

ІНФОРМАЦІЙНА БЕЗПЕКА

УДК 355.48

В.Г. Панін, канд. техн. наук,  
О.М. Борзак, С.П. Лалетін

РІЗНОВИДИ ТА ТЕНДЕНЦІЇ РОЗВИТКУ ІНФОРМАЦІЙНОЇ ЗБРОЇ

*Розглянуто особливості, різновиди та тенденції розвитку інформаційно-технічної та інформаційно-психологічної зброї.*

*Ключові слова: інформаційна зброя, фізична зброя, інформаційно-психологічна зброя.*

*Peculiarities, kinds and tendencies of informational-technical and informational-psychological weapons development were analyzed in the article.*

*Keywords: information, weapon, physical weapon, and psychological weapon.*

Як свідчить досвід локальних війн і збройних конфліктів в сучасній війні неможливо досягти поставлених цілей без постійного здійснення заходів інформаційної боротьби не тільки в ході, але ж ще задовго до її початку та після завершення. Тому фахівці виділяють як самостійний вид зброї – інформаційну зброю, яка розглядається як засоби ведення інформаційної боротьби. Враховуючи багатогранність заходів інформаційної боротьби [1], інформаційну зброю можна визначити як сукупність засобів і технологій, призначених для негативного впливу на інформацію та інформаційні процеси в соціальних, соціотехнічних та технічних системах. Критерієм віднесення до розряду інформаційної зброї може розглядатися ефективність того чи іншого озброєння при вирішенні завдань інформаційної боротьби.

Класифікація інформаційної зброї може бути проведена за наступними напрямками [1]: за метою застосування; за об'єктами впливу; за механізмами реалізації впливу; за характером впливу на інформацію та інформаційні процеси; за масштабом вирішуваних завдань; за терміном дії тощо.

За об'єктами впливу інформаційну зброю можна поділити на два основних класи [2]:

1. Інформаційно-технічна зброя, що впливає на інформаційні ресурси, інформаційну інфраструктуру збройних сил, держави в цілому.

2. Інформаційно-психологічна зброя, що впливає на морально-психологічний стан людини, соціальних та інших груп населення, суспільства в цілому.

Інформаційна зброя може характеризуватись такими показниками, як цілеспрямованість, вибірковість, розосередженість, масштабність впливу, досяжність, швидкість доставки, комплексність впливу на людей, технічні засоби і системи, можливість регулювання (дозування) "потужності" впливу тощо. Їй притаманні такі особливості [1,3]: скритність, масштабність, універсальність, економічність.

Окремі різновиди інформаційна зброя можуть бути віднесені до асиметричної зброї, проти якої традиційні системи захисту не спрацьовують або система захисту взагалі відсутня [3]. Це дозволяє наносити значні збитки більш сильному за традиційними видами озброєння противнику.

Як свідчить досвід локальних війн і збройних конфліктів кінця XX, початку XXI століття, на відміну від ударної високоточної зброї, яка вражає точечні спеціально вибрані важливі об'єкти, інформаційна зброя є системоруйнуючою. Тобто вона виводить з ладу цілі бойові, економічні і соціальні системи. За результатами впливу інформаційна зброя може бути співставлена зі зброєю масового знищення.

Інформаційно-технічна зброя визначається як засоби знищення, викривлення або викрадення інформаційних масивів, добування з них необхідної інформації

після подолання системи захисту, обмеження або заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів, виводу з ладу телекомунікаційних мереж, комп'ютерних систем, усіх засобів високотехнологічного забезпечення життя суспільства і функціонування держави [4].

За принципом дії можна виділити наступні види інформаційно-технічної зброї: фізична, радіоелектронна, програмно-технічна.

Фізична зброя – засоби вогневої поразки та фізичного знищення важливих елементів систем управління і зв'язку противника та елементів його інформаційної інфраструктури. Однак більш коректним було б віднести до інформаційної зброї фізичного впливу засоби, призначені винятково для впливу на елементи інформаційної системи: протирадіолокаційні ракети, засоби генерації електромагнітного імпульсу, графітові бомби, біологічні і хімічні засоби впливу на елементну базу.

Радіоелектронна зброя – засоби радіоелектронної боротьби та радіоелектронної розвідки. Основним призначенням такої зброї є контроль інформаційних ресурсів потенційного супротивника і приховане чи явне втручання в роботу його систем управління і зв'язку з метою їх дезорганізації, порушення нормального функціонування чи виводу з ладу.

Програмно-технічна зброя – засоби несанкціонованого доступу до інформаційних ресурсів з подальшим їх викривленням, знищенням або викраденням, порушення нормального функціонування комп'ютерно-телекомунікаційних мереж.

Засоби несанкціонованого збору інформації дозволяють здійснити несанкціонований доступ до комп'ютерних систем, визначати коди доступу, ключі до шифрів чи іншу інформацію про зашифровані дані. До них відносяться програмні продукти типу "KNOWBOT" та "TRAP DOOR". Програмні продукти типу "KNOWBOT" (пошуковий робот) здатні переміщуватися в інформаційній мережі від комп'ютера до комп'ютера і при цьому розмножуватися, створюючи копії. Знайшовши цікавлячу його інформацію, "KNOWBOT" залишає в цьому місці свою копію, що збирає інформацію й у визначений час передає її. З метою виключення виявлення в програмних продуктах такого типу можуть бути передбачені функції самопереміщення і самознищення.

Програмні продукти типу "TRAP DOOR" (програми-пастки, програми-закладки) призначені для збору та передачі інформації про ключі даних та паролі. Вони, звичайно, вмонтовуються в програмні продукти широкого вжитку (офісні та сервісні програми, операційні системи, локальні модулі онлайн-комп'ютерних ігор тощо).

Створені і постійно модернізуються спеціальні технічні пристрої, що дозволяють зчитувати інформацію з моніторів комп'ютерів. Перспективним є також створення мініатюрних спеціалізованих комплексів збору, об-

робки і передачі інформації, що можуть впроваджуватися під видом звичайних мікросхем до складу всіляких радіоелектронних пристроїв.

Засоби перекручування і знищення інформації включають численні комп'ютерні віруси. Особливу небезпеку становлять останні різновиди вірусів типу "WORM", які, на відміну від звичайних вірусів, являють собою не закінчену програму, а набір стандартних команд операційної системи (сценарій), що значно ускладнює процеси їх знаходження та нейтралізації.

До засобів порушення функціонування комп'ютерно-телекомунікаційних мереж відносяться "Логічні бомби", "Бомби електронної пошти", атаки на відмову в обслуговуванні (DoS attacks) і т.д.

В окремий різновид програмно-технічної зброї відносяться програмні продукти типу "TROJAN HORSE" (троянський кінь). Програмні продукти даного типу здатні відкривати повний доступ до цікавлячого комп'ютера при роботі в мережах різного типу.

Інформаційна зброя як і інформаційна боротьба з розвитком суспільства та інформаційних технологій набули відповідних змін. Аналіз досвіду сучасних локальних війн і збройних конфліктів дозволяє визначити основні тенденції розвитку інформаційно-технічної зброї (табл. 1).

До 1991 року використовувалися традиційні засоби радіоелектронної боротьби, вогневого ураження, які були спрямовані на дезорганізацію систем управління військами, введення противника в оману.

Наступний етап розвитку інформаційної зброї пов'язаний з цифровою революцією. З'являється програмно-комп'ютерна зброя і всі її різновиди.

На перспективу, враховуючі, що розвиток сучасної комп'ютерної техніки підійшов до створення штучного інтелекту, очікується поява "інтелектуальної" інформаційно-технічної зброї, нових її зразків на базі нано- та біотехнологій.

Таблиця 1

Період до 1991 р.	Період 1991–2004 рр.	Перспективи
Засоби РЕБ, засоби вогневого ураження об'єктів інформаційної інфраструктури збройних сил, засоби входження в радіомережі противника, засоби оперативного маскування.	Комп'ютерна зброя (комп'ютерні віруси, програмні закладки, логічні бомби); засоби імпульсної поразки (електронні бомби, електромагнітні генератори).	Зброя на засадах штучного інтелекту, нано- та біотехнологій, семантичні віруси, технології боротьби в комп'ютерних мережах на базі квантової фізики та теорії хаосу, мікрохвильова енергетична зброя.

Під інформаційно-психологічною зброєю розуміють засоби і технології, які реалізують інформаційні по своїй природі впливи на психіку, в першу чергу свідомість особи, соціальних груп, з метою впровадження необхідних ідеологічних і соціальних установок, формування помилкових стереотипів поведінки та прийняття рішень, трансформації в потрібному напрямку їхніх настроїв, почуттів, волі.

На сьогодні, за механізмами реалізації фахівці виділяють наступні види психофізичних впливів на психіку особи /5/: пропагандистський, нейролінгвістичний, психоаналітичний, психотронний, психотропний, психогенний – перші чотири з яких мають безпосередньо інформаційну основу.

Пропагандистський та нейролінгвістичний впливи на об'єкти може здійснюватись: друкованими засобами; електронними засобами; безпосереднім (опосередкованим) спілкуванням.

Психоаналітичний вплив здійснюється шляхом безпосереднього спілкування, а також за допомогою електронних засобів.

Новітнім видом інформаційно-психологічної зброї є психотронна зброя [2]– спеціальні технічні засоби (психотронні генератори), які використовують вплив так званих енергоінформаційних полів. Окремо розглядають психотронні генератори, психотронні формують генератори, спінорні генератори, ретранслятори енергії космосу, багатополлярні генератори. До психотронної зброї також відносять людей, наділених особливими якостями, які здатні приховано здійснювати

вплив на інших людей на відстані з метою управління їх поведінкою.

Психотронна та психогенна зброя безпосередньо не використовують інформаційні впливи. Але ж кожна з них впливає на стан свідомості особи, спроможність обробляти інформацію і приймати рішення. Крім того, ці види впливу можуть використовуватись в різних комбінаціях з іншими видами інформаційно-психологічного впливу чим підсилюють загальний ефект. Різні комбінації психофізичних впливів складають основу нелетальної зброї XXI століття [2].

Аналіз різновидів інформаційно-психологічної зброї свідчить як про надзвичайну небезпечність і різноманітність її видів, так і про небезпечність і різноманітність каналів її впливу – від засобів масової інформації до технологій та засобів впливу на свідомість і підсвідомість людей, що вкрай небезпечно у зв'язку з практичною відсутністю засобів контролю цих процесів.

Аналіз досвіду сучасних локальних війн і збройних конфліктів дозволяє також визначити основні тенденції розвитку інформаційно-психологічної зброї (табл. 2).

До 1991 року використовувалися традиційні засоби і технології інформаційно-психологічного впливу на війська, населення противника.

Наступний етап розвитку інформаційної зброї також обумовлений бурхливим розвитком інформаційних технологій. Для здійснення інформаційно-психологічного впливу використовуються Інтернет – технології, телерадіотрансляційні комплекси повітряного базування "Командо Соло", цифрові синтезатори мови, голографічні генератори тощо.

Таблиця 2

Період до 1991 р.	Період 1991–2004 рр.	Перспективи
ЗМІ, засоби радіо-, теле-, звукомовлення, засоби залистування (авіаційні, артилерійські).	Інтернет, телерадіотрансляційні комплекси повітряного базування "Командо Соло", технології рефлексивного керування противником, технології нейролінгвістичного програмування та зомбування особи, соціальних груп; голографічні генератори, синтезатори мови.	Психотронна зброя (акустичні, електромагнітні, біологічні генератори, комп'ютерні психовіруси); сомато-психологічна зброя (засоби створення дискомфорту, тепла зброя), генетична зброя, етнічна зброя.

На перспективу, очікується розвиток як вже існуючих засобів і технологій інформаційно-психологічного впливу на людину і суспільство, так і принципово нових їх різновидів, як наприклад, одного з найбільш небезпечних видів нелетальної зброї – психотронної зброї.

За оцінками експертів інформаційна зброя є одною з головних загроз не тільки інформаційній, але й національній безпеці держави взагалі [7]. На сьогодні, вже десятки країн планують і здійснюють різноманітні інформаційні операції. А сумарні витрати на розробки в галузі інформаційної зброї в світі перевищують 120 млрд доларів на рік.

УДК 159.9.075

В.В. Вітковський, здобувач

## СПЕЦІАЛЬНА ПРОПАГАНДА РАДЯНСЬКИХ ВІЙСЬК НА ТЕРЕНАХ УКРАЇНИ У РОКИ ВЕЛИКОЇ ВІТЧИЗНЯНОЇ ВІЙНИ

*Проведено ретроспективний аналіз ефективності інформаційно-психологічного впливу на особовий склад військ противника за результатами спеціальної пропаганди Червоної Армії на землях України в 1941–1944 роках.*

*Ключові слова: інформаційно-психологічний вплив, спеціальна пропаганда.*

*Make getrospective analyses of the informational-psychological influence on enemy troops persounel based on the results of the Red Army special propaganda across the lands of Ukraine in 1941–1944.*

*Keywords: information-psychological influence, a special promotion.*

**Вступ.** Розвиток Збройних Сил України у контексті умов інформаційного суспільства вимагає посиленої уваги аспектам інформаційно-психологічного впливу (далі ІПВ) на соціальні об'єкти. Особливу вагу цей фактор набув в умовах збройних конфліктів сучасності. Проблема історичного дослідження ІПВ під час воєнних дій набуває останнім часом особливої актуальності. Вона вийшла на чільне місце у світлі недавніх подій в Іраку, Афганістані, Єгипті, Лівії та в інших країнах Північної Африки та Близького Сходу.

Актуальність теми також полягає у її значущості для активізації діяльності військовослужбовців у якості об'єктів ІПВ для досягнення морально-психологічної переваги над противником. Важливим є розгляд поєднання форм і методів збройної боротьби з ІПВ, а також узагальнення досвіду ІПВ для Збройних Сил України [8].

Особливістю роботи є виділення невирішених досі питань організації ІПВ на вояків Вермахту, як частини загальної проблеми проведення радянської військової спеціальної пропаганди (далі СП) [1]. Важливо дослідити, як відбулося трансформування німецької армії із зразкової машини швидкої агресії та окупації цілого ряду країн у дезорганізоване, деморалізоване та постійно і майже безперервно відступаюче військо [2]. Вимагаючи надмірного морально-психічного напруження, високого професіоналізму, засобами ІПВ, зокрема СП, вдалося сприяти перелому у ході війни. Відтак, не в останню чергу цей перелом відбувся саме у свідомості військовослужбовців. Тому, підвищення ефективності професійної діяльності особового складу Збройних Сил України значно залежить від запобігання виникненню та своєчасному виявленню негативних психічних станів, що зумовлені сукупністю причинно-наслідкових зв'язків із системою факторів впливу оточення на людину. Одним із цих факторів є ІПВ [11].

Аналіз теоретичних і джерельних досліджень [1–4, 6–8, 10] з вивчення ІПВ загалом та діяльності органів інформаційної боротьби, дозволяє стверджувати, що цей спеціальний ІПВ має бути одним із факторів успішності службової діяльності особового складу Збройних Сил України.

**Постановка проблеми.** Таким чином, важливість і актуальність проблеми та недостатня її розробленість зумовили вибір теми дослідження. Виходячи з цієї теми,

1. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): Монографія. – К.: НАОУ, 2003. – 320с. 2. Прокоф'єв В.Ф. Тайное оружие информационной войны: атака на подсознание. – М.: СИНТЕЗ, 2003. – 408с. 3. Монойло А.В., Петренко А.И., Фролов О.Б. Государственная политика в условиях информационно-психологической войны. – М.: Горячая линия. Телеком, 2003. – 541с. 4. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. – Санкт-Петербург: Фонд "Университет", 2000. – 428 с. 5. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003. 6. Крысько В. Секреты психологической войны (цели, задачи, методы, формы, опыт) / Под общей редакцией А.Е.Тараса. Мн.: Харвест, 1999. – 448с. 7. Толубко В.Б., Жук С.Я., Косевцов В.О. Концептуальні основи інформаційної безпеки України // Наука і оборона. – 2004. – №2. – С. 19-25.

Надійшла до редколегії 24.05.12

метою дослідження є: узагальнення досвіду ІПВ СП Червоної Армії (далі СП ЧА) на військовослужбовців противника; виявлення закономірностей ІПВ в особливих умовах; розроблення рекомендацій щодо застосування кращого досвіду СП ЧА у Збройних Силах України.

Наукові завдання дослідження полягають в: аналізуванні СП, як складової ведення воєнних дій; визначенні впливу СП на підвищення ефективності бойових дій; узагальненні досвіду ІПВ СП на війська III-го Рейху та його союзників; розробці пропозицій щодо його ефективного застосування у Збройних Силах України.

**Об'єкт дослідження:** спецпропаганда ЧА як елемент інформаційно-психологічного протидіювання за Україну у ході світової війни. Предмет дослідження: радянська військова СП сьомого відділу ГПУ ЧА на землях України у роки Великої Вітчизняної війни.

Пропаганда, як процес, являє собою поширення певних ідей, поглядів чи ідеологій. Часто пропаганда є засобом конкретної політики. Головними інструментами пропаганди є засоби масової інформації та комунікації. Пропаганда – це цілеспрямовані, систематичні заходи формування потрібного сприйняття, маніпулювання свідомістю та спрямовування поведінки людей у необхідний для пропагандиста напрям. Спецпропаганда є складовою та напрямом пропаганди, яка спрямована на війська противника з метою їх деморалізації. Тому саме СП стала найважливішим засобом ведення боротьби на ідеологічному фронті. Її головною зброєю є слово. СП впливала на ворога простим словом для досягнення комплексної мети – тиснути психічно, накопичувати та підсилювати відчуття песимізму і відчаю, невпевненості, підсилювати та поглиблювати настрої поразки, змушувати солдатів ворога сумніватися у доцільності спротиву.

На війні сучасної епохи, на жаль, не має місця для шляхетної поведінки. Тому для перемоги над ворогом використовують усі можливі засоби та методи, у тому числі й маніпулювання свідомістю. У часи Другої світової війни цим займалися усі сторони.

Пропаганда, навіть спеціальна, сама по собі не в змозі визначати або змінювати хід війни. Вона здатна послабити та морально добити лише програвшого противника. Тому з початку війни радянській СП було особливо важко. Дійсно, хто ж із німецької наступаючої армії буде здаватися у полон? Так, наприклад, одна з