

УДК 004.89

DOI: 10.15587/2313-8416.2015.37460

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕОРІЇ НЕСИЛОВОГО ВПЛИВУ В ВІЙСЬКОВІЙ КОНТРРОЗВІДЦІ

©М. Б. Кубявка, Л. Б. Кубявка, Ю. М. Тесля

Стаття присвячена аналізу можливого застосування теорії несилової взаємодії в військовій контррозвідці. Метою такого застосування є забезпечення національної безпеки, яке спрямоване на адекватну протидію реальним та потенційним загрозам, що виникають або можуть виникнути внаслідок розвідувально-підривної діяльності спеціальних органів іноземних держав (розвідки, контррозвідки), недержавних розвідувальних і контррозвідувальних структур, організацій та окремих осіб

Ключові слова: спеціальні інформаційні операції, військова контррозвідка, теорія несилової взаємодії

The paper analyzes the possible application of the theory of non-coercive interaction in the military counterintelligence. The purpose of this application is to ensure national security, which is aimed at countering adequate real and potential threats that arise or may arise as a result of intelligence and subversive activities of foreign special powers (intelligence, counterintelligence), non-intelligence and counter-intelligence agencies, organizations and individuals

Keywords: special information operations, military counterintelligence; theory of non-coercive interaction

1. Вступ

В зв'язку з переходом людства від індустріальної до інформаційної цивілізації, інформація стала однією з головних складових історичного прогресу. Вона має ключове значення для успішного функціонування всіх суспільних і державних інститутів, адекватного поведіння кожної окремої людини. Інформація необхідна кожній людині як умова, так і засіб її існування у суспільстві. Але які тенденції використання інформації в сучасному світі?

2. Постановка проблеми

На сучасному етапі розвитку суспільства швидко зростає значення непрямих (м'яких) методів впливу на перебіг політичних та економічних процесів в державах. Провідне місце серед м'яких методів впливу звісно посідають інструменти несилової (інформаційної) дії. І в цьому основна тенденція розвитку суспільства – перехід від фізичних способів ведення військових дій (знищення або примус), до несилової зміни відношення людей до ворогуючої сторони – від ненависті до прийняття. Подібна тенденція спостерігається в усьому світі [1]. Але на сьогодні не існує достатньо обґрунтованої теоретичної бази проведення несилових (інформаційних) впливів на протидіючу (антагоністичну) сторону.

3. Літературний огляд

Впливам на масову та індивідуальну свідомість присвячена значна кількість наукових

праць [1–7]. Приділяється значна увага створенню власних систем впливу на супротивника та захисту союзників, власного народу і армії від дії спеціальних інформаційних операцій інших держав.

Актуальність безпеки нашої держави саме у цій, інформаційній сфері, підтверджує прийняття Верховною Радою України Закону України “Про основи національної безпеки України” (ВВР, 2003 № 39, ст. 351), який визначає протидію інформаційній експансії іноземних держав, однією з форм якої і є спеціальні інформаційні операції як один з напрямів політики національної безпеки. Ця проблема – одна з ключових у контексті гарантування інформаційної безпеки держави. [2]

Однією з структур України, яка займається забезпеченням національної безпеки є Контррозвідка Служби безпеки України - система підрозділів Служби безпеки України, що протидіють діяльності іноземних спецслужб, а також їхнім легальній і технічній розвідкам. Діяльність контррозвідки здійснюється відповідно до законів «Про оперативно-розшукову діяльність» і «Про Службу безпеки України» Військова контррозвідка, складова частина СБУ, являє собою систему органів, що здійснюють оперативну розшукову діяльність у Збройних Силах, Національній гвардії, Прикордонних військах та військах МВС України [3].

4. Аналіз можливого застосування теорії несилової взаємодії в військовій контррозвідці

З давніх часів було відомо, що справжньою перемогою є лише така, що не містить у собі зерен

реваншу. Після неї немає зруйнувань, а супротивник не відчуває себе переможеним. «Найкраще з найкращого – перемогти супротивника без боротьби» [4].

Запорукою такої перемоги є успіх у боротьбі за свідомість людей (супротивників, союзників та власного народу і армії), їх інформування чи дезінформування. Саме цю мету передбачають дії, що отримали останніми кількома роками назву спеціальних інформаційних операцій, які по своїй суті використовують поняття теорії несилового впливу на думки та дії людей.

“Інформаційні операції - попередньо сплановані психологічні дії в мирний і воєнний час, спрямовані на ворожу, дружню або нейтральну аудиторію засобами впливу на настанови та поведінку з метою досягнення політичних або воєнних переваг. Вони поєднують психологічні дії зі стратегічними цілями, психологічні консолідуючі дії та психологічні дії з безпосередньої підтримки бойових дій” [5].

Основними структурами, які розроблюють, перевіряють та впроваджують в дію такі спеціальні операції є розвідувальні управління, військові контррозвідки та інші спецслужбами іноземних держав.

На військовому рівні інформаційні операції являють собою комплекс заходів, які проводяться у масштабах збройних сил, їх видів, і є складовою частиною воєнної кампанії. Вони спрямовані на досягнення інформаційної переваги над противником (у першу чергу – в управлінні військами) та на захист своїх систем управління.

Захистом від загроз національної безпеки, що виникають або можуть виникнути внаслідок розвідувально-підривної діяльності спеціальних органів іноземних держав (розвідки, контррозвідки), недержавних розвідувальних і контррозвідувальних структур, організацій та окремих осіб і займається таке формування Служби безпеки України як військова контррозвідка.

Для чого ж потрібна військова контррозвідка і як її застосувати теорію несилового взаємодії для захисту національної безпеки нашої держави?

На теперішній час перед військовою контррозвідкою стоять такі завдання:

– контррозвідувальна діяльність, під якою розуміється діяльність органів безпеки у військах в межах своїх повноважень, спрямована на вирішення завдань щодо виявлення, попередження, припинення розвідувальної та іншої діяльності спеціальних служб і організацій іноземних держав, а також окремих осіб, що переслідує мету нанесення шкоди безпеці країни, інших військ і військових формувань, а також їх органів управління;

– боротьба зі злочинністю і терористичною діяльністю, яка передбачає для органів безпеки у військах рішення завдань: виявлення, попередження і припинення злочинів, віднесених до підслідності органів служби безпеки; виявлення, попередження і припинення терористичної і диверсійної діяльності, спрямованої проти Збройних Сил України, інших військ і військових формувань, а також їх органів управління; організації та здійснення спільно з

іншими державними органами боротьби з організованою злочинністю, корупцією, контрабандою, незаконним обігом зброї, боєприпасів, вибухових і отруйних речовин, наркотичних засобів і психотропних речовин, спеціальних технічних засобів, призначених для негласного отримання інформації, а також боротьбі з незаконними збройними формуваннями, злочинними групами, окремими особами та громадськими об'єднаннями, які ставлять своєю метою організацію озброєного замаху, насильницьку зміну конституційного ладу України, насильницьке захоплення або насильницьке утримання влади. Боротьбу зі злочинністю і терористичною діяльністю органи безпеки у військах здійснюють шляхом проведення в межах своєї компетенції оперативно-розшукових заходів, дізнання та попереднього слідства.

– адміністративно-правова діяльність, яка спрямована на вирішення завдань щодо забезпечення належного адміністративно-правового режиму, а саме: виявлення, попередження й припинення адміністративних правопорушень, порушення та (або) розгляд справ по яких віднесено до відання органів служби безпеки; запобігання в межах своїх повноважень несанкціонованих дій з ядерною, хімічною, біологічною чи іншою зброєю великої вражаючої здатності, застосування якого викликає масові втрати і (або) руйнування (зброї масового ураження); участь у розробці і здійсненні заходів щодо захисту державної таємниці, а також здійснення контролю за забезпеченням схоронності відомостей, складових державну таємницю, у Збройних Силах, інших військах і військових формуваннях, а також в їх органах управління; здійснення заходів, пов'язаних з допуском військовослужбовців та осіб цивільного персоналу до державної таємниці; участь у вирішенні питань, що стосуються їх виїзду за межі України; участь у вирішенні питань режиму перебування іноземних громадян та осіб без громадянства на території України, відвідування ними військових об'єктів;

– інформаційна діяльність органів безпеки у військах, яка передбачає вирішення наступних завдань: здійснення аналізу інформації про реальних і потенційних загроз безпеки Збройних Сил, прогнозування тенденцій їх розвитку; отримання інформації й обмін інформацією на основі міжнародних договорів з правоохоронними органами, контррозвідувальними і розвідувальними службами іноземних держав; інформування органів військового управління та посадових осіб про виявлену діяльність спеціальних служб і організацій іноземних держав; про виявленні, попередженні і припиненні інший протиправної діяльності, а також порушень встановлених вимог до забезпечення різних видів безпеки у Збройних Силах, інших військах, військових формуваннях і органах; участь в інформуванні військово-політичного керівництва країни, органів державної влади України, органів військового управління та посадових осіб про загрози безпеки Україні, її Збройних Сил, інших військ, військових формувань і їх органів управління, про

передумови до виникнення надзвичайних ситуацій, а також у наданні інших відомостей, необхідних для забезпечення оборони і безпеки держави [8, 9].

Але на жаль серед цих заходів відсутні ті, які були б чітко направлені проти інформаційного впливу ворога як на війська, так і на населення. Адже останніми роками неабиякої популярності набули дослідження проблем створення та застосування інформаційної зброї, а також захисту від неї. Поряд із значним інтересом до проблем захисту інформації, хакерської війни, інших специфічних питань застосування новітніх інформаційних, зокрема комп'ютерних технологій з метою завдання шкоди супротивникові, спостерігається підвищення уваги до теорії спеціальних психологічних операцій та теорії несилового впливу. Успіхи соціально-психологічних технологій, що почали з середини 60-х років активно проникати в теорію та практику публік релейшнз, пропаганди, комунікативістики, викликали появу нових, надзвичайно ефективних і цікавих підходів до проблем здійснення інформаційного впливу. Це мало наслідком те, що спеціальні інформаційні операції зараз визнаються багатьма дослідниками як невід'ємний, навіть ключовий елемент доктрини інформаційних воєн.

Цікаві думки щодо місця спеціальних інформаційних операцій у загальному контексті інформаційних воєн репрезентує Л. С.Джонсон [6]. Згідно з його твердженнями, суттю будь-якої інформаційної війни є реалізація впливу на інформаційний масив. Інформаційний масив можна розглядати як певну сукупність повідомлень. Ще з часів К.Шеннона (середина ХХ ст.) відомо, що впливи можуть бути двох основних типів:

– вплив безпосередньо на повідомлення, на їхню форму, механізми передачі, збереження, обробку тощо;

– вплив на зміст повідомлень.

Сьогодні можна говорити про один вплив, який змінює і повідомлення, і його зміст. Це несильовий (інформаційний) вплив на джерело повідомлення з метою вироблення у нього реакції, що відповідає нашим цілям. Саме такий вплив може бути розроблений з застосуванням теорії несилової взаємодії. В чому його суть.

Інформаційно-психологічний вплив являє собою цілеспрямовану психологічну атаку на конкретні сфери психіки людини, групи осіб або суспільну свідомість у цілому. Вплив може здійснюватися засобами інформаційних подразників з використанням усього спектру методів і форм технічного, візуального, звукового, медикаментозного, фізичного, больового, віртуального придушення волі.

Якщо звзвити питання до контррозвідки, то їх діяльність може бути на:

1. Вплив на повідомлення, що призводить до його викривлення, неможливості використання та ін.

2. Вплив на зміст повідомлення. Заміна одного повідомлення іншим.

3. Вплив на джерело повідомлення. Як слідує з теорії несилової взаємодії несильовий вплив призводить до змін у внутрішньому стані контрагенту взаємодії, що призводить до змін в його поведінці. Тому для отримання потрібного для контррозвідки результату необхідно:

– дати джерелу повідомлення таку інформацію, щоб його повідомлення відповідало інтересам контррозвідки. Наприклад – перебільшення військової міцності своєї країни;

– вплинути несильовим чином на джерело повідомлення так, щоб його відношення до предмету розвідки змінилось. І його повідомлення відповідало б інтересам контррозвідки.

5. Апробація результатів досліджень

Автори пропонують в якості науково-методичного базису дій контррозвідки в сфері інформаційного впливу на противника використати теорію несилової взаємодії [7]. Теорія дає математичний інструментарій для визначення найбільш ефективних способів інформаційного впливу в період підготовки чи проведення військових дій, а також в постійній роботі спецслужб України. Для створення такого базису пропонується:

1. Представити в поняттях теорії несилової взаємодії атрибути «м'якої сили». Основним таким поняттям є поняття інтроформації. Під **інтроформацією** розуміється внутрішня організація взаємодіючих суб'єктів, яка формує їх відношення до дійсності і проявляється у їх діях. Щоб досягти необхідних дій необхідно спочатку змінити відношення контрагенту до дійсності. А це досягається зміною інтроформації. В свою чергу для зміни інтроформації необхідно щоб на контрагента здійснювались інформаційні впливи. Дружніх контрагентів (з таким же або близьким відношенням до дійсності), направлені на потрібні зміни. Не дружніх, направлені на протилежні зміни.

2. Розробити математичну модель інформаційного впливу контррозвідки на противника, в основі якої буде розрахунок необхідної величини несильової дії на агентів розвідки.

3. Реалізувати методи несильової дії на суб'єктів впливу.

Розглянемо математичну модель такого впливу на розвідку противника рис. 1.

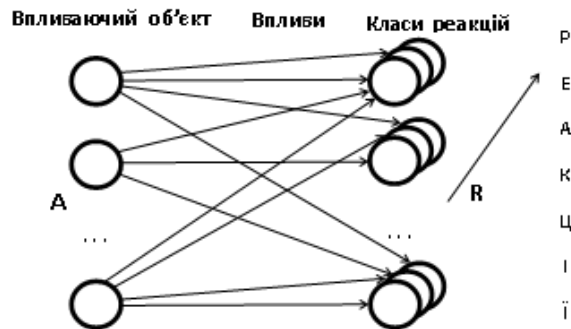


Рис. 1. Схема несильового впливу на противника з метою вироблення у нього необхідної реакції (поведінки)

Модель розрахунку необхідної реакції суб'єктів впливу (агентів противника) містить етапи [7]:

1. Розрахунок визначеності реакцій суб'єктів впливу. В такій моделі розглядаються дві групи об'єктів – ті що впливають шляхом «інформування» противника (власна контррозвідка), і ті, на які впливають (розвідка противника), і у яких формується необхідна реакція. Із (5.12) і (5.10) монографії [7]:

$$d(R_i) = \pm 0,5 \sqrt{\frac{p(R_i)}{1-p(R_i)} + \frac{1-p(R_i)}{p(R_i)} - 2};$$

$$i(R_i) = \sqrt{d^2(R_i) + 1};$$

$$d(R_i / A_j) = \pm 0,5 \sqrt{\frac{p(R_i / A_j)}{1-p(R_i / A_j)} + \frac{1-p(R_i / A_j)}{p(R_i / A_j)} - 2};$$

$$i(R_i / A_j) = \sqrt{d^2(R_i / A_j) + 1},$$

де $p(R_i)$ – безумовна ймовірність реакції (поведінки) R_i у противника; $d(R_i)$ – визначеність противника відносно реакції R_i ; $i(R_i)$ – інформованість противника відносно реакції R_i ; $p(R_i / A_j)$ – умовна ймовірність вибору реакції R_i при існуванні впливу A_j ; $d(R_i / A_j)$ – визначеність суб'єкта впливу відносно реакції R_i , після впливу A_j ; $i(R_i / A_j)$ – інформованість суб'єкта впливу відносно реакції R_i , після впливу A_j .

2. Використовуючи вираз (5.21) із [7] вираховуємо додаткову визначеність, яку додатково вносять об'єкти, що впливають на суб'єкт впливу:

$$\Delta d(R_i / A_j) = d(R_i / A_j) \times i(R_i) - d(R_i) \times i(R_i / A_j),$$

де $\Delta d(R_i / A_j)$ – зміни визначеності реакції R_i противника при впливі A_j .

3. Із (5.27) [7] розраховуються сумарний вплив на поведінку противника:

$$\Delta d_{\Sigma}(R_i) = \sum_j \Delta d(R_i / A_j),$$

де $\Delta d_{\Sigma}(R_i)$ – зміна визначеності реакції R_i у противника.

Із (5.10) [7]:

$$\Delta i_{\Sigma}(R_i) = \sqrt{\Delta d_{\Sigma}^2(R_i) + 1},$$

де $\Delta i_{\Sigma}(R_i)$ – зміни інформованості противника відносно реакції R_i .

4. Розраховується нова визначеність поведінки противника (5.22):

$$\overline{d(R_i)} = \Delta d_{\Sigma}(R_i) \times i(R_i) + d(R_i) \times \Delta i_{\Sigma}(R_i),$$

де $\overline{d(R_i)}$ – нова визначеність відношення противника до реакції R_i .

Розраховуючи результати різноманітних впливів з використанням наведеної моделі можна визначити стратегію поведінки власної контррозвідки з тим, щоб застосувати такий набір несилових дій, який забезпечить потрібну реакцію противника (відведення військ, перекидання їх на другорядні напрямки, відміна наступу і т. п.).

Щоб визначити необхідну величину інформаційної дії на агентів розвідки з використанням наведеної моделі потрібно вирішити такі основні задачі: виділити можливі впливи та шляхи їх реалізації; експертно оцінити результати цих впливів; підібрати таку комбінацію впливів, яка забезпечить необхідну реакцію противника; реалізувати підібрані впливи.

6. Висновки

Як показано в статті існує нагальна необхідність розвитку наукових досліджень спеціальних інформаційних операцій. А в Україні є всі передумови для формування потужної наукової школи у цій галузі. Так вітчизняними вченими розроблена теорія несилової взаємодії, яку рекомендовано використати в якості науково-методичної бази для підготовки та проведення дій, направлених на перемогу над противником.

На основі апарату теорії несилової взаємодії запропонована математична модель впливу на розвідку противника з метою формування необхідних для контррозвідки повідомлень.

В подальшому буде розроблено метод розрахунку впливу на суб'єктів розвідки, застосування якого дозволить чітко планувати способи проведення контроперацій, відносно діяльності противника.

Література

1. Nye, J. S. Jr. America's Information edge [Text] / J. S. Jr. Nye, W. A. Owens; R. M. Lloyd, course director; H. C. Bartlett et. al.; 2nd edition. – Strategy and force planning Faculty, National Security Decision Making Department, Naval War College, 1996. – P. 630–648.
2. Закон України Про основи національної безпеки України. [Текст] / Відомості Верховної Ради України (ВВР). – 2003. – № 39. – ст. 351.
3. Контррозвідка Служби безпеки України [Електронний ресурс] / Режим доступу: <http://schoolib.com.ua/pravoznavstvo/1/554.html> — Загол. з екрана.
4. Сунь, Цзы О Войне [Текст] / Цзы Сунь, Н. И. Конрад. – Синология. – М. : Ладомир, 1995. – 28 с.
5. FM 33-1, Оборони і безпеки розвідки та аналізу: IHS Jane [Електронний ресурс] / Режим доступу: <http://www.janes.com>
6. Джонсон, Л. С. Основний інтелектуальний виклик. До функціональної моделі інформаційної війни. Вплив

інформаційних технологій [Електронний ресурс] / Л. С. Джонсон. – Режим доступу: <http://www.janes.com/FM 33-1>
7. Тесля, Ю. Н. Введение в информатику Природы [Текст] / Ю. Н. Тесля. – К. : Маклауг, 2010. – 255 с.
8. Закон України Про контррозвідувальну діяльність [Текст] / Відомості Верховної Ради України (ВВР). – 2003. – № 12. – ст. 89.
9. Закон України про службу безпеки України. [Текст] / Відомості верховної ради України (ВВР). – 1992. – № 27. – ст. 382.

References

1. Nye, J. S. Jr, Owens, W. A. America's; Lloyd, R. M. (coursedirector); Bartlett, H. C. et. al. (1996). Informationedge. Second edition. Strate gyandforce planning Faculty, National Security Decision Making Department, Naval War College, 630–648.
2. The Law of Ukraine on basics of national security of Ukraine (2003), [Zakon Ukrainy pro osnovy natsionalnoi

bezpeky Ukrainy], Vedomosti Verkhovnoi rady Ukrainy, 39, st. 351.
3. Counterintelligence Security Service of Ukraine. Available at: <http://schoollib.com.ua/pravoznavstvo/1/554.html>
4. Sun, Tszyi (1995). About War. [O Voyne], Sinology, Moscow, Ladomir, 28.
5. FM 33-1, Defense and Security Intelligence and Analysis: IHS Jane's, Available at: <http://www.janes.com/>
6. Johnson, L. S. A Major Intelligence Challenge. Toward a Functional Model of Information Warfare. Impact of Information Technology. Available at: <http://www.janes.com/FM 33-1>.
7. Teslya, Y. U. (2010). Introduction to computer science-Nature. Mclaut, 255.
8. Law of Ukraine On counterintelligence activities (2003). Supreme Council of Ukraine (SC), 12, 89.
9. Law of Ukraine Security Service of Ukraine (1992). Supreme Council of Ukraine (SC) , 27, st. 382.

Дата надходження рукопису 27.01.2015

Тесля Юрій Миколайович, доктор технічних наук, професор, факультет інформаційних технологій, Київський національний університет ім. Тараса Шевченка, вул. Ломоносова, 81, м. Київ, Україна, 03680
E-mail: teslyas@ukr.net

Кубявка Микола Богданович, ад'юнкт, капітан, Військовий інститут, Київський національний університет ім. Тараса Шевченка, вул. Ломоносова, 81, м. Київ, Україна, 03680
E-mail: nick.kub@meta.ua

Кубявка Любов Богданович, аспірант, факультет інформаційних технологій, Київський національний університет ім. Тараса Шевченка, вул. Ломоносова, 81, м. Київ, Україна, 03680
E-mail: lyubov.kubyavka@mail.ru