В. Б. Толубко, Л. Н. Беркман, Л. А. Комарова, И. Э. Похабова

МЕТОД ОБЕСПЕЧЕНИЯ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ В КРИТИЧНОМ РЕЖИМЕ

Рассмотрен метод синтеза сигнала, оптимального по критерию минимума помехового влияния на входе демодулятора, и приведен пример практического применения этого метода в случае, когда система управления сетью функционирует в чрезвычайной ситуации.

Ключевые слова: система управления; достоверность передачи информации; метод синтеза сигнала по критерию минимума помехового влияния; критичный режим; инвариантность.

V. B. Tolubko, L. N. Berkman, L. O. Komarova, I. E. Pokhabova

THE METHOD GARANTEEING VALIDITY OF CONTROL SYSTEM INFORMATION TRANSMISSION IN EMERGENCY OPERATION

The method permitting synthesize the optimal sygnal reducing to a minimum disturbances effect on demodulator input is considered as well as example illustrating this method.

Keywords: control system; validity of information transmission; sygnal synthes method meeting the demands for minimum disturbunces effect; emergency operation; invariance.

УДК 351.746.1

В. БОГДАНОВИЧ, д-р техн. наук, професор; **Д. МІЩЕНКО,** аспірант;
А. ТУПАЛО; Т. ХРОПКО, Державний університет телекомунікацій, Київ

Методологічні аспекти організації управління інформаційно-психологічною безпекою населення в умовах низького рівня соціально-політичної стабільності в країні

Розглянуто методологічні підходи до організації управління інформаційно-психологічною безпекою населення в умовах низького рівня соціально-політичної стабільності в державі. Обґрунтовано мету, завдання, а також цілі такого управління. Розглянуто методичний підхід до формування системи показників оцінювання ефективності протидії деструктивним інформаційно-психологічним впливам і запропоновано методику управління інформаційно-психологічною безпекою політичного керівництва та населення. Наведено цільову функцію та узагальнений алгоритм управління. Сформульовано умови забезпечення достатнього рівня інформаційно-психологічної безпеки.

Ключові слова: спеціальна інформаційна операція; деструктивний інформаційно-психологічний вплив; психологічна безпека; загрози психологічного характеру; управління інформаційно-психологічною безпекою; ефективність протидії.

Постановка проблеми

Статтю присвячено проблемі захисту найширших верств населення від деструктивних інформаційних впливів за умов сучасного інформаційного протиборства. Актуальність проблеми зумовлено недостатньою розробленістю науково-методологічного апарату організації ефективної протидії деструктивним інформаційно-психологічним впливам з боку недружніх держав, що утруднює розвиток та забезпечення соціально-політичної стабільності в державі.

Аналіз останніх досліджень і публікацій

У монографії [1] досліджено природу маніпуляції свідомістю як окремих особистостей, так і великих груп людей, але проблема управління інформаційно-психологічною безпекою не стала предметом докладного розгляду. У монографії [2] наведено фактори, які визначають ефективність психологічної операції, спрямованої на невеликі групи людей. Серед відповідних показників виокремлено прямі і непрямі. Але по цих показниках неможливо коректно оцінити ефективність тієї чи іншої спеціальної інформаційної операції (СІО), що проводиться проти населення країни.

У публікаціях [3–7] подано загальну характеристику інформаційно-психологічних операцій, але питання оцінювання їх ефективності там не розглянуто. Через це немає змоги виявити найбільш суттєві характеристики інформаційних операцій, обґрунтувати критерії оцінювання їх ефективності і, відповідно, сформулювати стратегічні вимоги до системи протидії таким операціям, аби зрештою організувати управління інформаційно-психологічною безпекою великих груп людей.

У статті [8] запропоновано граф-модель процесу організації протидії спеціальним інформаційним операціям, але питання реалізації управління інформаційно-психологічною безпекою не розглянуто.

Нерозв'язана досі проблема

У зазначених публікаціях та інших наукових працях, з якими змогли ознайомитися автори, питання системного підходу до організації управління інформаційно-психологічною безпекою не досліджено.

Мета цієї статті — розробити такі методологічні підходи до організації управління інформаційно-психологічною безпекою населення за умов низького рівня соціально-політичної стабільності в країні, які дозволили б виокремити зазначене управління в самостійний інформаційно-аналітичний процес безпекового супроводу реалізації національних інтересів України.

Виклад основного матеріалу

Технічний прогрес, удосконаливши засоби комунікації, зробив сучасний світ не лише більш взаємозв'язаним, а й більш керованим. Процеси глобалізації активно впливають на формування моделі світоустрою, яку психіка і свідомість людини мають сприйняти сьогодні. Можна погодитися з думкою Ф. Бекон, який помітив, що суспільство (соціум) називає правильним не те, що справді істинне, а те, що панує в думці більшості. Через багатогранність інформаційної сфери інформаційно-психологічні засоби дії стають не лише малопомітними, гуманними, а й у ряді випадків надзвичайно небезпечними.

Протиборство між країнами, що розгорталося передусім в інформаційній сфері, особливо загострилося вже в середині XX сторіччя. Інформаційне протиборство, інформаційно-психологічна війна, незважаючи на позірну безневинність і безпечність, довели свою високу результативність у досягненні переваги однієї протиборчої сторони над іншою. Тому духовний, інтелектуальний та інформаційний потенціал перетворився на фундаментальний чинник національної безпеки [9; 11].

Справді, країни, що перебувають на найвищому рівні розвитку інформаційних технологій, мають значну перевагу над іншими країнами. Увесь хід розвитку світової історії підтверджує це дуже переконливо. Мета країни в будь-якій війні, що завжди являє собою продовження певної політики кожної з протиборчих сторін,— змусити супротивника, конкурента, партнера ухвалити вигідне для своєї країни рішення. Громадська думка сама по собі перетворилася на щонайпотужніший інструмент досягнення цієї мети. Здійснюючи вплив за допомогою тієї чи іншої інформації, яка надходить через засоби комунікації, на світогляд, свідомість, психіку людей, вдається досягати того, що уряди країн, котрі зазнали інформаційних нападів, ухвалюють «нав'язані», невигідні для свого народу і своєї країни рішення [1; 9].

Насиченість світу новітніми засобами відтворення, передавання та отримання інформації значно спростила механізми інформаційно-психологічної дії на людей. Мозок людини, її психіка, свідомість зазнають змін і самі, у свою чергу, здатні змінювати об'єктивну реальність через людську діяльність [2]. У цьому велике благо (активне творче начало в людині) і велика небезпека (дедалі вища ймовірність стати жертвою чиєїсь маніпуляції). Сучасні технології інформаційної дії дозволяють дезорієнтовувати людину в подіях, що відбуваються, керувати її поведінкою та вчинками непомітно для неї самої. Більш того, сьогодні така дія можлива на рівні не лише свідомості, а й підсвідомості. Інформаційно-психологічна дія дозволяє керувати як окремими особами, так і великими соціальними групами, державними інститутами та цілими державами. Керування великими групами людей за допомогою маніпулювання громадською думкою з метою формування того чи іншого ставлення до події (коментар) через засоби масової інформації (ЗМІ) продемонструвало високу ефективність. Контроль над громадською думкою в другій половині XX сторіччя став метою і засобом глобальної політичної боротьби.

Рішення, що ухвалюються на підставі несвоєчасно отриманої, неповної або спотвореної інформації, завжди призводять до втрат економічного, політичного, військового та іншого характеру. За всіх часів існування і виживання людини залежали від того, наскільки повно і своєчасно вона отримувала інформацію про загрози й небезпеки, а також від того, наскільки оперативно і адекватно реагувала на них [9; 11].

XXI сторіччя вже зарекомендувало себе як еру подальшого розвитку інформаційної сфери та боротьби за контроль над засобами комунікації. Зростаюча роль інформації у світопорядку зумовлює та посилює значущість і актуальність проблеми інформаційної безпеки та її складової — інформаційно-психологічної безпеки. Цю проблему можна схарактеризувати як необхідність протидії (у широкому розумінні) негативному інформаційно-психологічному впливу.

Протидія негативним інформаційно-психологічним діям у даному разі виступає як функція системи забезпечення інформаційної безпеки країни. Інформаційна безпека, у свою чергу, — це невід'ємна складова національної безпеки будь-якої держави.

Протидія негативній інформаційно-психологічній дії має відбуватись в інтересах забезпечення інформаційно-психологічної безпеки особи, суспільства, держави. Така безпека розуміється як стан захищеності особи, суспільства, держави від дії різноманітних інформаційних чинників (впливів, дій), що перешкоджають (або утруднюють) формуванню та функціонуванню адекватної інформаційно-орієнтованої основи соціальної поведінки людини і загалом життєдіяльності в сучасному суспільстві [9; 14]. При цьому відмітною особливістю слід вважати те, що інформаційно-психологічна дія спрямовується на орієнтувальну

основу діяльності людини, тобто на сам психологічний механізм людської діяльності [1].

Особливе місце при цьому відводиться органам державного управління, інститутам держави, що відповідають за формування морально-психологічного, економічного та військового потенціалу держави, її безпеку і оборону, тобто органам, які саме тому і є першочерговими об'єктами інформаційно-психологічної дії, що становить головну небезпеку, особливо в умовах низького рівня соціально-політичної стабільності в державі. Зазвичай негативні інформаційно-психологічні дії набирають форми СІО.

Головним джерелом поширення негативних інформаційно-психологічних впливів є національні й транснаціональні засоби масової інформації, інші інформаційні мережі, здатні впливати на світогляд, політичні погляди, правосвідомість, менталітет, духовні ідеали й ціннісні установки як окремої людини, так і суспільства в цілому.

Основними механізмами протидії деструктивним інформаційно-психологічним діям можуть бути:

- досягнення або підтримання морально-психологічного стану, що забезпечує функціонування держави та збереження соціально-політичної стабільності суспільства;
- нейтралізація або значне послаблення наслідків інформаційних і психологічних операцій та акцій супротивника, іншої негативної інформаційно-психологічної дії;
- захист моральної стійкості населення та морального духу співробітників державних управлінських і силових структур;
- створення необхідних умов для розв'язання поставлених завдань;
- формування та стимулювання в об'єкта, на якого спрямовано негативну дію, думок, поглядів, переконань, емоцій, поведінки, що відповідають інтересам забезпечення психологічної та інформаційної безпеки.

Організація управління інформаційно-психологічною безпекою населення може зводитися або до превентивного управління (за умови високого рівня соціально-політичної стабільності в державі), або до протидії реальним інформаційно-психологічним впливам.

Класична СІО містить чотири етапи [3; 4; 8]:

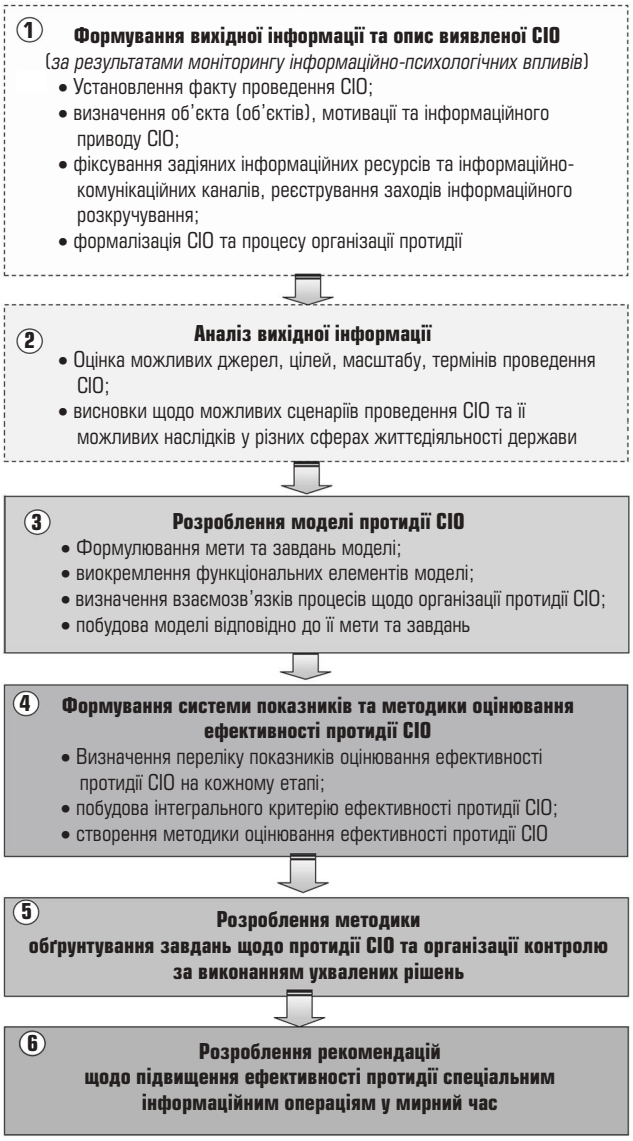
1) підготовчий етап (планування);

2) створення інформаційного приводу;

3) інформаційне розкручування;

4) етап виходу з операції (закріплення досягнутого ефекту).

Для організації ефективної протидії СІО, у ході якої здійснюються негативні інформаційно-психологічні впливи на населення країни, пропонується методика, що включає в себе шість відносно самостійних етапів (див. рисунок).



Загальна структура методики організації протидії СІО

Етап 1-й. ***Формування вихідної інформації, яка разом із формальним описом виявленої СІО, дала б змогу забезпечити організацію процесу протидії цій СІО.***

Інструментом отримання такої інформації є моніторинг інформаційно-психологічних впливів на вище політичне керівництво та населення держави. У ході моніторингу передбачається встановлення самого факту проведення СІО та об'єкта (об'єктів) такої операції, мотивів її проведення, а також визначення інформаційного приводу СІО. Необхідно також зафіксувати задіяні інформаційні ресурси сторони (сторін), що розпочинають СІО, і їхні інформаційно-комунікаційні канали, провести реєстрацію заходів інформаційного розкручування тощо.

Етап 2-й. ***Аналіз вхідної інформації з метою створення уявлення щодо можливих джерел, цілей, масштабу, термінів проведення СІО.***

На цьому етапі мають бути сформульовані висновки щодо вірогідних сценаріїв проведення СІО та її можливих наслідків у різних сферах життєдіяльності держави (ефективності СІО).

Ефективність СІО залежить від багатьох чинників, передусім від результативності впливу на емоційну складову $U_{\text{em}}(t)$ населення (об'єкта) протягом визначеного часу t, вибраних каналів $K_{\text{i}}(t)$ передавання інформації на момент часу t, залучених на період проведення операції інформаційних ресурсів $R_{\text{i}}(t)$ використовуваних інформаційних технологій $\text{It}(t)$, ступеня $U_{\text{z}}(t)$, активації зворотного зв'язку, а також від ефективності $E_{\text{z}}(t)$ захисту (протидії) системи, на яку в державі покладається ця функція, вибраних часових параметрів проведення операції тощо.

Відповідну залежність можна подати функціоналом

$$E_{\text{CIO}}(t) = F\{U_{\text{em}}(t), K_{\text{i}}(t), R_{\text{i}}(t), \text{It}(t), U_{\text{z}}(t), E_{\text{z}}(t), t\}. \quad (1)$$

Вочевидь, розробники СІО на етапі планування намагатимуться максимізувати очікувану ефективність за тих обмежень, які для них буде визначено замовником [16; 17]. Серед обмежень розглядаються насамперед ресурси (фінансові, людські, інформаційні тощо). Реальна ефективність здебільшого буде менша від запланованої. Проте можливий і неочікуваний ефект через прояв синергетичних закономірностей. Запланована ефективність визначатиме основні параметри етапу інформаційного розкручування, а реальна ефективність — параметри етапу виходу з операції.

Акцент робиться на визначенні сценарію проведення СІО, найбільш критичного (з погляду завдання максимальної шкоди) для вищого політичного керівництва держави та населення.

Етап 3-й. ***Розроблення моделі протидії СІО. Формування мети та проміжних завдань моделі, визначення функціональних її елементів; взаємозв'язки процесів щодо організації протидії СІО.***

Цей етап, як і всі наступні, є реалізацією *практичного втілення* загальної методики дослідження проблеми організації протидії СІО.

Етап 4-й. ***Формування системи показників та розроблення методики оцінювання ефективності протидії СІО.***

Головні завдання цього етапу такі:

- формування переліку показників оцінювання ефективності протидії СІО та їх структурування;
- синтез інтегрального критерію ефективності протидії СІО;
- розроблення методики оцінювання ефективності протидії СІО.

Показники оцінювання ефективності протидії СІО доцільно подати у формальному вигляді як багатовимірний вектор (функціонал) [11; 13; 14], елементами якого є вибрані напрямки (цілі) протидії деструктивним інформаційно-психологічним впливам:

$$E_{\text{z}}(t) = F\{E_{\text{МПс}}(t), E_{\text{н}}(t), E_{\text{м.с}}(t), E_{\text{зМПс}}(t), t\}, \quad (2)$$

де $E_{\text{МПс}}$ — вектор, що описує рівень забезпечення морально-психологічного стану населення; $E_{\text{н}}$ — вектор, що описує ступінь нейтралізації (послаблення) наслідків деструктивного інформаційно-психологічного впливу; $E_{\text{м. с}}$ — вектор, що описує рівень захисту морального духу населення, зокрема співробітників державних управлінських та силових структур; $E_{\text{зМПс}}$ — вектор, що описує рівень забезпечення морально-психологічної стійкості населення (думок, поглядів, переконань, емоцій, поведінки, що відповідають інтересам забезпечення психологічної та інформаційної безпеки).

На цьому етапі також визначаються (встановлюються) граничні значення векторів $E_{\text{МПс}_{\text{гр}}}$, $E_{\text{н}_{\text{гр}}}$, $E_{\text{м. с}_{\text{гр}}}$, $E_{\text{зМПс}_{\text{гр}}}$.

Залежно від характеру, мети, масштабу СІО вибрані показники можуть бути розширені (скорочені).

Етап 5-й. ***Розроблення методики обґрунтування завдань щодо протидії СІО та організації контролю за виконанням ухвалених рішень.***

У формалізованому вигляді управління G_{u} інформаційно-психологічною безпекою включатиме в себе вибір такої множини заходів:

$$G_{\text{u}} \Rightarrow \begin{cases} \text{Zp}_{\text{МПс1}}, \ \text{Zp}_{\text{МПс2}}, \ldots, \ \text{Zp}_{\text{МПс}K}, \\ \text{Zp}_{\text{н1}}, \ \text{Zp}_{\text{н2}}, \ldots, \ \text{Zp}_{\text{н}Q}, \\ \text{Zp}_{\text{м.с1}}, \ \text{Zp}_{\text{м.с2}}, \ldots, \ \text{Zp}_{\text{м.с}R}, \\ \text{Zp}_{\text{зМПс1}}, \ \text{Zp}_{\text{зМПс2}}, \ldots, \ \text{Zp}_{\text{зМПс}H}, \end{cases} \quad (3)$$

де Zp — захід реагування (протидії) за вибраним напрямком; K, Q, R, H — кількість заходів протидії за відповідним напрямком.

Ця множина забезпечить рівень інформаційно-психологічної безпеки, не нижчий від того, який узято за достатній $E_{\text{z}}(t) \geq E_{\text{zд}}(t)$ [15].

Етап 6-й. ***Обґрунтування рекомендацій щодо підвищення ефективності протидії спеціальним інформаційним операціям у мирний час.***

Як показує практика, протидія СІО має здійснюватися компетентними структурами, для чого в державі створюється відповідна система. Традиційно цю галузь діяльності в Україні віднесено до сфери забезпечення інформаційної безпеки держави [15]. А це означає, що ***в системі забезпечення інформаційної безпеки має функціонувати підсистема протидії спеціальним інформаційним операціям.*** Саме використання згаданої підсистеми у складі системи забезпечення інформаційної безпеки дає змогу більш ефективно використовувати ресурси та можливості системи вищого рівня (наприклад, результати моніторингу ЗМІ, державні ЗМІ, систему підготовки кадрів тощо).

Вибрані для розгляду типи СІО практично всі виходять із того, що об'єкти впливу мають специфічні системи інформаційного забезпечення своєї діяльності, зокрема й системи забезпечення інформаційної безпеки, що підпорядковуються відповідним адміністраціям або першим особам (Служба безпеки України, Служба зовнішньої розвідки України та ін.), «живуть» своїм внутрішнім життям. Тому їх можна розглядати як складні соціальні організації (підсистеми) зі своїми каналами інформації, інформаційними ресурсами, інформаційно-аналітичними структурами, які не тільки «фільтрують» та узагальнюють інформацію, а й за принципом лінзи подають її під певним кутом зору особі, що ухвалює рішення (ОУР), готують пропозиції щодо реагування з боку цієї особи на виявлені інформаційно-психологічні впливи [8; 11]. Ефективність таких впливів можна буде значно підвищити, якщо сили СІО матимуть в оточенні об'єктів впливу своїх «агентів впливу».

Для посилення ролі «агентів впливу» під гаслом демократизації до підготовки альтернативних варіантів реагування політичному керівництву держави-об'єкта «рекомендовано» ширше залучати структури так званого громадянського суспільства. В Україні таких структур, що фінансуються лише Заходом, понад 400. Звісно, що такі структури просуватимуть ті варіанти, які їм пропонуватимуть їхні спонсори, чим і буде досягатися потрібна ефективність СІО. Окрім того, «агенти впливу» мають значно ширші можливості деструктивно впливати на систему забезпечення інформаційної безпеки і, зокрема, на систему протидії СІО (наприклад, через процедуру добору та розставлення кадрів).

Висновки

Організація протидії деструктивним інформаційно-психологічним впливам, що набирають форми спеціальних інформаційних операцій проти населення держави, здійснювана згідно із запропонованою методикою, дасть змогу істотно підвищувати рівень захисту населення від деструктивних інформаційно-психологічних впливів, що відповідає суті та меті управління інформаційно-психологічною безпекою населення країни.

У подальших публікаціях буде докладно висвітлено окремі етапи запропонованої методики.

Література

1. ***Кара-Мурза, С. Г.*** *Манипуляция сознанием / С. Г. Кара-Мурза.—М.: Изд-во: Эксмо, 2005.— 832 с.*

2. ***Почепцов, Г.*** *Информационные войны: монографія [Електронний ресурс] / Г. Почепцов.— Режим доступу: www.novsu.ru/file/145368*

3. ***Литвиненко, О. В.*** *Спеціальні інформаційні операції та пропагандистські кампанії: монографія / О. В. Литвиненко.— К.: ВКФ «Сатсанга», 2000.— 225 с.*

4. ***Литвиненко, О. В.*** *Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія / О. В. Литвиненко.— К.: НІСД, 2003.— 240 с.*

5. ***Круглов, В.*** *Концепция информационно-ударной операции в современной войне / В. Круглов, Д. Ловцов // Обозреватель.— 1999.— № 12.— С. 49–51.*

6. ***Жуков, В.*** *Взгляды военного руководства США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение.— 2002.— № 1.— С. 3–5.*

7. ***Вепринцев, В.*** *Операции информационно-психологической войны [Електронний ресурс] / [В. Вепринцев, А. Манойло, А. Петренко, Д. Фролов].— Режим доступу: http://psyfactor.org/psyops/psyops4.htm*

8. ***Богданович, В. Ю.*** *Граф-модель процесу організації протидії спеціальним інформаційним операціям / В. Ю. Богданович, Д. А. Міщенко // Інформаційна безпека людини, суспільства, держави.— 2012.— № 1 (8).— С. 58–64.*

9. ***Богданович, В. Ю.*** *Теоретико-методологічні основи забезпечення національної безпеки України: монографія: у 7 т. Т.1: Теоретичні основи, методи й технології забезпечення національної безпеки України / В. Ю. Богданович, І. Ю. Свида, Є. Д. Скулиш; за заг. ред. Є. Д. Скулиша. — К.: Наук.-вид. відділ НА СБ України, 2012.— 548 с.*

10. ***Указ Президента України*** *від 12 лютого 2007 року № 105. Стратегія національної безпеки України «Україна у світі, що змінюється» (у редакції Указу Президента України від 8 червня 2012 року № 389 / 2012).*

11. ***Богданович, В. Ю.*** *Методичний підхід до агрегування засобів інформаційно-аналітичного забезпечення протидії інформаційним загрозам / В. Ю. Богданович, А. Л. Висідалко // Інформаційна безпека людини, суспільства, держави.— 2012.— № 3 (10).— С. 18–28.*

12. ***Богданович, В. Ю.*** *Забезпечення безпеки інформаційних процесів безпекового супроводу реалізації національних інтересів / В. Ю. Богданович, А. Л. Висідалко // Сучасний захист інформації.— 2013.— № 3.— С. 60–66.*

13. ***Богданович, В. Ю.*** *Концептуальна модель інформаційно-моніторингової системи національної безпеки / В. Ю. Богданович, А. Л. Висідалко // Захист інформації.— 2014.— Т. 16, № 1.— С. 81–88.*

14. ***Манойло, А. В***. *Государственная информационная политика в особых условиях: монографія / А. В. Манойло.— М.: МИФИ, 2003.— 388 с.*

15. ***Богданович, В. Ю.*** *Критерії, модель та методика оцінювання ефективності протидії спеціальним інформаційним операціям / В. Ю. Богданович, Д. А. Міщенко // Інформаційна безпека людини, суспільства, держави.— 2012.— № 2 (9). — С. 78–87.*

16. ***Saaty, Thomas L.*** *Multi-decisions decision-making: In addition to wheeling and dealing, our national political bodies need a formal approach for prioritization [Електронний ресурс] / Thomas L. Saaty // University of Pittsburgh, 322 Mervis Hall, Pittsburgh, PA 15260, United States / Mathematical and Computer Modelling.— 46 (2007) 1001–1016.— Режим доступу: www.elsevier.com/locate/mcm.*

17. ***Whitaker, R.*** *Validation examples of the Analytic Hierarchy Process and Analytic Network Process [Електронний ресурс] / R. Whitaker // Pittsburgh, PA, USA / Mathematical and Computer Modelling.— 46 (2007).— P. 840–859. — Режим доступу: www.elsevier.com/locate/mcm.*

В. Богданович, Д. Мищенко, А. Тупало, Т. Хропко

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ОРГАНИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТЬЮ НАСЕЛЕНИЯ В УСЛОВИЯХ НИЗКОГО УРОВНЯ СОЦИАЛЬНО-ПОЛИТИЧЕСКОЙ СТАБИЛЬНОСТИ В СТРАНЕ

Рассмотрены методологические подходы к организации управления информационно-психологической безопасностью населения в условиях низкого уровня социально-политической стабильности в стране. Обоснованы цель и задачи управления. Рассмотрен методический подход к формированию системы показателей оценивания эффективности противодействия деструктивным информационно-психологическим воздействиям и предложена методика управления информационно-психологической безопасностью политического руководства и населения. Проведены целевая функция и обобщенный алгоритм управления. Сформулированы условия обеспечения достаточного уровня информационно-психологической безопасности.

Ключевые слова: специальная информационная операция; деструктивное информационно-психологическое воздействие; психологическая безопасность; угрозы психологического характера; управление информационно-психологической безопасностью; эффективность противодействия.

V. Bogdanovitch, D. Mishchenko, A. Tupalo, T. Khropko

METHODOLOGICAL ASPECTS OF MANAGEMENT INFORMATION AND PSYCHOLOGICAL SECURITY OF THE POPULATION IN LOW-LEVEL SOCIAL AND POLITICAL STABILITY IN THE COUNRY

The article considers methodological approaches to management information and psychological safety of the population in terms of low socio-political stability. Reasoned goal, objectives, goals management. Considered methodical approach to building systems performance assessment effectiveness against destructive information and psychological impact and the method of management information and psychological Safety political leadership and the public. We give target function and generalized control algorithm. Formulated conditions provide a sufficient level of information-psychological security.

Keywords: special information operations; destructive information and psychological impact; psychological safety; threats psychological; management information and psychological security; effectiveness of countermeasures.

УДК 351.814.2

А. В. МІЩЕНКО, канд. техн. наук, доцент, Національний авіаційний університет, Київ

Методи дослідження економічної складової інформаційної безпеки авіаційної інфраструктури як складної системи інформаційної безпеки держави

Визначено методи дослідження економічної складової інформаційної безпеки авіаційної інфраструктури як складної системи інформаційної безпеки держави.

Ключові слова: національна безпека; інформаційна безпека; авіатранспортний комплекс; авіаінфраструктура; цільова ефективність; метод; методологія.

Актуальність

Наукове дослідження являє собою основний спосіб здобуття нових знань у будь-якій сфері людської діяльності. Це повною мірою стосується й системи інформаційної безпеки держави, що виступає рушієм її прогресу.

Методологія наукового дослідження економічної складової інформаційної безпеки авіаційної інфраструктури як складної системи інформаційної безпеки держави, що спирається на теоретичні засади економічної науки згідно із системним підходом [1], становить зміст фаху науковця, а її головні положення слугують керівникові підґрунтям для його здатності бачити проблемні завдання стосовно підвищення ефективності об'єкта своєї відповідальності, упроваджувати наукові новації та здійснювати керування на науковій основі. Отже, є сенс спинитися на фундаментальних методах реалізації принципів системного підходу в разі дослідження економічної складової інформаційної безпеки авіаційної інфраструктури.

Основна частина

Сучасна методологія науково-економічного дослідження економічної складової інформаційної безпеки авіаційної інфраструктури на ґрунті системного підходу вважає:

♦ ***об'єктом*** — ергатичну «складну» систему, якою є економічна складова інформаційної безпеки авіаційної інфраструктури;

♦ ***метою*** — удосконалення об'єкта дослідження — економічної складової інформаційної безпеки авіаційної інфраструктури;

♦ ***предметом*** виступає ефективність об'єкта як міра його досконалості за факторами «впливу» — системними ознаками;