УДК 354.42

Олександр Віталійович Левченко *(канд. військ. наук, професор, провідний експерт)*

Міністерство оборони України, Київ, Україна

КЛАСИФІКАЦІЯ ІНФОРМАЦІЙНОЇ ЗБРОЇ ЗА ЗАСОБАМИ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

Динамічний розвиток інформаційних технологій призвів до появи інформаційної зброї, яка на сьогодні стає найнебезпечнішим інструментом ведення протиборства між державами. За допомогою інформаційної зброї здійснюється вплив на інформаційні ресурси протилежної держави та суспільну свідомість її населення. Відповідно до цього, за цільовою ознакою вона класифікується на інформаційно-технічну зброю, яка впливає на інформаційні ресурси, мережі і системи державного і військового управління та інформаційно-психологічну, яка впливає на психіку, свідомість, підсвідомість, морально-психологічний стан люд`ини, соціальних груп та суспільства в цілому. Разом з тим, види цієї зброї визначаються засобами, які можуть застосуватися. Так, виходячи із засобів інформаційно-технічної зброї, вона поділяється на алгоритмічну, програмну і апаратну, а інформаційно-психологічна зброя – на пропагандистську, психофізичну, нейролінгвістичну, психотропну, психотронну, психогенну і психоаналітичну. Повний опис зазначених засобів наводиться у цій статті.

Ключові слова: *інформаційно-технічна зброя; інформаційно-психологічна зброя, засоби інформаційної зброї.*

Вступ

Постановка проблеми. Динамічний розвиток інформаційних технологій та глобальної мережі Інтернет обумовлює посилення залежності всіх держав світу, у тому числі й України, від застосування у всіх сферах життєдіяльності засобів і технологій, за допомогою яких не лише отримується, обробляється, відбувається обмін інформацією, а й здійснюється цілеспрямований вплив на суспільну свідомість населення та інформаційні ресурси держави. Такий вплив реалізується за допомогою інформаційної зброї, яка на сьогодні стає найнебезпечнішим інструментом ведення протиборства між державами. Саме тому всебічне вивчення питань, пов'язаних з цією зброєю, зокрема її класифікацією, є необхідною умовою для організації як ефективного її застосування, так і протидії їй.

Аналіз останніх досліджень і публікацій. Дослідженню сутності, можливостей та дії інформаційної зброї присвячено чимало праць науковців як за кордоном, так і в Україні. У частині з них розглядаються питання поділу інформаційної зброї за видами, класами групами тощо [1-10]. Проте окремі питання її класифікації на сьогодні ще остаточно не узгоджені. Зокрема, в існуючих дослідженнях розрізнено, неповно і не систематизовано розглядаються засоби інформаційної зброї, якими ведеться інформаційне протиборство між державами. Тому **метою цієї статті** є розроблення найбільш повної, у порівнянні з існуючими, класифікації інформаційної зброї за засобами ведення інформаційної боротьби.

Виклад основного матеріалу дослідження

Науковці відносять до інформаційної зброї широкий клас прийомів і засобів інформаційного впливу на противника – від дезінформації і пропаганди до засобів радіоелектронної боротьби [1–6]. Автор пропонує найбільш узагальнене визначення цього терміну. *Інформаційна зброя – це сукупність способів, прийомів, засобів і технологій інформаційного впливу на інформаційну інфраструктуру супротивної держави та психіку, свідомість і підсвідомість її населення та особового складу збройних сил.* Зазначена сукупність поділяється за різними ознаками, які пропонуються у відомих дослідженнях. Однією з найбільш повних можна вважати таку класифікацію інформаційної зброї [11]:

1) за метою застосування: зброя для цілеспрямованого формування складових морально-семантичного фільтра соціальних об'єктів (системи цінностей, пріоритетів, системи інтересів тощо); зброя для нав'язування супротивній стороні бажаних рішень і поведінки; зброя для ускладнення умов прийняття рішень супротивною стороною; зброя для зриву функціонування технічних та соціотехнічних систем (автоматизованих систем управління; інформаційно-телекомунікаційних систем та ін.); зброя для добування інформації про супротивну сторону тощо;

2) за об'єктами впливу: зброя впливу на соціосистеми (людина, соціальні групи, суспільство, країни); зброя впливу на соціотехнічні системи (автоматизовані системи управління, інформаційно-телекомунікаційні системи, Інтернет тощо); зброя впливу на технічні системи (системи управління технологічними лініями, загальносистемне програмне забезпечення, перехоплення управління безпілотними засобами ураження та ін.); зброя впливу на інші об'єкти інформаційної інфраструктури;

3) за механізмами реалізації впливу: зброя, що базується на реалізації механізмів вербального впливу на людину та соціосистеми; зброя, що базується на реалізації механізмів невербального впливу на людину та соціосистеми; зброя, що базується на реалізації механізмів впливу на функціонування математично-програмного забезпечення ЕОМ; зброя, що базується на

реалізації механізмів випромінювання енергії різної природи;

4) за реалізованими методами впливу: зброя, що базується на реалізації методів інтелектуального характеру (методи дезінформування, нейролінгвістичного програмування, рефлексивного управління та ін.); зброя, що базується на реалізації методів психологічного впливу на людину, суспільство; зброя, що базується на реалізації методів психофізіологічного впливу на людину, суспільство; зброя, що заснована на реалізації методів технічного характеру;

5) за характером впливу на інформацію та інформаційні процеси: зброя руйнівного характеру; зброя спотворювального характеру; зброя модифікуючого характеру;

6) за масштабом вирішуваних бойових завдань: стратегічна зброя; оперативно-тактична зброя; тактична зброя;

7) за терміном дії: зброя короткострокової дії; зброя довгострокової дії.

Разом з тим найбільш важливою у поділі інформаційної зброї на види, класи, групи тощо вбачається цільова ознака. Саме мета застосування тієї чи іншої зброї вказує на наслідки її дії, що, у підсумку, дає змогу адекватно визначити інформаційні загрози і своєчасно прийняти заходи протидії. Виходячи з цього, розроблено класифікацію інформаційної зброї за цільовим призначенням.

Встановлено, що цільове призначення інформаційної зброї полягає у:

1) впливі на компоненти радіоелектронного обладнання (у т.ч. систему його електроживлення), інформаційні системи і мережі та їх програмно-математичне забезпечення, а також процеси обміну інформацією. Наслідками такого впливу можуть бути:

тимчасове або повне виведення з ладу окремих компонентів радіоелектронних систем;

нав'язування асоціальних моделей поведінки, стандартизації шаблонів мислення, прищепленні елементів чужого мислення та менталітету;

маніпуляція громадською думкою, суспільною свідомістю та інформацією у засобах масової інформації.

Відповідно до цільового призначення інформаційна зброя поділяється на інформаційно-технічну та інформаційно-психологічну (рис. 1).

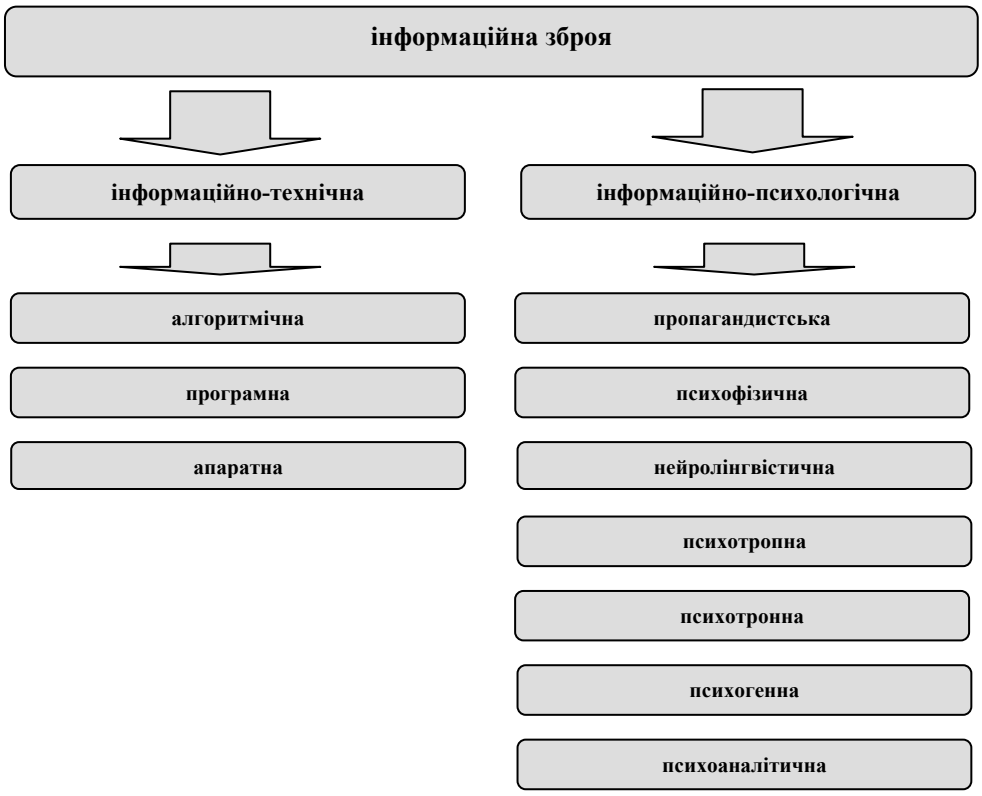

Рис. 1. Класифікація інформаційної зброї

Інформаційно-технічна зброя – це зброя, яка впливає на інформаційні ресурси, мережі і системи державного і військового управління. Вона поділяється на:

алгоритмічну, яка призначена для виведення з ладу або зміни алгоритму функціонування програмного забезпечення інформаційних систем, ресурсів і мереж;

програмну, яка призначена для руйнування, спотворення (довільним чином) кодів програм, блокування та підміни (фальсифікації) масивів інформації, а також нейтралізації тестових програм і систем захисту інформаційних ресурсів;

апаратну, яка призначена для тимчасового або повного виведення з ладу окремих компонентів радіоелектронних систем,

компонентів радіоелектронного обладнання (у т.ч. систем їх електроживлення), а також дезорганізації функціонування підсистем обміну інформацією та впливу на середовище розповсюдження сигналів.

Інформаційно-технічна зброя має певні засоби, завдяки яким вона реалізовується на практиці. Основні засоби інформаційно-технічної зброї наведені у табл. 1.

Таблиця 1

Основні засоби інформаційно-технічної зброї

Види інформаційно-технічної зброї	Засоби інформаційно-технічної зброї
Алгоритмічна	засоби впливу на інформаційні системи і мережі та їх програмно-математичне забезпечення
	засоби подолання систем захисту інформації для отримання можливості несанкціонованого доступу до інформаційних ресурсів
	засоби виведення з ладу конкретного програмного забезпечення інформаційної системи (у визначений момент часу або внаслідок виконання певної операції у системі)
	засоби впливу на системи охорони об'єктів
Програмна	комп'ютерні віруси (завантажувальні, файлові, макровіруси, резидентні, нерезидентні, поліморфні, віруси-невидимки, з деструктивними функціями, безпекові)
	засоби несанкціонованого доступу (різноманітне несертифіковане програмне забезпечення, троянські програми)
	програмні закладки (логічні бомби, логічні люки, програмні пастки, програмні черв'яки, дослідники, перехоплювачі, руйнівники, активні завади, асоційовані з програмно-апаратним середовищем, асоційовані з програмами первинного завантаження, асоційовані з завантаженням операційної системи, асоційовані з прикладним програмним забезпеченням, модулі, що містять тільки код закладки, модулі-імітатори, що збігаються з однією з програм, замасковані під програмні засоби)
Апаратна	засоби примусового радіоелектронного придушення (РЕП)
	надпотужні генератори НВЧ, вибухомагнітні генератори, засоби силового впливу через мережу електроживлення
	засоби впливу на джерела безперервного живлення
	засоби впливу на протоколи передачі даних в інформаційних мережах
	засоби виведення з ладу обладнання (резонанс головок жорстких магнітних дисків, випалювання моніторів)
	засоби впливу на алгоритми адресації та маршрутизації
	засоби перехоплення та порушення проходження інформації у технічних каналах її передачі
	апаратні закладки, що вбудовані у складові частини електронно-обчислювальної техніки та периферійного обладнання

Інформаційно-психологічна зброя – це зброя, яка впливає на психіку, свідомість, підсвідомість, морально-психологічний стан людини, соціальних груп та суспільства в цілому. Вона поділяється на:

пропагандистську, яка призначена для здійснення інформаційно-психологічного впливу, спрямованого на закріплення бажаних уявлень, звичок, переконань у людини (соціальної групи), або навпаки – руйнування небажаних уявлень, звичок та переконань;

психофізичну, яка призначена для здійснення інформаційного і (або) енергетичного впливу на психічні функції і на роботу фізіологічних органів і систем людини;

нейролінгвістичну, яка призначена для управління людською свідомістю та поведінкою за допомогою лінгвістичних конструкцій, набору певних символів, кольорів, звуків, архетипів, візуальних зображень тощо;

психотропну, яка призначена для впливу на мозок людини, збудження або зниження процесів мислення і сприйняття інформації за рахунок використання механізму зміни біохімічних характеристик процесів, що перебігають у нервовій системі людини;

психотронну, яка призначена для впливу спеціальними технічними засобами на свідомість та підсвідомість людини з метою зниження її волі, пригнічення, тимчасового виведення з ладу, зомбування тощо;

психогенну, яка призначена для внесення змін у нервово-психічну діяльність мозку людини;

психоаналітичну, яка призначена для впливу на підсвідомість людини терапевтичними засобами, зокрема у стані гіпнозу та глибокого сну з навіюванням їй необхідних установок тощо.

Основні засоби інформаційно-психологічної зброї наведені у табл. 2.

Основними особливостями інформаційної зброї можна вважати:

масштабність – можливість завдання значних збитків економіці та воєнному потенціалу держави;

універсальність – можливість багатоваріантного застосування як військовими, так і цивільними структурами проти об'єктів державного та військового управління;

Таблиця 2

Основні засоби інформаційно-психологічної зброї

Види інформаційно-психологічної зброї	Засоби інформаційно-психологічної зброї
Пропагандистська	засоби масової інформації: друковані, аудіовізуальні, електронні
	синтезатори (генератори) голографічних та звукових ефектів в атмосфері
	віртуальні інформаційно-психологічні засоби, комп'ютерні ігри; лінгвістичні засоби тощо
Психофізична	техногенні засоби цілеспрямованого інформаційного і (або) енергетичного впливу на психічні функції і на роботу фізіологічних органів і систем людини
Нейролінгвістична	засоби нейролінгвістичного програмування (НЛП)
	лінгвістичні конструкції, набори певних символів, кольорів, звуків, архетипів
	спеціальна відеографічна та телевізійна інформація (ефект "25" кадру)
Психотропна	антидепресанти, хімічні та наркотичні речовини, спеціальні лікарські та фармакологічні препарати
Психотронна	психотронні генератори надвисокочастотного випромінювання, генератори звукових коливань, інфразвуку, ультразвуку
	засоби створення віртуальної реальності, що негативно впливають на свідомість людини та спонукають до виникнення страху, втрати свідомості тощо
Психогенна	засоби фізичного впливу на мозок людини звуками та кольорами, що позбавляють здатності раціонально мислити
	засоби впливу навколишніх умов (фактори або шокуючі події, численні жертви тощо), що позбавляють здатності раціонально діяти
Психоаналітична	засоби впливу на підсвідомість людини терапевтичними препаратами у стані гіпнозу та глибокого сну

економічність – низька собівартість та вигідне співвідношення витрат порівняно з наслідками її застосування.

Але найбільш важливою відмінністю інформаційної зброї від звичайних засобів ураження є знеособлений характер її дії та прихованість застосування.

Висновки й перспективи подальших досліджень

Особливу небезпеку інформаційна зброя становить для інформаційних ресурсів, комп'ютерних систем і мереж органів державного управління, фінансових та банківських установ, систем управління військами і зброєю, а також для психіки, свідомості і підсвідомості населення та особового складу збройних сил. При цьому, за своєю результативністю і наслідками застосування, інформаційна зброя прирівнюються до зброї масового ураження. Тому володіння в сучасних умовах ефективною інформаційною зброєю і засобами захисту від неї є одним із пріоритетних напрямів забезпечення національної безпеки в інформаційній сфері.

Напрямом подальших досліджень доцільно вважати розроблення на основі наведеної у цій статті класифікації способів застосування, виявлення і протидії інформаційній зброї.

Література

1. Жук С. Я. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С. Я. Жук, В. О. Чмельов, Т. М. Дзюба // Наука і оборона. – 2006. – №2. – С. 35–41. **2. Рось А. О.** Інформаційна зброя: сутність і засади класифікації / А. О. Рось , С. М. Пустовіт, І. В. Замаруєва, Г. В. Подобедов // Труди академії. – 1999. – №18. – С. 84–98. **3. Богуш В.М.** Інформаційна безпека: Термінологічний навчальний довідник / Богуш В. М., Кривуца В. Г., Кудін А. М. ; за ред. Кривуци В. Г. – К. : ООО "Д.В.К. ", 2004. – 508 с. **4. Словник** основних термінів у галузі інформаційної безпеки держави у воєнній сфері / [уклад. А. Рось та ін.]; за ред. В. М. Телелима. – К. : НУОУ, 2012. – 54 с. **5. Соловцов Н. Е.** Классификация и способы применения "информационного оружия" / Н. Е. Соловцов, Б. И. Глазов, Д. А. Ловцов // Стратегическая стабильность. – 1999. – №4. – С. 17–22. **6. Война** в киберпространстве: уроки и выводы для России // Независимое военное обозрение. – №46(787). – 2013. – С. 1–4. **7. Ожеван М.А.** Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії / **М. А. Ожеван** // Стратегічні пріоритети. – 2011. – №3. – С. 118–126. **8. Сучасні** технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій / [Петрик В. М., Остроухов В. В. та ін.] – К. : Росава, 2006. – 208 с. **9. Інформаційна** безпека держави у контексті протидії інформаційним війнам: навчальний посібник / [Толубко В. Б., Рось А. О., ЯвтушенкоА. М., Жарков Я. М. та ін.] ; за ред. Толубка В. Б. – К. : НАОУ, 2004. – 176 с. **10. Руснак І. С.** Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І. С. Руснак, В. М. Телелим // Наука і оборона. – 2000. – №2. – С. 18–23. **11. Інформаційна** безпека держави у воєнній сфері: навчальний посібник / [Рось А. О., Биченок М. М., Віщун В. В., Дзюба Т. М., Замаруєва І. В., Катін П. Ю., Шемаєв В. М.] – К.: НУОУ, 2011. – 324 с.

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННОГО ОРУЖИЯ ПО СРЕДСТВАМ ВЕДЕНИЯ ИНФОРМАЦИОННОЙ БОРЬБЫ

Александр Витальевич Левченко *(канд. воен. наук, профессор, ведущий эксперт)*

Министерство обороны Украины, Киев, Украина

Динамичное развитие информационных технологий привело к возникновению информационного оружия, которое сегодня становится опаснейшим инструментом ведения противоборства между государствами. При помощи информационного оружия осуществляется влияние на информационные ресурсы противостоящего государства и общественное сознание его населения. В соответствии с этим, по целевому признаку оно классифицируется на информационно-техническое оружие, которое влияет на информационные ресурсы, сети и системы государственного и военного управления и информационно-психологическое, которое влияет на психику, сознание, подсознание, морально-психологическое состояние человека, социальных групп и общества в целом. Вместе с тем, виды этого оружия определяются применяемыми средствами. Так, исходя из средств информационно-технического оружия, оно подразделяется на алгоритмическое, программное и аппаратное, а информационно-психологическое оружие – на пропагандистское, психофизическое, нейролингвистическое, психотропное, психотронное, психогенное и психоаналитическое. Полное описание названных средств приводится в этой статье.

Ключевые слова: *информационно-техническое оружие; информационно-психологическое оружие, средства информационного оружия.*

INFORMATION WEAPON CLASSIFICATION ACCORDING TO THE METHODS OF CONDUCTING INFORMATION WARFARE

Oleksandr V. Levchenko *(Candidate of Military Sciences, Professor, Leading Expert)*

Ministry of Defense of Ukraine, Kyiv, Ukraine

Dynamic development of information technology has led to the development of informational weapon which is becoming the most dangerous tool of warfare between states. With the help of informational weapons can be conduct influence on informational resources of the hostile states and public opinion of the population. In accordance with it, informational weapon classified as information and technical weapon that affect the information resources, networks and systems of government and military management and as information-psychological weapon that affects the mental sphere, consciousness, subconsciousness, moral and psychological status of the social groups and society as a whole. At the some time, the types of informational weapons are defined by the ways of its usage. Also information weapon are subdivided on algorithmic, software and hardware, and information-psychological weapon which include propaganda, psychophysical, neurolinguistic, psychotropic, psychotronic, psychogenic and psychoanalytic ones. Complete description of these weapons is provided in this article.

Keywords: *information technology weapons, information and psychological weapons, means of information weapons.*

References

1. Zhuk S.Y., Chmelev V.O., Dzuba T.M. (2006), Tendency and perspectives of the development informational warfare and weapon. [*Tendeciy ta perspectivy rozvytku informacsynoi borotby i informaciynoi zbroi*], Nauka i oborona, Kiev, No. 2, pp. 35–41. **2. Ros A.O.**, Pustovit S.M., Zanarueva I.V., Pobedov G.V. (1999), Information weapon – content and classification. [*Informaciynaya zbroya: sutnist i zasady klasyficatsiy*], Trudy akademiy, Kiev, No. 18, pp. 84–98. **3. Bogush V.,** Kryvutsa V., Kudin A. (2004), Information security: reference book of terminology. [*Informacivnava bezpeka: Terminologichniy navchalniy dovidnyk*], Kiev, 508 p. **4. Telelym V.M.,** Ros A.O. (2012), Dictionary of the general definitions in the military sphere of information security of the state. [Slovnyk osnovnyh terminiv u galuzi informaciynoi bezpeky derzgavy u voenniy sferi], Kiev, 54 p. **5. Solovtsov N.E.,** Glazov B.I., Lovtsov D.A. (1999), Classification and the ways of use "information weapon. [*Klassifikaciya i sposoby primenenija* "informacionnogo oruzhija"], Strategicheskaya stabilnost, Moskva, No. 4, pp. 17–22. **6. The war** in cyberspace – lessons learned for Russia, (2013), [*Voina v kiberprostranstve: uroki i vyvody dla Rossii*], Nezavisimoe voennoe obozrenie, No. 46(787), pp. 1–4. **7. Ozhevan M.A.** (2011), General directions of outside information and manipulation affect on public transformation in Ukraine: countermeasures. [*Osnovni naprjamy zovnishnih informacijno-manipulacijnyh vpliviv na suspilstvo transformacii Ukrainy: zasoby protydiij*], Strategichni stereotypy, No. 3, pp. 118–126. **8. Petrik V.,** Ostrouhov, V. (2006), Modern technologies and means for mental manipulation, conducting information warfare and special information operations. [*Suchasni tehnologii ta zasoby manipuluvanija svidomistju, vedenja informacijnih viyn i specialnih informacijnih operacij*], Kiev, 208 p. **9. Tolubko V**., Ros A., Yavtushenko A., Zharkov Y. (2004), Information security of the state as a ground for information warfare countermeasures: student textbook. [*Informacijnaja bezpeka derzhavy u kontexti protydij informacijnim vijnam: navchalnij posibnik*], Kiev, 176 p. **10. Rusnak I.S**., Telelym V.M. (2000), Development the forms and methods of conducting information warfare in nowadays. [*Rozvitok form i sposobiv vedenja informacijnoi borotby na suchasnomu etapi*], Nauka i oborona, Kiev, No. 2, pp. 18–23. **11. Ros A.,** Bychenko M., Vischun V., Dzjuba T., Zamarueva I., Katin P., Shemaev V. (2011), Information security of the state in the military sphere: student textbook. [*Informacijnaja bezpeka derzhavy u voenniy sferi: navchalnij posibnik*], Kiev, 324 p.

O.V. Levchenko: levch@i.ua

Отримано: 10.06.2014 р.