УДК 355/359.07 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/27-34

Зубков В. П. (0000-0003-1616-2795)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Механізм впливу на інформаційні системи противника як складова інформаційного забезпечення сил оборони України

Резюме. У статті аналізується сутність інформаційно-технічного впливу на інформаційні системи противника як складової інформаційного забезпечення сил оборони України. За результатами аналізу пропонуються механізм реалізації інформаційно-технічного впливу як інструмента інформаційної зброї та підходи до подальшого його вдосконалення.

Ключові слова: інформаційне забезпечення; інформаційна зброя; інформаційно-технічний вплив.

Постановка проблеми. У XXI столітті глобалізація та стрімкий розвиток інформаційної сфери дають істотне підґрунтя для поширення нових інформаційних загроз, які потребують негайного реагування. Бурхливе втілення інформаційних технологій сучасності супроводжується активним виникненням таких загроз, а також відповідного їм *інформаційного впливу*, під яким розуміється "… організоване цілеспрямоване втручання у свідомість (підсвідомість) чи фізичний стан цільової аудиторії та/або в процес функціонування технічних об'єктів інформаційної інфраструктури шляхом застосування інформаційних засобів і технологій" [1].

Розвиток інформаційних технологій у воєнній сфері призводить до посилення інформаційного протиборства, зокрема за рахунок тотальної інформатизації засобів збройної боротьби, яка дала змогу об'єднати пункти управління, засоби розвідки, озброєння, зв'язку, навігації в єдине інформаційно-мережеве середовище у рамках мережецентричної війни [2–4]. Водночас таке середовище стає більш вразливим від засобів інформаційного протиборства, зокрема проявів інформаційного впливу [5].

Концепція мережецентричних воєн виводить на новий рівень сферу ведення військового протиборства – *інформаційний простір*, під яким розуміється інформаційне середовище, у якому відбуваються інформаційні процеси та інформаційні відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації, інформаційних продуктів та інформаційних ресурсів [1]. У цьому просторі актуальне значення набуває новий вид озброєння – *інформаційна зброя*, одним з інструментів якої є інформаційно-технічний вплив (ІТВ) на інформаційні системи противника як складова інформаційного забезпечення сил оборони України [6, 7]. У таких умовах потребує більшої конкретизації сутність механізму реалізації інформаційно-технічного впливу на інформаційні системи противника.

Особливої актуальності це питання набуває у зв'язку з повномасштабною збройною агресією Російської Федерації проти України, коли інформаційна складова постала щонайважливішим елементом забезпечення ефективного спротиву.

Аналіз останніх публікацій. Стан інформаційного забезпечення у воєнній сфері неодноразово висвітлювався в наукових публікаціях. Цій темі присвячено низку робіт [6–15]. Так, у [9] стверджується, що "інформаційна зброя, як правило, не спрямована на досягнення втрат у живій силі супротивника. Вона не знищує фізично й не руйнує людські, матеріально-технічні та інші ресурси, а лише підриває основи дії механізмів організації управління". З таким твердженням можна лише частково погодитися. У воєнному плані виведення з ладу системи управління розглядатиметься як важлива умова завдання противнику поразки. Адже порушення алгоритмів управління будь-якої системи в сучасних умовах неминуче призведе до погіршення її стану. Крім того, важливим способом ведення боротьби з противником із застосуванням інформаційної зброї вважатиметься віддалене ураження економічного (енергетичного) потенціалу будь-якої держави шляхом виведення з ладу засобів автоматизації управлінських процесів [5].

У деяких працях головна увага приділяється, в основному, термінологічним визначенням. Зокрема, в [13] автори, формулюючи аспекти інформаційної війни, дають загальне визначення ІТВ як "впливу на інформаційну інфраструктуру об'єкта для забезпечення реалізації необхідних змін у її

роботі (зупинку роботи, несанкціонований виток інформації, програмування на певні помилки, зниження швидкості опрацювання інформації тощо)". Водночас роль, сутність, питання організації та оцінювання ІТВ на інформаційні системи противника в цих наукових працях не розкриваються.

З огляду на це, існує проблемне питання визначення механізму реалізації негативного ІТВ на інформаційні системи противника, що потребує більш детального наукового опрацювання.

Метою статті є обґрунтування системно-цільового підходу до визначення механізму реалізації ІТВ на інформаційні системи противника як складової інформаційного забезпечення сил оборони.

Виклад основного матеріалу. Сутність системно-цільового підходу до визначення механізму реалізації ІТВ на інформаційні системи противника полягає в застосуванні цілісної системи, що складається з відносно відокремлених взаємодіючих і взаємопов'язаних між собою елементів (підсистем), вивчення всієї сукупності параметрів і показників функціонування такої системи в динаміці з постійною орієнтацією діяльності на кінцеві результати, коли цілепокладання та цілереалізація ІТВ здійснюється покроково в кожному елементі з урахуванням специфіки їх функціонування.

Загалом, системно-цільовий підхід може бути реалізований у загальних межах теорії кібернетичного управління [14, 15], при якому будь-яку функцію в системі управління неможливо реалізувати без належного інформаційного забезпечення цього процесу. Інформаційний вплив здійснюється виключно за допомогою елементів інформаційної інфраструктури та наявних інформаційних ресурсів, під якими розуміються дані та знання, відмінною і невід'ємною характеристикою яких є їх прагматична цінність, що визначається практичними потребами в інтересах вирішення певних завдань [1].

Будь-який інформаційний простір формується за наявності необхідних інформаційних ресурсів із застосуванням відповідної інформаційної інфраструктури. *Інформаційна інфраструктура* – це сукупність інформаційних систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування.

Засоби, що здійснюють деструктивну дію в інформаційному просторі, об'єднані в новий клас зброї – інформаційну зброю. Нині до інформаційної зброї відносять широкий клас прийомів і способів інформаційного впливу на противника – від дезінформації і пропаганди до засобів радіоелектронної боротьби та дій у кіберпросторі. *Інформаційна зброя* – це сукупність способів, прийомів, засобів і технологій інформаційного впливу, призначених для нанесення збитку (ураження) елементам інформаційної інфраструктури протилежної сторони під час ведення інформаційної боротьби шляхом:

придушення елементів інформаційної інфраструктури державного та військового управління;

електромагнітного впливу на елементи інформаційних та телекомунікаційних систем;

доступу до інформаційних ресурсів з подальшою деформацією (спотворенням), знищенням або витоку інформації;

інформаційно-психологічного впливу на військовослужбовців та громадянське населення.

Інформаційній зброї притаманні такі *якісні характеристики* [5]:

універсальність (застосування не залежить від кліматичних та географічних умов, часу доби, сезонів року тощо);

прихованість – не потрібно проводити мобілізацію, створювати великі угруповання військ;

непомітність;

раптовість застосування;

економічна ефективність (розроблення інформаційної зброї та її застосування потребує істотно менших витрат у порівнянні з іншими видами зброї);

масштабність застосування (вирішення завдань не тільки тактичного, але й можливо стратегічного рівня);

наявність ефекту "ланцюгової реакції" (вплив інформаційної зброї на окремий елемент інформаційної системи, інформаційного ресурсу може призвести до виведення з ладу інших елементів системи, а можливо і системи в цілому);

складність здійснення контролю за створенням та випробуванням інформаційної зброї (факти розроблення і застосування можна надійно приховати від розвідки противника).

Відповідно до сфери свого застосування інформаційна зброя поділяється на

інформаційно-технічну зброю та інформаційно-психологічну зброю.

Інформаційно-психологічна зброя – вид інформаційної зброї як сукупність засобів, форм, способів і прийомів прихованого маніпулювання інформацією в інформаційному просторі протиборчої сторони для ураження індивідуальної і масової свідомості (підсвідомості), зокрема через друковані, електронні та аудіовізуальні засоби масової інформації [5].

Зосередимо увагу на розгляді інформаційно-технічної зброї, особливістю функціонування якої є її орієнтованість на поразку апаратно-програмних засобів систем передачі, зберігання та обробки інформації противника, що функціонують в інформаційному просторі електронних інформаційних ресурсів (кіберпросторі).

Інформаційно-технічна зброя – сукупність спеціально організованої інформації, інформаційних технологій, способів і засобів, які дають змогу цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск санкціонованих користувачів, порушувати функціонування систем обробки інформації, здійснювати дезінформацію, дезорганізацію роботи технічних засобів комп'ютерних систем та інформаційно-обчислювальних мереж, а також інших інфраструктур забезпечення функціонування систем управління.

Інформаційно-технічна зброя включає технічні та програмні засоби, що забезпечують несанкціонований доступ до баз даних, порушення штатного режиму функціонування апаратно-програмних засобів, а також виведення з ладу ключових елементів інформаційної інфраструктури. Застосування інформаційно-технічної зброї спрямоване на зрив виконання цільових завдань із застосуванням інформаційної системи. Приклади деяких видів інформаційно-технічної зброї, що ґрунтуються на різних технологіях, наведено у Табл. 1.

Таблиця 1

Види інформаційно-технічної зброї, що ґрунтуються на різних технологіях

Вид інформаційно-технічної зброї	Засоби, що використовуються	Тип технології
Засоби впливу на компоненти радіоелектронного обладнання та системи їх енергозабезпечення	Засоби силового радіоелектронного придушення; надпотужні генератори НВЧ-випромінювання (гіротрони, магнетрони та ін.); вибухомагнітні генератори (ВМГ), вибухові магнітогідродинамічні генератори (МГД-генератори); засоби силового впливу через електромережу; засоби виведення з ладу електромереж	На основі енергетичної дії
	Програмні засоби виведення з ладу обладнання (резонанс головок жорстких дисків, випалювання моніторів та ін.); програмні засоби стирання пам'яті, що перезаписується; програмні засоби впливу на системи безперебійного живлення	На основі інформаційних технологій
Засоби впливу на інформаційні ресурси та апаратно-програмні засоби АСУ	Засоби подолання систем захисту інформації; засоби проникнення в інформаційні системи противника; засоби маскування джерел отримання інформації; засоби виведення з ладу інформаційної системи; засоби прихованої часткової зміни алгоритму функціонування програмного забезпечення; засоби збору даних, що циркулюють в інформаційних системах противника; засоби доставки та впровадження певних алгоритмів у конкретне місце інформаційної системи; засоби впливу на системи охорони об'єктів	На основі інформаційних технологій
Засоби впливу на процес передачі інформації	Засоби радіоелектронної боротьби; станції перешкод радіозв'язку (у тому числі з елементами штучного інтелекту); передавачі перешкод одноразового використання, що закидаються	На основі енергетичного впливу
	Засоби впливу на протоколи передачі даних систем зв'язку та передачі даних; засоби впливу на алгоритми адресації та маршрутизації; засоби перехоплення та порушення проходження інформації в технічних каналах її передачі; засоби виклику перевантаження системи хибними запитами на встановлення зв'язку	На основі інформаційних технологій

Застосування інформаційно-технічної зброї реалізується шляхом ІТВ на відповідні об'єкти.

ІТВ на інформаційні системи противника – це цілеспрямоване втручання в процес функціонування технічних об'єктів

інформаційної інфраструктури противника з метою порушення їх роботи або виведення з ладу шляхом застосування засобів і технологій радіоелектронного впливу та кіберзброї [1]. Такий вплив – основний вражаючий фактор інформаційно-технічної зброї, що є дією або на інформаційний ресурс, або на інформаційну систему, або на засоби отримання, передачі, обробки, зберігання та відтворення інформації в її складі, з метою викликати певні деструктивні структурні та/або функціональні зміни [5].

ІТВ можуть бути поодинокі або групові. ІТВ також класифікують за характером вражаючих властивостей [5, 6]:

вибіркові впливи – на визначений певний ресурс в інформаційно-обчислювальній мережі;

комплексні впливи – на всю інформаційно-телекомунікаційну інфраструктуру.

За способом реалізації ІТВ можуть бути поділені на алгоритмічні; програмні; апаратні; фізичні: електромагнітні (радіоелектронні; оптико-електронні; оптичні; електричні); акустичні; гідроакустичні; радіаційні; хімічні; біологічні; на основі інших фізичних принципів [5].

ІТВ різних видів можуть застосовуватися спільно. Крім того, деякі види інформаційно-технічних впливів одночасно несуть у собі риси кількох видів.

До *алгоритмічного ІТВ* відноситься дія на алгоритми використання засобів (програмного, апаратного, фізичного) для здійснення несанкціонованого впливу на інформаційні ресурси. Прикладом алгоритмічного впливу є DoS-атака (Denial of Service – відмова в обслуговуванні). Сутність такого впливу полягає в тому, що на систему, що атакується, посилаються з високою інтенсивністю коректні запити на використання її інформаційних ресурсів. Це призводить до того, що можливості інформаційної системи обслуговування таких запитів швидко вичерпуються, і вона відмовляє в обслуговуванні всім своїм користувачам.

До *програмного ІТВ* належить дія на програмне забезпечення з метою несанкціонованого впливу на інформаційні системи противника, їх інформаційні ресурси. До такого ІТВ можна віднести засоби організації віддалених мережевих атак, комп'ютерні віруси, програмні закладки, нейтралізатори тестових програм та програм аналізу коду.

До *апаратного ІТВ* можуть бути віднесені дії на засоби, які вбудовані в інформаційну систему або несанкціоновано впроваджені до неї, а також на санкціоновані апаратні засоби, які дають змогу у процесі своєї роботи здійснювати несанкціонований вплив на інформаційні ресурси системи. До найпоширенішого типу апаратного інформаційно-технічного впливу належить дія на апаратні закладки.

До *фізичного ІТВ* можуть бути віднесені дії стосовно добування інформації шляхом доступу до інфраструктури інформаційного простору, аналізу фізичних полів, що генеруються об'єктами цієї інфраструктури, а також засоби радіоелектронного та вогневого ураження її фізичних елементів. Здійснювати фізичний інформаційно-технічний вплив можливо через: засоби технічної розвідки; засоби радіоелектронного придушення; засоби оптико-електронного придушення; засоби ураження електромагнітним випромінюванням (генератори електромагнітних імпульсів, генератори НВЧ-випромінювання, генератори лазерного випромінювання та ін.); засоби ураження силовими електромагнітними впливами (генератори електричного струму надвисокої напруги); засоби виведення з ладу елементної бази радіоелектронних систем. Інформаційно-технічний вплив на інформаційні системи противника може бути реалізований шляхом:

віддаленої мережевої атаки – це руйнівний або дестабілізуючий ІТВ, що здійснюється по каналах зв'язку віддаленим щодо атакованої системи суб'єктом і характерний для структурно- та просторово-розподілених інформаційних систем;

використання комп'ютерних "вірусів" – приховані програми, що застосовуються для деструктивної зміни програмного забезпечення комп'ютерів та комп'ютерних мереж;

поширення фальшивої (недостовірної) інформації в комп'ютерних мережах;

обмеження або заборони доступу до інформаційного ресурсу легальним користувачам комп'ютерних мереж;

радіоелектронного придушення радіотехнічних засобів (зв'язку, спостереження, навігації, радіо, телебачення тощо).

Деструктивний ІТВ має бути спрямований на такі об'єкти в інформаційній інфраструктурі противника, як: інформаційно-телекомунікаційні мережі (мережі та засоби зв'язку, електронні засоби масової інформації,

електронні архіви (сховища) та банки даних, засоби автоматизації систем управління військами (силами) та зброєю, радіоелектронні засоби і системи управління, навігації, спостереження тощо, а також на інформацію (інформаційний ресурс), що циркулює в таких об'єктах у реальному часі.

Проведений аналіз дає змогу орієнтовно визначити такі *основні напрями* ІТВ на процес функціонування інформаційних об'єктів противника:

порушення встановленого порядку інформаційного обміну, несанкціонований доступ (або обмеження будь-якого доступу) до інформаційних ресурсів противника, збір, отримання, використання та розповсюдження інформації (дезінформація, приховування або спотворення інформації);

порушення ефективності функціонування інформаційних засобів противника, цілеспрямоване розповсюдження комп'ютерних "вірусів" і спеціальних програм перехоплення інформації у комп'ютерних мережах, поширення недостовірної інформації, радіоелектронне ураження (придушення) тощо, спотворення (знищення) інформаційного ресурсу, зокрема програмного забезпечення;

спрямований (відкритий і прихований) негативний ІТВ в інформаційному просторі противника з метою масового розповсюдження по інформаційних каналах противника дезінформації для введення в оману та коригування намірів осіб, які приймають рішення;

створення перешкод для розроблення та впровадження інформаційних технологій противника.

Сутністю деструктивного ІТВ на інформаційні системи противника є: пошук, добування (одержання), збір, оброблення, накопичення, збереження і використання інформації, планування та здійснення вражаючого (придушуючого) впливу, аналіз наслідків цього впливу з можливістю його корекції.

Модель функціонування механізму реалізації ІТВ на інформаційні системи противника базується на кібернетичній схемі як послідовності часткових функцій загального процесу управління – таких, як збір інформації про інформаційну систему противника, аналіз зібраної інформації, виявлення вразливостей інформаційної системи противника, прийняття рішення щодо застосування ІТВ на противника з використанням цих вразливостей, здійснення ІТВ виконавчими силами і засобами інформаційної інфраструктури, оцінку результатів ІТВ та уточнення подальших завдань (рис.1).

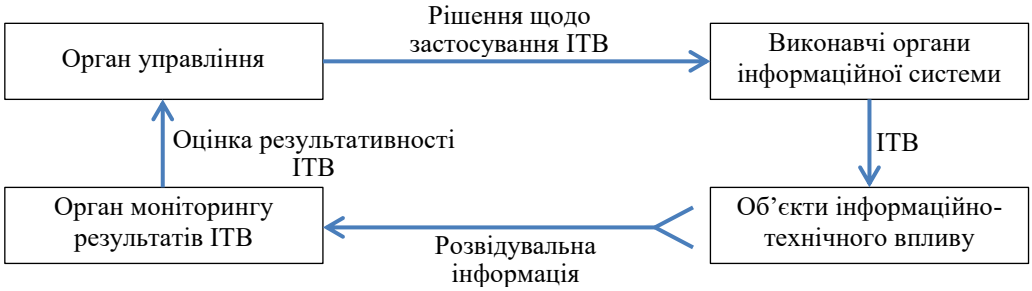

Рис. 1. Кібернетична модель механізму реалізації інформаційно-технічного впливу на інформаційні системи противника

Управляти механізмом реалізації ІТВ на інформаційні системи противника відповідно до теорії управління [14, 15] означає виконання декількох етапів.

1-й етап процесу управління механізмом ІТВ на інформаційні системи противника є найбільш складним утворенням логічної послідовності окремих часткових функцій, коли *орган управління* на підставі збору та аналізу розвідувальної інформації про об'єкти інформаційної системи противника, виявлення їх уразливостей приймає рішення щодо застосування ІТВ на конкретні об'єкти такої системи противника. З цією метою визначають:

наявність потенційних загроз з боку об'єктів інформаційної системи противника;

ступені важливості об'єктів інформаційної системи противника;

рівень вразливості об'єктів інформаційної системи противника;

визначення першочергових об'єктів інформаційної системи противника, порядку та послідовності здійснення на них впливу;

вибір засобів і способів реалізації ІТВ на визначені об'єкти інформаційної системи противника;

час початку та закінчення ІТВ на визначені об'єкти інформаційної системи противника;

заходи прикриття здійснення ІТВ на об'єкти інформаційної системи противника;

завдання виконавчому (им) органу (ам) щодо підготовки та здійснення ІТВ на визначені об'єкти інформаційної системи противника.

2-й етап процесу управління механізмом ІТВ на інформаційні системи противника здійснюється *виконавчим органом* та спрямований на реалізацію заходів ІТВ на конкретні об'єкти інформаційної системи противника. Відповідно до завдань, визначених органом управління, *виконавчий орган* готує та здійснює відповідний вид ІТВ на такі об'єкти інформаційної системи противника з використанням існуючої інформаційної інфраструктури, виходячи з можливостей засобів ІТВ, що є у наявності. При цьому:

усвідомлюються (за необхідністю – уточнюються) завдання, визначені органом управління щодо впливу на об'єкти інформаційної системи противника з урахуванням існуючої інформаційної інфраструктури;

проводиться оцінка можливостей власних сил та засобів ІТВ, а також противника відповідно до отриманих завдань;

здійснюється вибір способів реалізації ІТВ за характером вражаючих властивостей для виконання завдань з максимальною ефективністю;

здійснюється розподіл наявних засобів ІТВ по завданнях, визначених органом управління;

визначається порядок виконання завдань щодо ІТВ на об'єкти противника з урахуванням можливостей власних засобів інформаційної інфраструктури та противної сторони;

здійснюється постановка завдань безпосереднім виконавцям ІТВ.

3-й етап процесу управління (*контроль результатів ІТВ*) виконується *органом моніторингу*, який здійснює постійний контроль за результативністю впливу на визначені об'єкти інформаційної системи противника. Сутність виконання 3-го етапу полягає в оцінці результатів змін інформаційної активності об'єктів інформаційної системи противника та надання об'єктивної інформації про їх стан до органу управління.

4-й етап – *орган управління* на підставі даних, отриманих від органу моніторингу щодо результатів змін рівня функціонування об'єктів інформаційної системи противника, по яких було здійснено ІТВ, приймає *рішення про результати ІТВ* та робить висновок щодо необхідності подальшого впливу.

Запропонований 4-етапний механізм організації ІТВ на інформаційні системи противника дозволяє реалізувати адаптивну систему управління впливом. Зазначені етапи виконуються циклічно, оскільки залежно від ситуації можуть змінюватися загрози, з'являтися нові інформаційні ресурси або змінюватися порядок їх використання, а також можуть змінюватися технології та методи впливу на інформаційні системи. Такий підхід потребує постійного контролю та (за необхідності) удосконалення методів впливу на інформаційні системи противника.

На підставі зазначеного можна сформувати деякі рекомендації щодо визначення напрямів поліпшення інформаційного забезпечення сил оборони, зокрема його складової – ІТВ на інформаційні системи противника, пов'язаного з удосконаленням методів та способів:

добування необхідних даних щодо інформаційних систем противника з використанням усіх можливих джерел;

отримання розвідувальної інформації шляхом перехоплення та розшифровування інформаційних потоків, що передаються каналами зв'язку противника, а також за рахунок побічних випромінювань;

здійснення доступу до інформаційних ресурсів противника з подальшим добуванням інформації та її перекручуванням;

формування та масове поширення по інформаційних каналах противника або глобальних мережах дезінформації для впливу на оцінки, наміри осіб ворога, які приймають рішення;

ведення радіоелектронної боротьби (радіоелектронного ураження або придушення радіоелектронних засобів противника);

вогневого ураження (у воєнний час) елементів інформаційної інфраструктури державного та військового управління противника.

Таким чином, для вирішення завдання адекватної протидії у гібридній агресії проти Україні із застосуванням системно-цільового підходу передбачає створення та впровадження системи забезпечення інформаційної безпеки сил оборони, зокрема її складової – підсистеми ІТВ як складової інформаційного забезпечення сил оборони України, яка діє превентивно для рішучого нівелювання переваги технологічно більш розвиненого противника. Водночас, для

комплексного вирішення проблем захисту національного інформаційного простору потрібні спільні зусилля як з боку органів влади, усіх складових сектору безпеки і оборони, так і громадських організацій, бізнесових структур.

Висновки

1. У світовому інформаційному просторі перманентно зростає рівень інформаційного протиборства як один з головних напрямів реалізації інформаційної політики сучасних міжнародних відносин. Збільшується кількість та складність інформаційних загроз. Унаслідок бурхливого втілення інформаційних технологій набирає актуальності інформаційна зброя, одним з інструментів якої є ІТВ на інформаційні системи противника як складова інформаційного забезпечення сил оборони України.

2. Системно-цільовий підхід до визначення механізму реалізації ІТВ на інформаційні системи противника передбачає виконання послідовності етапів: аналіз потенційних загроз на підставі збору розвідувальної інформації про об'єкти інформаційної системи противника; прийняття рішення щодо застосування ІТВ; підготовку та здійснення ІТВ на призначені об'єкти інформаційної системи противника; контроль за результативністю впливу на визначені об'єкти противника, по яких було здійснено ІТВ; прийняття рішення про результати ІТВ та висновок щодо подальших управлінських дій.

3. Роль ІТВ на інформаційні системи (об'єкти) противника як складової інформаційного забезпечення сил оборони України полягає в організації та проведенні комплексу акцій та атак, якими реалізується деструктивне електронне втручання в інформаційні ресурси противника та процес функціонування об'єктів його інформаційної інфраструктури з метою виведення їх з ладу або порушення сталого режиму функціонування.

Перспектива подальших досліджень. Метою подальшого дослідження є визначення комплексу заходів ІТВ на інформаційні об'єкти противника як складової інформаційного забезпечення сил оборони України, що повинні бути органічно пов'язані із заходами безпеки власної інформації (інформаційно-технічним захистом). Зазначені завдання можуть бути вирішені із застосуванням системно-цільового підходу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ВСТ 01.004.004–2014(01). Інформаційна безпека держави у воєнній сфері. Терміни та визначення. [Чинний від 2014-02-27] . Київ, 2014. (Військовий стандарт).

2. Ільяшов О. А. Тенденції розвитку збройної боротьби у війнах четвертого – шостого поколінь // Наука і оборона. 2009. № 3. С.43–48.

3. Макаренко С. И., Иванов М. С. Сетецентрическая война – принципы, технологии, примеры и перспективы. Санкт-Петербург : Наукоемкие технологии, 2018. 898 с.

4. Воєнна доктрина США "Joint Vision 2020". URL: http:// Joint Vision 2020.pdf (дата звернення: 07.08.2023).

5. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. № 3. 2016. URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата звернення: 08.08.2023).

6. Саричев Ю. О. Аналіз підходів щодо визначення сучасної ролі та місця інформаційного забезпечення в системі державного управління // Вісник НАДУ при Президентові України. 2016. Вип. 3 (82). С.138–143.

7. Сніцаренко П. М., Саричев Ю. О., Ткаченко В. А. Комплексна система протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України // Наука і оборона. 2018. № 2. С. 40–45.

8. Саричев Ю. О. Теоретичний підхід до інформаційного забезпечення в системі державного управління у воєнній сфері // Вісник НАДУ при Президентові України. Серія "Державне управління" 2016. Вип. 4 (83). С. 153–160.

9. Горбулін В. П., Качинський А. Б. Засади національної безпеки України : підручник. Київ : Інтертехнологія, 2009. 272 с.

10. Смалько О. А. Захист інформаційних ресурсів : монографія. Кам'янець-Подільський : ПП Буйницький, 2011. 704 с.

11. Сніцаренко П. М. Організаційні основи державної системи забезпечення інформаційної безпеки України у воєнній сфері // Інформаційна безпека людини, суспільства, держави. 2012. № 2 (9). С. 46–52.

12. Теоретичні основи управління угрупованням військ (сил) у сучасних умовах збройної боротьби : монографія / О. М. Загорка, А. К. Павліковський, А. А. Корецький, С. О. Кириченко, І. О. Загорка ; за заг. ред. І. С. Руснака. Київ : НУОУ, 2020. 248 с.

13. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. 2008. № 4. С.136–140. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/ostroukhov_do_problemy.pdf (дата звернення: 09.08.2023).

14. Винер Н. Кибернетика или управление и связь в животном и машине. Москва : Сов. Радио, 1968. 328 с.

15. Глушков В. М. Кибернетика. Вопросы теории и практики. Москва : Наука, 1986. 488 с.

Стаття надійшла до редакційної колегії 08.09.2023

Mechanism of influence on enemy information systems as a component of information support for the Ukrainian defense forces

Annotation

The development of information technologies in the military sphere leads to the intensification of information confrontation, in particular due to the total informatization of armed struggle, which has made it possible to combine control points, intelligence, weapons, communications, navigation into a single information and network environment within the framework of network-centric warfare. The concept of network-centered warfare brings to a new level the sphere of military confrontation - the information space, which means the information environment in which information processes take place. In this space, a new type of weapon – information weapons – is gaining importance, one of the tools of which is information and technical influence (ITI) on enemy information systems as a component of information support for the Ukrainian defense forces. In such circumstances, the essence of the mechanism of realization of information and technical influence on the enemy's information systems needs to be more specified. This issue is especially relevant in connection with the full-scale armed aggression of the Russian Federation against Ukraine, when the information component has become a crucial element of ensuring effective resistance.

The model of functioning of the mechanism of implementation of ITI on enemy information systems is based on a cybernetic scheme as a sequence of partial functions of the general management process. A 4-stage mechanism for organizing ITE on adversary information systems is proposed, which allows to implement an adaptive impact management system. The stages are carried out cyclically, since, depending on the situation, threats may change, new information resources may appear or the order of their use may change, and technologies and methods of influence on information systems may change. Such an approach requires constant monitoring and (if necessary) improvement of methods of influencing the enemy's information systems.

Keywords: information support; information weapons; information and technical influence.