УДК 007:304:001

С. А. Стародуб

ІНФОРМАЦІЙНІ ВІЙНИ ТА СИСТЕМИ ЗАХИСТУ В УМОВАХ ГЛОБАЛІЗАЦІЙНИХ ПРОЦЕСІВ

Інформація XXI ст. набуває матеріальної форми, і володіння нею стає вельми жаданим. Будь-які цілком «матеріальні» рішення сьогодні проходять випробування та реалізовуються в інформаційній сфері, а їх результати стають вирішальними. Світовий сучасний глобальний простір постійно перебуває в стані війни. Характерною особливістю цієї війни є те, що вона не кровопролитна, але більш руйнівна. Наш світ переживає бурхливе протистояння інформаційних битв у медіапросторі. Особливістю інформаційних битв є постійний обмін інформацією, яка негативно впливає на ворога.

Ключові слова: *війна, конфлікт, бойові дії, інформаційна війна, глобалізація, комунікаційні процеси, інформація.*

І. Вступ

Прогрес нашої цивілізації можна поділити на три хвилі: аграрну, промислову та інформаційну. Кожній із цих хвиль або фаз властиві специфічні засоби ведення війни. Розвинені держави сучасного світу, згідно з поширеним уявленням, у другій половині минулого сторіччя увійшли в інформаційну фазу. Для аграрного суспільства характерні ополчення землевласників – такі були армії грецьких міст-держав або Риму в його республіканський період. Промислові держави мають постійні професійні армії. Війна третього типу – інформаційна.

Глобальне суспільство все більше і більше покладається на інформацію та засоби її доставки. Інтернет – це лише вершина цієї інформаційної конструкції. Будь-яка розвинена країна має телефонну, банківську та безліч інших мереж, що керуються комп'ютерами, отже, мають властиві для них слабкі місця.

Інформаційна війна – це вже не туманна галузь футурології, а реальна військова дисципліна, яку вивчають і розробляють у відповідних академічних закладах. У найбільш широкому розумінні інформаційна війна включає засоби пропаганди, але обсяг цієї статті надає нам змогу зупинитися лише на суто технологічних засобах.

ІІ. Постановка завдання та методи

Мета статті – розкрити можливі системи захисту під час інформаційних війн в умовах глобалізаційних процесів. Основою дослідження є інформаційний, системний, діяльнісний підходи. Використано такі методи: аналізу, синтезу, генералізації – для виявлення можливих систем захисту під час інформаційних війн в умовах глобалізаційних процесів; термінологічний аналіз поняття «інформаційна війна».

ІІІ. Результати

Термін «інформаційна війна» (англ. information war) означає використання й управління інформацією з метою набуття конкурентоспроможної переваги над супротивником. Характерною особливістю інформаційного протистояння є те, що це окремий вид управління отриманою інформацією. Багато хто плутає інформаційну війну з ***кібервійною***, мета якої – домінування в кіберпросторі. Також сюди належить психологічна війна – за психологічне домінування. Крім цих основних понять, ще існує «радіоелектронна боротьба», а також «мережева війна» – система ведення «бойових дій» з використанням мережевих технологій (не лише Інтернет, ідеться про технології, властиві нетократії).

Характерною особливістю також є й те, що в період масштабної глобалізації світу в міжнаціональних відносинах застосовують технології інформаційної війни. Така тенденція пов'язана з тим, що більшість економічно розвинених країн намагаються за будь-якої нагоди завоювати інформаційний світовий простір. Існує давня приказка: «Хто володіє інформацією, той володіє світом». Саме цього принципу й дотримуються країни, що ворогують.

Сам процес ведення війни пов'язаний не лише з обміном негативною чи позитивною інформацією, а й зі збиранням тактичної інформації, забезпеченням безпеки власних інформаційних ресурсів, поширенням пропаганди або дезінформації, щоб деморалізувати ворога й населення, підривом якості інформації супротивника та запобіганням можливості збору інформації супротивником. Часто інформаційну війну ведуть у комплексі з кібер- та психологічною, залучаючи радіоелектронну боротьбу та мережеві технології.

Основні засоби ведення інформаційної війни – інформаційна зброя й інформаційні операції [9].

Враховуючи роль інформації в сучасному світі, американський дослідник М. Маклюен виводить цікаву тезу: «Істинно тотальна війна – це війна за допомогою інформації». Саме він першим проголосив, що в наш час економічні зв'язки й відносини все більше набувають форми обміну знаннями, а не обміну товарами. А засоби масової комунікації самі є новими «природними ресурсами», що збільшують багатства суспільства. Тобто боротьба за капітал, простори збуту тощо відходить на другий план, а головним зараз постає доступ до інформаційних ресурсів, знань, що призводить до того, що війни відбуваються переважно в інформаційному просторі та за допомогою інформаційних видів озброєнь.

Уперше це поняття закріплено в директиві Міністерства оборони США DOD S 3600.1 від 21 грудня 1992 р., де воно вжито у вузькому значенні як різновид радіоелектронної боротьби. У 1996 р. вперше використали термін «Strategic Information Warfare. A new face of War» – «стратегічна інформаційна війна (інформаційне протиборство)» – війна з використанням державного глобального інформаційного простору й інфраструктури для проведення стратегічних військових операцій і зміцнення впливу на власний інформаційний ресурс [7].

Суспільні зміни в громадсько-політичному житті ряду держав зумовлені швидкими темпами інформатизації й комп'ютеризації суспільства, а це призводить до перегляду геополітичних поглядів керівництва, виникнення нових стратегічних інтересів (зокрема в інформаційній сфері), наслідком чого є зміна політики цих країн. Низка авторів підкреслює, що, враховуючи визначення війни, дане К. Клаузевіцем («війна – це продовження політики іншими засобами»), глобальні суперечності потребують нових засобів і методів їх вирішення – стратегічного інформаційного протиборства [2].

Як і в будь-якій війні, є ***тактика, стратегія, напад та оборона.*** Кожна країна самостійно вибирає стратегію. Її визначають у законодавчих актах, які стосуються безпосередньо інформаційного простору держави. У нашій державі таким документом має стати Закон України «Про інформаційну безпеку», який ніяк не можуть прийняти вже протягом 19 років незалежності. Відсутність такого закону призводить до того, що держава не спроможна протистояти зовнішнім інформаційним агресорам, не має виписаної структури ведення захисту, оборони, стримування та нападу, тобто відбиття атак ворога.

Структура оборонного захисту інформаційного простору має будуватися відповідно до законів про інформацію, ЗМІ та інформаційну безпеку, якого немає в удосконаленому вигляді.

Мета інформаційної війни – порушити обмін інформацією в таборі супротивника. Неважко зрозуміти, що цей вид зброї зазвичай узагалі не спрямований на завдання втрат у живій силі. У цьому сенсі крива технології вивела, нарешті, до цілком безкровної й водночас надзвичайно ефективної зброї. Вона знищує не населення, а державний механізм, послаблюючи моральні й матеріальні сили супротивника або конкурента, і передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній сферах. Очевидно, що інформаційна війна – складова ідеологічної боротьби. Вона не спричиняє безпосередньо кровопролиття, руйнування, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує небезпечну безпечність у ставленні до них. Проте, руйнування, яких завдають інформаційні війни у суспільній психології, психології особистості, за масштабами й значенням цілком співмірні, а часом і перевищують наслідки збройних воєн.

Головне завдання інформаційних війн полягає в маніпулюванні масами. Цілі такої маніпуляції найчастіше такі:

1) внесення в суспільну та індивідуальну свідомість ворожих, шкідливих ідей і поглядів;
2) дезорієнтація та дезінформація мас;
3) послаблення певних переконань, устоїв;
4) залякування свого народу образом ворога;
5) залякування супротивника своєю могутністю.

Система – об'єкт інформаційної операції, може включати будь-який елемент в епістемології супротивника. Епістемологія містить у собі організацію, структуру, методи й імовірність знань. На стратегічному рівні мета кампанії інформаційної війни – вплинути на рішення супротивника або конкурента, як наслідок – на його поведінку таким чином, щоб він не знав, що на нього впливали.

Структура захисту має будуватися за таким принципом (рис. 1): *першими в бій вступають районні ЗМІ, другими – обласні, третіми – регіональні; вирішальний бій залишається за загальнодержавними ЗМІ.*

Характерною особливістю цієї структури є те, що в обороні або наступі участь беруть практично вісі ЗМІ, незалежно від форм власності та політичних уподобань. Також важливою є реакція керівного складу держави на будь-які зазіхання на історію, культуру та внутрішню політику з боку інших держав, незалежно від того, чи це добрі партнери й сусіди, чи це держава, з якою немає жодних міждержавних відносин. Кожний має право на захист.

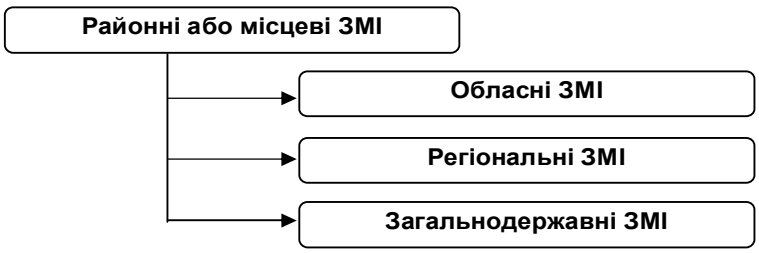

Рис. 1. Система ЗМІ

Відомо і те, що великомасштабні інформаційні технології, які дістали назву інформаційних воєн, мають тисячолітню історію, і кожна історична подія такого масштабу потребує детального дослідження з погляду використання технологій оборони та захисту. Прикладів інформаційного впливу на моральну, духовну стійкість супротивника можна знайти чимало й у Давньому Римі, і в добу феодалізму (боротьба з «єрессю», за «істинну віру» тощо), і в пізніші часи. Особливого значення інформаційні війни набули у XX ст., коли газети, радіо, а потім і телебачення стали справді засобами масової інформації, а поширювана через них інформація – справді масовою. Уже у 20-х рр. XX ст. США вели радіопередачі на регіони своїх «традиційних інтересів» – країни Латинської Америки, Великобританія – на свої колонії. Німеччина, яка домагалася перегляду умов Версальського миру – на німців Померанії та Верхньої Сілезії а Польщі, судетів – у Чехії. Тоді ж, у 30-х рр. XX ст. інформаційні війни перестали бути додатком до збройних і перетворилися на самостійне явище (наприклад, німецько-австрійська радіовійна 1933–1934 рр. з приводу приєднання Австрії до рейху) [7].

За умов трансформації інформаційної боротьби будуть змінюватися також її форми [2].

Так, для інформаційної боротьби першого покоління – це:

1) вогневе придушення (у воєнний час) елементів інфраструктури державного та військового управління;
2) ведення радіоелектронної боротьби;
3) одержання розвідувальної інформації шляхом перехоплення й розшифрування інформаційних потоків;
4) здійснення несанкціонованого доступу до інформаційних ресурсів з наступною їх фальсифікацією чи викраденням;
5) масове подання в інформаційних каналах супротивника чи глобальних мережах дезінформації для впливу на осіб, які приймають рішення;
6) одержання інформації від перехоплення відкритих джерел інформації [7].

Інформаційна боротьба другого покоління передбачає:

1) створення атмосфери бездуховності й аморальності, негативного ставлення до культурної спадщини противника;
2) маніпулювання суспільною свідомістю соціальних груп населення країни з метою створення політичної напруженості та хаосу;
3) дестабілізацію політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції й навіть громадянської війни;
4) зниження рівня інформаційного забезпечення органів влади й управління, інспірацію помилкових управлінських рішень;
5) дезінформування населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;
6) підрив міжнародного авторитету держави, його співробітництва з іншими країнами;
7) заподіяння збитків життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах [7].

IV. Висновки

Інформаційна війна являє собою цілеспрямовані інформаційні впливи в глобалізаційному просторі, що здійснюються суб'єктами впливу на цілі (об'єкти впливу) з використанням інформаційної зброї для досягнення запланованої мети.

Під впливом розуміють переважно вплив на свідомість людей. Тобто інформаційна зброя – спеціально підготована та подана інформація для цільової групи осіб (так звана «пропаганда»). Основна зброя такої «війни» – повідомлення засобів масової інформації та нетрадиційних джерел інформації. Щодо інформаційної зброї, то це сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виведення з ладу функцій або служб інформаційної інфраструктури загалом або окремих її елементів. Основна дія інформаційної зброї – блокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника [8].

В умовах інформаційної війни інформацію розуміють як окремий об'єкт або як потенційну зброю та вигідну мету. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активну протидію в інформаційному просторі. Інформаційна війна – це атака інформаційної функції, незалежно від засобів, які застосовують. Наприклад, бомбардування АТС або виведення з ладу інформаційно-комп'ютерної системи противника – операція інформаційної війни. Щоб операція була ефективною, потрібно виконати такі дії:

1) примусити противника спостерігати за нашими діями;
2) змусити його вважати обман правдою;
3) діяти відповідно до цілей того, хто вводить в оману.

Сучасні засоби виконання інформаційних функцій в умовах глобалізаційних процесів зробили саму інформацію вразливою з погляду доступу до неї та маніпулювання нею. Перш за все, уразливість інформації зумовлена:

1) концентрованим зберіганням інформації, наявністю великих, можна сказати, глобальних, баз даних;
2) швидкістю доступу до інформації, яка здійснюється від кількох секунд до кількох годин;
3) можливістю інформаційних систем працювати автономно [4].

Інформаційна війна в умовах глобалізації полягає також у діях, які розпочаті для досягнення інформаційної переваги шляхом завдання шкоди процесам, що базуються на інформації й інформаційних системах супротивника при одночасному захисті власної інформації. Основні методи інформаційної війни – блокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника.

Оборонні дії в ході інформаційної війни передбачають заходи безпеки, що мають на меті захистити інформацію – не дозволити противнику провести успішну інформаційну атаку на свою країну. Забезпечення операційної й комунікаційної безпеки надають змогу запобігати й виявляти побічні дії ворога, спрямовані на військові інформаційні функції. Навпаки, комп'ютерна безпека потребує дій щодо запобігання, виявлення прямих інформаційних дій ворога та організації контрдій.

Список використаної літератури

1. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. Москва : СИНТЕГ, 1999. 232 с.
2. Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства. *Зарубежное военное обозрение.* 2001. № 8. URL: http://psyfactor.org (дата обращения: 20.04.2018).
3. Дмитриев А. В., Латыпов В. В., Хлопьев А. Т. Неформальная политическая коммуникация. Москва, 1997. 197 с.
4. Леонтьєва Л. Інформаційна війна в епоху глобалізації. URL: http://www.ji-magazine.lviv.ua/-seminary/ 2000/sem13-04.htm (дата звернення: 20.04.2018).
5. Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны : монография. Москва : Горячая линия – Телеком, 2003. 541 с.
6. Манойло А. В. Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта. 2005. URL: http://psyfactor.org/ (дата обращения: 20.04.2018).
7. Присяжнюк М., Жарков Я. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. *Центр воєнної політики та політики безпеки*. 2009. 10 серпня. URL: http://defpol.org.ua (дата звернення: 20.04.2018).
8. Прокофьєва Д. М. Інформаційна війна та інформаційна злочинність. URL: http://www.crime-research.iatp.org.ua/library/Prokop.htm (дата звернення: 20.04.2018).
9. Інформаційна війна. *Вікіпедія*. URL: http://uk.wikipedia.org/wiki/Інформаційна_війна (дата звернення: 20.04.2018).

References

1. Grinyaev, S. N. (1997). Intellectual countering information weapons. Moscow. (in Russian).
2. Grinyaev, S. (2001). Views of US military experts on the conduct of informational conflict. *Foreign Military Review*, 8. Retrieved from: http://psyfactor.org. (in Russian).
3. Dmitriev, A. V., Latypov, V. V., Khlopev, A. T. (1997). Informal political communication. Moscow. (in Russian).
4. Leontievf, L. Information war in the era of globalization. Retrieved from: http://www.ji-magazine.lviv.ua/seminary/ 2000/sem13-04.htm. (in Ukrainian).
5. Manoilo, A. V., Petrenko, A. I., Frolov, D. B. (2003). State information policy in the context of the information-psychological war. Moscow. (in Russian).
6. Manoylo, A. V. (2005). Information-psychological war: factors determining the format of the modern armed conflict. Retrieved from: http://psyfactor.org/ (in Russian).

7. Prysyazhnyuk, M., Zharkov, Ya. (2009). Analysis of means of conducting information struggle against the use of information technologies, forms and methods of their application. *Center for Military Policy and Security Policy*. August 10th. Retrieved from: http://defpol.org.ua. (in Ukrainian).
8. Prokofiev, D. M. Information warfare and information crime. Retrieved from: http://www.crime-research.iatp.org.ua/library/Prokop.htm. (in Ukrainian).
9. Information warfare. *Wikipedia*. Retrieved from: http://uk.wikipedia.org/wiki/Інформаційна_війна. (in Ukrainian).

Стаття надійшла до редакції 04.05.2018.

Стародуб С. А. Информационные войны и системы защиты в условиях глобализационных процессов

Информация XXI в. приобретает материальную форму, и владение нею становится очень востребованным. Любые вполне «материальные» решения сегодня испытываются и реализуются в информационной сфере, а их результаты становятся решающими. Мировое современное глобальное пространство постоянно находится в состоянии войны. Характерной особенностью этой войны является то, что она не кровопролитная, но более разрушительна. Нынешний мир переживает бурное противостояние информационных битв в медиапространстве. Особенностью информационных сражений является постоянный обмен информацией, негативно влияющей на врага.

Ключевые слова: *война, конфликт, боевые действия, информационная война, глобализация, коммуникационные процессы, информация.*

Starodub S. A. Information Wars and Defense Systems in the Context of Globalization Processes

Research methodology. *The basis of the research is informational, systemic, activity approaches. The following methods were used: analysis, synthesis, generalization – to determine possible defense systems during information wars in the context of globalization processes; the terminological analysis of the «information war».*

Results. *Info XXI century selects the shape and material possessions it becomes very desirable. Any quite «material», today tested solutions and implement in the information field, and their results are crucial. World modern global space is always at war. But the characteristic of this war is that it is not bloody, but more destructive. The current world is undergoing rapid information confrontation battles in the media space. A characteristic feature of information battle is a constant exchange of information which adversely affects the enemy.*

Novelty. *The article covers possible defense systems during information wars in the context of globalization processes. Defense aspect of an information war is security measures aimed to information protection – do not let the enemy to execute a successful information assault to Ukrainian information functions. Modern defense measures as operational security and communication security are typical for prevention and identification of enemy's harmful impact, aimed at Ukrainian military information functions. Computer security includes actions for prevention, identification of enemy's direct information actions and organization of counteractions.*

Practical significance. *The research results can be used in a state and individuals level to information policy formation.*

Key words: *war, conflict, warfare, information warfare, globalization, communication processes, information.*