-російському конфлікті на сході нашої країни Росія використовує традиційні військові засоби поряд з добре організованим поєднанням інформаційної війни та дипломатії. Зокрема Росія вдається до таких дій, як фінансування політичних партій, що діють на території України, створення та фінансування проросійських військово-патріотичних молодіжних організацій, кібератаки, залякування, прямий пропагандистський вплив, формування громадської думки через контрольовані засоби масової інформації та соціальні мережі тощо, на що звертають увагу як вітчизняні, так і закордонні дослідники [3; 9; 12—14].

Можна зазначити, що невійськові методи, включаючи інформаційні операції, використовувалися практично у всіх війнах, тому недоречно виділяти використання альтернативних (невійськових) методів як ознаку асиметричної відповіді у гібридних війнах. Проте сучасні мас-медіа, безперечно, мають більші можливості використання, ніж традиційні ЗМІ. Сучасні інформаційно-комунікаційні засоби, порівняно із традиційними, є значно оперативнішими як з точки зору реагування на черговий інформаційний привід, так і з позицій оновлення і доповнення інформації, надають можливість отримувати та оприлюднювати інформацію анонімно, позбавлені географічних кордонів тощо. Подача інформації в соціальних мережах, на фоні зневіри в об'єктивність офіційних ЗМІ, створює атмосферу неупередженості, плюралізму і паритету думок та ідей, тобто підвищує рівень довіри до інформації, що транслюється в соціальних мережах. Цим пояснюється перспективність використання різноманітних соціальних мереж як інструментів асиметричної відповіді в гібридній війні. Крім того, сприйняття конфлікту через посередництво мас-медіа має більше значення, ніж реальних фактів на місцях, адже аудиторія мас-медіа значно ширша: за розгортанням подій в режимі реального часу може спостерігати як внутрішня аудиторія, так і представники діаспори, іноземні громадяни та будь-які інші заінтересовані сторони. Завдяки такій можливості формувати громадську думку сучасні масмедіа є потужним засобом впливу, який варто брати до уваги як в мирний час, так і в період активного протистояння.

Можемо стверджувати, що висловлена Девідом Стаплсом думка щодо того, що інформаційна війна, яка об'єднує радіоелектронну війну, кібервійни і психологічні операції в єдиний комплекс, матиме ключове значення для всієї війни у майбутньому [14; 15], із передбачення вже зараз перетворилося на реальність. Цей комплекс може використовуватися як для нападу, так і для захисту. Під радіоелектронною зброєю маються на увазі засоби, які використовується для руйнування або нейтралізації електромагнітних потоків, які забезпечують передачу сигналів (комунікацію) через супутникові або наземні мережі зв'язку; кібератаки спрямовані на втручання в системи управління промислових, бізнесових організацій та систем життєзабезпечення суспільства через проникнення в їх електронні (цифрові) мережі; психологічні операції мають на меті вплив на поведінку та руйнування морального стану громадян [15].

На наш погляд, тут слід звернути увагу на терміни "інформаційний простір" та "кібернетичний простір", "кібер-зброя", а також інші наразі модні терміни з префіксом кібер-, оскільки в публікаціях українських науковців немає одностайної позиції щодо їх змісту.

У вітчизняних публікаціях термін інформаційний простір з'явився на початку 90-х років минулого століття, визначаючи якусь системну сутність, структурними компонентами якої є інформаційні ресурси, засоби інформаційної взаємодії та інформаційна інфраструктура. У передмові до словника-довідника [5] "інформаційний простір — середовище, в якому здійснюються процеси створення, збору, реєстрації, обробки, накопичення, заощадження, пошуку, захисту, поширення і використання інформації ... ". Одне з офіційно прийнятих визначень (Рішення економічної ради СНД "Про

концепцію науково-інформаційного забезпечення програм і проектів держав-учасниць СНД в інноваційній сфері"): "інформаційний простір — сукупність баз і банків даних, інформаційно-телекомунікаційних мереж і систем, а також технологій їх ведення і використання, що функціонують на основі загальних принципів і за правилами, що забезпечує інформаційну взаємодію організацій і громадян ... "

Кіберпростір — простір, утворений інформаційними потоками і інформаційними полями, які породжуються в процесі функціонування кібернетичних систем, тобто систем, які забезпечують вирішення управлінських завдань для різних видів діяльності. Об'єктом атаки в кіберсистемах є специфічний вид інформації — управлінська інформація, тобто інформація, яка використовується виключно для вироблення управлінських рішень [1]. Таким чином, наприклад, поняття "інформаційні загрози" є родовим по відношенню до поняття "кібернетичні загрози", а кібернетичний простір є складовою простору інформаційного. Відповідно, кібернетична атака — атака, спрямована на руйнування, модифікацію, блокування, несанкціонований витік та інші неправомірні дії з інформацією, що забезпечує вирішення управлінських задач; кібернетична зброя — комплекс програмних і технічних засобів, які дозволяють здійснити кібернетичну атаку тощо.

Лише станом на 2012 рік експерти відзначали, що розробкою кіберзброї займаються щонайменше 25 країн, тоді як загалом країни, які мають фінансові, людські та інфраструктурні можливості для реалізації програм із кібернетичною проблематикою у 2015 р. налічується близько 140 [3].

Варто нагадати, що комп'ютерний вірус Stuxnet, метою якого була ядерна програма Ірану, його розробники позиціонували саме як асиметричну відповідь на цю програму. Цей комп'ютерний хробак, створений внаслідок тривалого співробітництва США та Ізраїлю, був "заточений" під системи, що управляють іранськими центрифугами для збагачення урану: він змінював умови роботи центрифуг так, що їх оператори не помічали жодних відхилень, тоді як центрифуги фізично виходили з ладу внаслідок абсолютної неконтрольованості процесу. США сподівалися, що за допомогою кібердару по ядерній інфраструктурі Ірану вони одночасно досягнуть двох цілей: не дозволять Ізраїлю завдати ракетно-бомбових ударів по Ірану, а також не дадуть втягнути себе в новий конфлікт на Близькому Сході [3; 11].

Під час планування, розробки та реалізації асиметричної відповіді необхідно ясно усвідомлювати, що інформаційний, зокрема кіберпростір як арена для розгортання гібридної війни чи будь-яких інших протистоянь буде використовуватися дедалі активніше. Вже зараз бюджети безпекових відомств розвинених країн, що задіяні в системі кібербезпеки держави, складають мільярди доларів. Про обсяги й масштаби підготовки розвинених держав до кіберпротистояння красномовно свідчать дані викривальних заяв Е. Сноудена. Масштаб програм, які реалізуються лише Агентством національної безпеки США, красномовно демонструють занепокоєність уряду США кібербезпековою проблематикою. При цьому слід пам'ятати, що в США існує ряд інших державних структур, які розробляють та втілюють у життя програми з кібербезпеки.

Випадок із вірусом Stuxnet є доказом того, що розвинені держави чітко усвідомлюють, що кіберзброя може виявитися реальним асиметричним інструментом протидії тим країнам, які загрожують існуючому міжнародному порядку [11].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Для перемоги у протистоянні із сильним супротивником наша держава мусить шукати способи надання асиметричної відповіді, яка може включати як військові, так і невійськові елементи (політичні, економічні, інформаційні, дипломатичні тощо). Одним із перспективних векторів асиметричної відповіді агресору є кібернетичний.

Наявність могутніх наступальних та захисних кіберпотенціалів може виконувати роль стримуючого фактора для потенційних зловмисників та диверсантів, а функціонування кіберпростору на засадах безпеки є необхідною умовою нормального життєзабезпечення всього соціуму, враховуючи включеність у нього керівних систем критичної інфраструктури. Таким чином, Україна повинна активно розробляти та застосовувати як оборонні, так і наступальні заходи, в тому числі для реалізації в кіберпросторі, чому сприятиме наявність у нашій країні великої кількості гарних фахівців з IT та порівняно невеликий бюджет витрат. У такому разі при спробі заподіяти шкоду інтересам української держави, суспільства чи людини, супротивник має отримати потужну кібервідповідь, що призведе до зменшення загарбницьких амбіцій та зростання військових і інших видатків, що є одними з цілей асиметричної відповіді.

Для забезпечення гідної інформаційної та кібервідповіді на агресивні дії супротивника необхідно здійснити системні зміни підходу держави до кібербезпеки, зокрема в інституційній та нормативно-правовій площині.

Література:

1. Архипов О.Є. Приставка кібер-: чи все очевидно? / О.Є. Архипов // Захист інформації. — 2016. — 18 (3). — С. 203—209. doi:10.18372/2410-7840.18.10849

2. Бєлєсков М. Нова військова стратегія Японії: асиметрична відповідь на виклик із боку КНР [Електронний ресурс] / М.Бєлєсков // Хвиля. — 08.01.2016. — Режим доступу: http://hvylya.net/analytics/geopolitics/nova-viyskova-strategiya-yaponiyi-asimetrichna-vidpovid-na-viklik-iz-boku-knr.html

3. Горбулін В. У пошуках асиметричних відповідей: кіберпростір у гібридній війні [Електронний ресурс] / В. Горбулін // Дзеркало тижня. — 20.02.2015. — Режим доступу: http://gazeta.dt.ua/internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html

4. Ивашов Г. Иран демонстрирует возможности ассиметричного ответа армии США. Тенденция? [Электронный ресурс] / Г. Ивашов. — 25.08.2016. — Режим доступа: https://cont.ws/post/354798

5. Інформаційний простір України: Словник-довідник законодавчих термінів / Автор-укладач Я.О. Чепуренко. — К.: Освіта України, 2008. — 544 с.

6. Мясников В. Как ковалась асимметричность [Электронный ресурс] / В. Мясников // Независимое военное обозрение. — 17.10.2008. — Режим доступа: http://nvo.ng.ru/history/2008-10-17/15_asimmetrichnost.html

7. Оборона на новых физических принципах [Электронный ресурс] // Независимая газета. — 28.11.2016. — Режим доступа: http://www.ng.ru/editorial/2016-11-28/2_6870_red.html

8. Ознобищев С.К., Потапов В.Я., Скоков В.В. Как готовился "асимметричный ответ" на "Стратегическую оборонную инициативу" Р. Рейгана. Велихов, Кокошин и другие. — М.: ЛЕНАНД, 2008. — 56 с.

9. Судольский Р. Дмитрий Шимкив: "Россия создает специальные компьютерные вирусы для атак на украинские госсайты" [Электронный ресурс] / Р. Судольский // Интернет-журнал AIN.UA. — 19.01.2015. — Режим доступа: http://ain.ua/dmitrij-shimkiv-rossiya-sozdaet-specialnye-kompyuternye-virusy-dlya-atak-na-ukrainskie-gossajty

10. Фененко А. Асимметричній ответ в новом веке / Алексей Фененко // Международные процессы. — 2008. — Т. 6. — 3 (18). — С. 121—126.

11. Хлапковский В. Взломать целую страну. Вирус Stuxnet оказался частью плана США по кибернападению на Иран [Электронный ресурс] / В. Хлапковский // Информационный портал RUS DELFI. — 18.02.2016. — Режим доступа: http://rus.delfi.lv/techlife/detali/vzlomat-celuyu-stranu-virus-stuxnet-okazalsya-chastyu-plana-ssha-po-kibernapadeniyu-na-iran.d?id=47076733

12. Andersson, Jan Joel. (2015), "Hybrid operations: lessons from the past", European Union Institute for Security Studies, Brief Issue, No. 33, October 2015, available at: http://www.iss.europa.eu/uploads/media/Brief_33_Hybrid_operations.pdf (Accessed 14 Nov 2016).

13. Popescu, Nicu. Hybrid tactics: neither new nor only Russian. European Union Institute for Security Studies, Issue Alert. — 2015. — No. 4. — January. — 2015. — P. 1—2.

14. Social media as a tool of hybrid warfare. NATO StratCom Centre of Excellence. Riga, May 2016, 45 p.

15. Stupples, David. (2015). The next big war will be digital — and we're not ready for it, available at: http://gizmodo.com/the-next-big-war-will-be-digital-and-we-re-not-ready-fo-1744865435 11/27/15 (Accessed 15 Nov 2016).

References:

1. Arkhypov, O.Ye. (2016), "Prefix cyber-: all is obvious?", Ukrainian Information Security Research Journal, no. 18(3), pp. 203—209. doi:10.18372/2410-7840.18.10849

2. Bielieskov, M. (2016), "The new Japan military strategy: asymmetrical response to the challenge of PRC", Khvylia, 08.01.2016, available at: http://hvylya.net/analytics/geopolitics/nova-viyskova-strategiya-yaponiyi-asimetrichna-vidpovid-na-viklik-iz-boku-knr.html (Accessed 14 Nov 2016).

3. Gorbulin, V. (2015), "Finding asymmetric responses: cyberspace in hybrid warfare", Dzerkalo tyzhnia, 20.02.2015, available at: http://gazeta.dt.ua/internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html (Accessed 15 Nov 2016).

4. Ivashov, G. (2016), Iran demonstrates the possibility of an asymmetric response to the US Army. Is it a trend?", 25.08.2016, available at: https://cont.ws/post/354798 (Accessed 15 Nov 2016).

5. Chepurenko, Ya. O. (2008), The information space of Ukraine: The dictionary-directory of legislative terms, Osvita Ukrainy [Education of Ukraine], Kyiv, Ukraine.

6. Mjasnikov, V. (2008), "As asymmetry was forged". Nezavisimoe voennoe obozrenie, 17.10.2008, available at: http://nvo.ng.ru/history/2008-10-17/15_asimmetrichnost.html (Accessed 15 Nov 2016).

7. Independent newspaper (2016), "The defense, based on new physical principles", available at: http://www.ng.ru/editorial/2016-11-28/2_6870_red.html (Accessed 15 Nov 2016).

8. Oznobishhev, S.K. Potapov, V.Ja. and Skokov, V.V. (2008), Kak gotovilsja "asimmetrichnyj otvet" na "Strategicheskuju oboronnuju iniciativu" R.Rejgana. Velihov, Kokoshin i drugie [How was prepared "asymmetric response" to the "Strategic Defense Initiative" of R. Reagan. Velikhov, Kokoshin and others], LENAND, Moscow, Russia.

9. Sudolskiy, R. (2015), "Dmitry Shimkiv: "Russia creates special computer viruses to attack Ukrainian government websites", Internet-journal AIN.UA, 19.01.2015, available at: http://ain.ua/dmitrij-shimkiv-rossiya-sozdaet-specialnye-kompyuternye-virusy-dlya-atak-na-ukrainskie-gossajty(Accessed 15 Nov 2016).

10. Fenenko, A. (2008), "Asymmetrical response in the new century", Mezhdunarodnye process, vol. 6, no. 3 (18), pp. 121—126.

11. Hlapkovsky V. (2016), "Hack the whole country. Virus Stuxnet is a part of a US plan for cyber attacks on Iran", Information portal RUS DELFI, 18.02.2016, available at: http://rus.delfi.lv/techlife/detali/vzlomat-celuyu-stranu-virus-stuxnet-okazalsya-chastyu-plana-ssha-po-kibernapadeniyu-na-iran.d?id=47076733 (Accessed 14 Nov 2016).

12. Andersson, Jan Joel. (2015), "Hybrid operations: lessons from the past", European Union Institute for Security Studies, Brief Issue, No. 33, October 2015, available at: http://www.iss.europa.eu/uploads/media/Brief_33_Hybrid_ operations.pdf (Accessed 14 Nov 2016).

13. Popescu, Nicu (2015), "Hybrid tactics: neither new nor only Russian". European Union Institute for Security Studies, Issue Alert, No. 4, January 2015, pp 1—2.

14. NATO (2016), Social media as a tool of hybrid warfare. NATO StratCom Centre of Excellence, May 2016, Riga, Latvia.

15. Stupples, David (2015), The next big war will be digital — and we're not ready for it, available at: http://gizmodo.com/the-next-big-war-will-be-digital-and-we-re-not-ready-fo-1744865435 11/27/15 (Accessed 15 Nov 2016).

Стаття надійшла до редакції 19.12.2016 р.