Ясміна Короход, к.політ.н., адвокат
Національний університет «Одеська юридична академія», Україна

ІНФОРМАЦІЙНА ВІЙНА ЯК ОСНОВНА ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ: ПОНЯТТЯ, ФОРМИ І МЕТОДИ ВЕДЕННЯ

Yasmina Korokhod, PhD in Political science, advocate
National University "Odesa Law Academy", Ukraine

INFORMATION WAR AS THE MAIN THREAT TO INFORMATION SECURITY OF THE STATE: CONCEPT, FORMS AND METHODS OF CONDUCTING

In the article the main approaches to the definition of information threats classified by different criteria. The basic levels of information security threats of the modern state are studied (threat to national security, common threats to the state and the private sector, local infiltration) and their species, and among them information warfare.
Determined wide and narrow interpretation to understand the essence of the information war, analyzed its form (the war in the field of command and control, intelligence and information warfare, network warfare, psychological warfare, "hacker-war", economic information warfare, "cyberwar"). The concepts of "information warfare" and "cyberwar" were differentiated. It was found distinctive features and basic methods of information warfare in modern conditions of social development.
Key words: information security, information warfare, intelligence and information warfare, network warfare, psychological warfare, "hacker-war" economic information war, cyberwar.

Постановка проблеми у загальному вигляді. Стрімкий розвиток інформаційно-комунікаційних технологій став каталізатором численних соціальних, культурних, економічних і політичних процесів як на національному рівні, так і в глобальному масштабі. На зміну індустріальній епосі прийшла інформаційна, в якій головну роль відіграють нові технології та інформація. В результаті відбулася трансформація як суспільства, так і держави: виник новий тип суспільства – глобальне інформаційне суспільство, новий тип економіки – інноваційна або інформаційна економіка, нова форма управління державою – електронний уряд, прискорилися всі процеси обміну і отримання інформацією, істотно змінився ритм і стиль життя. Сьогодні рівень розвитку сектора інформаційно-комунікаційних технологій визначає роль держави в світовій економіці та її політичну вагу на міжнародній арені. Таким чином, боротьба за володіння інформацією, досягнення і утримання інформаційної переваги займає значне місце в геополітичній конкуренції країн, це призводить до розширення і поширенню загроз інформаційній безпеці, головною серед яких є інформаційна війна.

Аналіз останніх досліджень і публікацій. До аналізу сутності інформаційної війни звертались в свої наукових працях як зарубіжні, так і вітчизняні вчені. Праці Д. Белла, М. Кастельса, Й. Масуди і М. Пората заклали основу концепції інформаційного суспільства та визначили його основні характеристики.

Наслідки трансформації суспільства і держави під впливом інформаційно-комунікаційних технологій, їх вплив на політичні процеси на національному та міжнародному рівні розглянуті в роботах західних дослідників У. Бека, Дж. Коена, М. Мура, Дж. Розенау, А. Тоффлера, Т. Фрідмана, Е. Шмідта та ін., а також російських – Г.А. Атаманова, Д.Г. Балуєва, О.Н. Вершинського, М.М. Лебедєвої, Д.Н. Пєскова, В.Ф. Пилипенка, А.В. Торкунова та ін. До вітчизняних вчених, які займаються вивченням феномену інформаційної війни належать В. Бебик, О. Гапченко, Я. Жарков, О. Литвиненко, В. Петрик, Г. Почепцов, М. Присяжнюк, І. Рабінович, Д. Фельдман, Ю. Шайгородський та інші.

Метою статті є комплексний аналіз сучасного змісту поняття «інформаційна війна» як основна загроза економічній безпеці держзави, її ознак, форм та методів ведення в умовах інформаційного суспільства.

Виклад основного матеріалу дослідження. Слід зазначити, що міжнародне співтовариство до цих пір не прийшло до єдиного розуміння ключових термінів в області інформаційної безпеки. Країни по-різному тлумачать і визначають її межі. В цілому можна виділити два основні підходи до визначення інформаційної безпеки:

– широкий – поняття інформаційної безпеки включає в себе як інформаційно-технічні, так і інформаційно-психологічні аспекти. Даний підхід відповідає баченню Росії, а також країн-партнерів по Шанхайської організації співпраці, Організації договору про колективну безпеку та ряду інших держав, які визначають інформаційну безпеку як «стан захищеності особистості, суспільства і держави та їх інтересів від загроз, деструктивних і інших негативних впливів в інформаційному просторі»[1];

– вузький підхід (його дотримуються США) – термін «інформаційна безпека» обмежується технологічними аспектами та визначається як захист інформації та інформаційних систем і мереж від несанкціонованого доступу, використання, розкриття, пошкодження, внесення змін або знищення з метою забезпечення цілісності, конфіденційності та доступності[2]. Це пов'язано з тим, що США не співвідносять захист інформації з інформаційно-психологічними аспектами, включаючи застосування цензури або контроль за інформованістю населення[3].

Таким чином, питання інформаційної безпеки, з точки зору США, не включають контент та управління ім. Пріоритетом для Сполучених Штатів є забезпечення кібербезпеки, де «кібер» являє собою глобальний простір в рамках інформаційної сфери, що охоплює взаємопов'язані мережі інформаційної технологічної інфраструктури та розміщені в них дані, в тому числі Інтернет, телекомунікаційні мережі, комп'ютерні системи і вбудовані процесори і системи управління[4].

За природою виникнення загрози інформаційної безпеки діляться на природні і антропогенні. До природних загроз відносяться: загрози природного характеру (пов'язані з природними явищами, стихійними лихами: землетрусами, повенями, пожежами, ураганами і т.д.); загрози техногенного характеру (пов'язані з проблемами, що виникають в обладнанні і техніці).

Загрози антропогенного характеру пов'язані з діями людини щодо інформації, комп'ютерних систем і мереж та можуть бути як умисними (адресні атаки – їх метою є певна інформаційна система або об'єкт критичної інфраструктури; безадресні атаки – використання шкідливих програм), так і ненавмисними[5].

Зростання числа засобів в методів здійснення деструктивних дій в мережі обумовлює той факт, що саме людський фактор стає основною загрозою інформаційної безпеки.

В якості суб'єктів (джерел) загроз інформаційній безпеці можуть виступати численні актори, що володіють необхідними знаннями або можливостями для проведення деструктивних дій в інформаційному просторі. Найбільшу небезпеку при цьому представляють держави, які використовують кіберінструменти для збору інформації та здійснення розвідувальної діяльності, включаючи економічне шпигунство, з метою отримання політичної, військової та економічної переваги. Крім того, ряд держав веде розробки в області інформаційної війни, яка проводиться з метою скорочення простору супротивника для прийняття рішень, отримання стратегічної переваги і руйнування конкретних цілей, в тому числі тих. Що підтримують комунікацій і економічної інфраструктури, що забезпечують військову міць країни.

---

[1] *Доктрина информационной безопасности Российской Федерации* от 9 сентября 2000 г. *Российская газета*.<http://www.rg.ru/oficial/doc/min and vedom/mim bezop/doctr.shtm>; *Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности* от 16 июня 2009 г., г. Екатеринбург. Приложение 1.<www.konsultant.ru> ; *Положение о сотрудничестве государств-членов Организации договора о коллективной безопасности в сфере обеспечения информационной безопасности* от 10 декабря 2010 г. <http://docs.pravo.ru/document/view/16657605/14110649/>

[2] *Federal Information Security Act.* 2002. Subchapter III – Informationa Security. § 3542. Definitions. <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

[3] The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations (2011). *EastWest Institute*, Issue 1. April 2011, 17. <http://www.ewi.info/idea/russia-us-bilateral-cybersecurity- critical-terminology-foundations>

[4] Department of Defense Dictionary of Military and Associated Terms (2010). *Joint Chiefs of Staff.* November 8, 64. <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>

[5] Батуева, Е.В. (2014). *Американская концепция угроз информационной безопасности и ее международно-политическая составляющая*: дисс. … кандидата политических наук. полит. н.: спец. 23.00.04. Москва, 27.

Залежно від цілей і завдань, переслідуваних акторами в кіберпросторі, а також від їх потенціалу виділяють три рівня загроз інформаційній безпеці:

– загрози національній безпеці (інформаційна війна, кібершпіонаж);

– загальні загрози для держави і приватного сектора (терористична діяльність, індустріальний шпигунство, організована злочинність);

– локальні загрози (хакери, професійні групи і любителі)[1].

Забезпечення інформаційної безпеки вимагає комплексу заходів на рівні держави, приватних компаній і окремих індивідів. При цьому ефективна протидія даним загрозам на національному рівні можлива тільки при тісній взаємодії державного і приватного сектору, оскільки значна частина критичної інфраструктури країни і мереж знаходяться в приватній власності. У зв'язку з цим виникає потреба в підвищенні рівня загальної відповідальності за забезпечення безпеки, а також у встановленні зворотного зв'язку та забезпеченні міжрівневої взаємодії.

Таким чином, можна сформулювати загальну концепцію загроз інформаційній безпеці, яка включає в себе інформаційні війни, кібершпіонаж, кіберзлочинність та кібертероризм.

Варто відзначити, що сама концепція «інформаційної війни» зародилася в США і отримала свій розвиток на початку 1990-х років після успішного проведення операції «Буря в пустелі» в 1991 році, яку часто називають «першою інформаційною війною». Інформаційні технології, використані силами коаліції в якості зброї, а також з метою координації дій, проведення розвідувальних заходів, аналізу ситуації та тилового забезпечення дозволили в значній мірі скоротити втрати в ході операції.

Термін «інформаційна війна» сьогодні використовується досить широко, однак однозначного визначення цього поняття поки немає. Дослідниками термін «інформаційна війна» на сьогоднішній день трактується як:

– комплексне спільне застосування сил і засобів інформаційної та збройної боротьби;

– комунікативна технологія по впливу на інформацію та інформаційні системи противника при одночасному захисті власної інформації і своїх інформаційних систем;

– психо-комунікативні технології впливу на масову свідомість;

– протиборство між державами в інформаційному просторі з метою завдати шкоди інформаційним системам, процесам і ресурсам, підриву політичної та соціальної систем;

– масована психологічна обробка особового складу військ і населення з метою дестабілізувати суспільство і держава (інформаційно-психологічна війна)[2].

На даний момент існує кілька підходів до визначення інформаційної війни:

– вузький підхід – американська концепція (виходить з того, що під інформаційною війною розуміється протиборство з інформаційними системами супротивників, яке включає в себе проникнення в інформаційні системи, їх перекручення чи знищення при забезпеченні захисту власних систем від аналогічних дій[3]). Таким чином, на рівні військового керівництва США основний акцент був зроблений на технологічних аспектах ведення інформаційних війн, що у вузькому сенсі є кібервійною;

– широкий підхід – інформаційна війна включає в себе дві концепції кібервійну (cyberwar) і мережеву війну (netwar)[4].

Слід зазначити, що головною зброєю інформаційної війни є пристрої, способи і прийоми обробки інформації, які з кожним днем мають все більше можливостей цілеспрямовано, таємно та широкомасштабно впливати на інформаційні системи ворога, підриваючи його моральні підвалини, економіку, віру в систему управління, боєготовність, боєздатність і т.п.

Виділяють такі технології застосування інформаційної зброї: контроль і управління над подіями, що відбуваються в суспільстві; контроль над засобами накопичення, зберігання,

[1] Critical Foundations: Protecting America's Infrastructures. *President's Commission on Critical Infrastructure Protection Report*. October 1997, 20. <https://www.fas.org/sgp/library/pccip.pdf>

[2] Пилипенко, В.Ф. (2005). *Безопасность: теория, парадигма, концепция, культура. Словарь-справочник*. Изд. 2-е. Москва: ПЕР СЭ-Пресс.

[3] *Information Warfare*: Department of Defense Directive. TS 3600.1. December 21, 1992. <http://www.dod.mil/pubs/foi/administration and Management/admin matters/14-F-0492 doc 01 Directive TS-3600-1.pdf>

[4] Попов, И.М. (2004). *Война будущего: взгляд из-за океана: Военные теории и концепции современных США*. Москва: ООО «Издательство АСТ», 112-113.

поширення, спотворення, розкрадання і знищення інформації; володіння способами охорони і захисту інформації, а також наявними способами та прийомами впливу; контроль над допуском обмеженого числа користувачів; розробка і впровадження нових засобів, спрямованих на дезорганізацію роботи «противника», його технічних засобів, комп'ютерних систем і людських ресурсів[1].

Об'єктами інформаційного та психологічного впливу є життєва сила (людські ресурси; маси), еліта (владна керуюча сила держави), а також матеріальні об'єкти та інфраструктура.

Інформаційна війна впливає на свідомість людини, змінює її світогляд і погляди.

Найбільш відомим прикладом інформаційної та психологічної війни є «Холодна війна».

Аналізуючи різні трактування поняття «інформаційні війни» російський дослідник Г.А. Атаманов дає їй таке визначення: «процеси, засоби і методи реалізації яких кардинально різняться: це не тільки комп'ютерні віруси, а стан суспільної свідомості та панівна в суспільстві картина світу впливає на роботу інформаційно-телекомунікаційних систем. На думку автора, в сучасному світі інформаційна війна – це не тільки протиріччя, а протиборство двох соціальних систем і головною відмінною рисою її є не застосування засобів збройного насильства, а можливість повного або часткового знищення інформаційно-телекомунікаційних інфраструктур протиборчої сторони, включаючи її базового елементу – людини, а головним засобом ведення інформаційної війни є інформаційні технології[2].

Але найближче і докладніше, до визначення сутності та змісту інформаційної війни прийшов, провідний американський дослідник в області інформаційних воєн, М. Лібіцкі. Він вважає що, «інформаційна війна являє собою мозаїку різних форм, а не якусь одну певну» [3]..

Основних компонентів в цій «мозаїці форм», на думку професора М. Лібіцкі, є сім. Звідси виникають і сім форм інформаційної війни[4]:

– війна в сфері управління військами (націлена на позбавлення військ противника системи управління, тобто на фізичне знищення центрів і пунктів управління, порушення систем управління військами, ліній комунікацій і в цілому системи управління противника на стратегічному, оперативному або тактичному рівнях);

– розвідувально-інформаційна війна (передбачає нанесення противнику фізичної шкоди – вогневого ураження, стеження – на основі широкого впровадження сенсорів і датчиків);

– мережева війна (конфронтаційне протистояння, яке здійснюється на підставі єдності ідеології та інформаційно-комунікаційної мережної взаємодії[5]). Вона охоплює економічні, політичні, соціальні, а також військові форми протиборства, і її метою є вплив на громадську думку і думку еліт за допомогою дипломатичних методів, пропаганди, психологічних кампаній, втручання в діяльність місцевих ЗМІ, несанкціоноване проникнення в комп'ютерні системи і бази даних, а також підтримка дисидентів в і опозиційних рухів в інформаційних мережах;

– психологічна війна (використання інформаційних можливостей і ресурсів проти людської свідомості: операції проти національної волі противника; операції проти керівництва супротивника; операції проти військ противника; культурний конфлікт);

– «хакер-війна» (порушення комп'ютерних мереж з використанням комп'ютерних вірусів, логічних бомб, чіппінг-технологій і т.п.);

– економічна інформаційна війна (інформаційна блокада і інформаційний імперіалізм);

– «кібервійна» (зосереджена на військових аспектах і являє собою конфлікт високої інтенсивності виключно між збройними силами протиборчих сторін, які ведуть боротьбу

[1] Лаврентьева, М.А., Димитренко, В.В. (2016). Информационные и психологические войны в СМИ. *Научные труды КубГТУ, № 7, 66-75.*

[2] Атаманов, Г.А. (2010). Информационная война: экспликация понятия. *Новые направления в решении проблем АПК на основе современных ресурсосберегающих, инновационных технологий: материалы Международной научно-практической конференции, посвященной 65-летию Победы в Великой Отечественной войне (*Волгоград 26-28 января 2010 г.) Том 4. Волгоград: ИПК «Нива», 126-129.

[3] Попов, И.М. (2004). *Война будущего: взгляд из-за океана: Военные теории и концепции современных США*. Москва: ООО «Издательство АСТ», 101-102.

[4] Попов, И.М. (2004). *Война будущего: взгляд из-за океана: Военные теории и концепции современных США*. Москва: ООО «Издательство АСТ», 102-105.

[5] Дугин, А., Коровин, В., Бовдунов, А. *Сетевые войны.* Аналитический доклад. *ПРАВДИНФОРМ*. <http://trueinform.ru/modules.php?name=News&file=article&sid=23164>

з системами командування і управління з метою спотворити або знищити інформаційні системи противника[1]).

Таким чином, інформаційна війна може приймати різні форми, які, в свою чергу, містять дії, спрямовані на досягнення інформаційної переваги або перемоги над противником за допомогою впливу на інформацію, інформаційні процеси та інформаційні системи супротивника, при забезпеченні безпеки власних аналогічних інформаційних ресурсів, систем і мереж. Що важливо, інформаційну війну відрізняє від всіх інших форм деструктивного використання інформаційно-комунікаційних технологій той факт, що вона ведеться в політичних цілях.

Як відзначають аналітики, інформаційна війна має низку ключових особливостей: порівняно низька вартість створення засобів інформаційного протиборства; можливість управління світосприйняттям противника; складність встановлення початку інформаційної операції; складність встановлення джерела атаки і, як наслідок, складність здійснення дій у відповідь; інформаційна війна підвищує вразливість національної безпеки, так як дія нових технологій не залежить від географічної відстані[2].

Дані характеристики інформаційних воєн зумовили привабливість їх проведення і, як наслідок, зростання загрози використання державами інформаційно-комунікаційних технологій у військово-політичних цілях.

Отже, за результатами проведеного дослідження приходимо до **висновку**, що проблема «інформаційних» воєн, маючи багату історію, не тільки не втратила свого значення в даний момент, але стає все більш актуальною. Війни, в якому б вигляді вони не були представлені, це завжди війни. Сила їх впливу на людей висока. Саме тому практично в усіх країнах світу витрачаються величезні моральні та фізичні сили і засоби на створення нових технологій та методик протидії різного роду інформаційним і психологічним способам впливу, накопиченим протягом тривалого часу.

На сучасному етапі соціального розвитку, виходячи з аналізу останніх збройних конфліктів, і з появою нових способів впливу на противника, назріла необхідність створення в структурі збройних сил підрозділів і засобів з протидії інформаційно-психологічному впливу; розвитку теоретичної бази щодо їх застосування і накопичення практичного досвіду, що в майбутньому буде стримуючим фактором від зовнішніх та внутрішніх загроз для країни.

References:

1. Critical Foundations: Protecting America's Infrastructures. *President's Commission on Critical Infrastructure Protection Report*. October 1997, 20. <https://www.fas.org/sgp/library/pccip.pdf> [in English].
2. Department of Defense Dictionary of Military and Associated Terms (2010). *Joint Chiefs of Staff*. November 8, 64. <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf> [in English].
3. *Federal Information Security Act*. 2002. Subchapter III – Informationa Security. § 3542. Definitions. <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf> [in English].
4. *Information Warfare*: Department of Defense Directive. TS 3600.1. December 21, 1992. <http://www.dod.mil/pubs/foi/administration and Management/admin matters/14-F-0492 doc 01 Directive TS-3600-1.pdf> [in English].
5. Molander, R., Riddile, A., Wilson, P. (1996). *Strategic Information Warfare: A New Face of War. National Defense Research Institute RAND*. <http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf> [in English].
6. The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations (2011). *EastWest Institute*, Issue 1. April 2011, 17. <http://www.ewi.info/idea/russia-us-bilateral-cybersecurity- critical-terminology-foundations> [in English].
7. Atamanov, G.A. (2010). Informacionnaja vojna: jeksplikacija ponjatija [Information war: concept explication]. *Novye napravlenija v reshenii problem APK na osnove sovremennyh resursosberegajushhih, innovacionnyh tehnologij: materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii, posvjashhennoj 65-letiju Pobedy v Velikoj Otechestvennoj vojne* [The new directions in the solution of problems of agrarian and industrial complex on the basis of modern resource-saving, innovative technologies: materials of the International scientific and practical conference devoted to the 65 anniversary of the Victory in the Great Patriotic War] (Volgograd 26-28 janvarja 2010 g.) Tom 4. Volgograd: IPK «Niva», 126-129. [in Russian].

[1] Батуева, Е.В. (2014). *Американская концепция угроз информационной безопасности и ее международно-политическая составляющая*: дисс. … кандидата политических наук. полит. н.: спец. 23.00.04. Москва, 38.
[2] Molander, R., Riddile, A., Wilson, P. (1996). *Strategic Information Warfare: A New Face of War. National Defense Research Institute RAND*. <http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf>

8. Batueva, E.V. (2014). *Amerikanskaja koncepcija ugroz informacionnoj bezopasnosti i ee mezhdunarodno-politicheskaja sostavljajushhaja* [American concept of threats of information security and its international and political component]: diss. … kandidata politicheskih nauk. polit. n.: spec. 23.00.04 [Thesis for PhD degree in law]. Moscow. [in Russian].
9. *Doktrina informacionnoj bezopasnosti Rossijskoj Federacii* [The doctrine of information security of the Russian Federation] ot 9 sentjabrja 2000 g. *Rossijskaja gazeta* [Russian newspaper].<http://www.rg.ru/oficial/doc/min and vedom/mim bezop/doctr.shtm> [in Russian].
10. Dugin, A., Korovin, V., Bovdunov, A. *Setevye vojny* [Network wars. Analytical report]. Analiticheskij doklad. *PRAVDINFORM* [PRAVDINFORM]. <http://trueinform.ru/modules.php?name=News&file=article&sid=23164>
11. Lavrent'eva, M.A., Dimitrenko, V.V. (2016). Informacionnye i psihologicheskie vojny v SMI [Information and wars of nerves in media]. *Nauchnye trudy KubGTU* [Scientific works of KUBGTU], № 7, 66-75. [in Russian].
12. Pilipenko, V.F. (2005). *Bezopasnost': teorija, paradigma, koncepcija, kul'tura. Slovar'-spravochnik* [Safety: theory, paradigm, concept, culture. Dictionary reference]. Izd. 2-e. Moscow: PER SJe-Press. [in Russian].
13. *Polozhenie o sotrudnichestve gosudarstv-chlenov Organizacii dogovora o kollektivnoj bezopasnosti v sfere obespechenija informacionnoj bezopasnosti* [The provision on cooperation of member states of the Collective Security Treaty Organization in the sphere of ensuring information security] ot 10 dekabrja 2010 g. <http://docs.pravo.ru/document/view/16657605/14110649/> [in Russian].
14. Popov, I.M. (2004). *Vojna budushhego: vzgljad iz-za okeana: Voennye teorii i koncepcii sovremennyh SShA* [War of the future: a look because of the ocean: Military theories and concepts of the modern USA]. Moscow: OOO «Izdatel'stvo AST». [in Russian].
15. *Soglashenie mezhdu pravitel'stvami gosudarstv-chlenov Shanhajskoj organizacii sotrudnichestva o sotrudnichestve v oblasti obespechenija mezhdunarodnoj informacionnoj bezopasnosti* [The agreement between the governments of member states of the Shanghai Cooperation Organisation on cooperation in ensuring the international information security] ot 16 ijunja 2009 g. Ekaterinburg. Prilozhenie 1. <www.konsultant.ru> [in Russian].