DOI:**10.33099/2311-7249/2019-34-1-103-108**

УДК 355.40:356.35

Віталій Олександрович Кацалап *(кандидат військових наук)* [1]
Олександр Володимирович Войтко *(кандидат військових наук)* [1]
Юрій Володимирович Цурко [2]

[1] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***
[2] ***Центральний науково-дослідний інститут Збройних Сил України***

МЕТОДИЧНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ДЖЕРЕЛ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ У ВОЄННІЙ СФЕРІ

Запропоновано методичний підхід до визначення джерел загроз інформаційній безпеці у воєнній сфері, яка на відміну від існуючих враховує інформаційну можливість кожної складової воєнної організації. Використання такого підходу дасть можливість передбачити можливі зміни в інформаційному просторі. Відповідно до розробленої методики проведена якісна оцінка характеристик, які впливають на вагу часткових критеріїв відносної пріоритетності загроз інформаційної безпеки держави у воєнній сфер. Особливості квантифікації комплексних інформаційних загроз дозволяє: практично оцінювати стан інформаційної безпеки за кожною сферою національної безпеки; цілеспрямовано формувати і розвивати моніторинг зовнішніх і внутрішніх загроз інформаційній безпеці на основі системи показників цих загроз; більш обґрунтовано приймати рішення щодо підвищення рівня інформаційної безпеки за всіма сферами національної безпеки.

Ключові слова: *загрози, інформаційна безпека, воєнна організація держави*

Вступ

Забезпечення ефективного управління воєнною організацією держави вимагає своєчасного реагування на загрози інформаційній безпеці, зокрема, інформаційному середовищу у воєнній сфері. Перелік загроз національній безпеці у воєнній сфері викладений у Воєнній доктрині України, а спектр загроз воєнній безпеці України, до нейтралізації яких можуть залучатися Збройні Сили України, у Стратегічному оборонному бюлетені. Аналіз джерел [1-3] показує наявність суттєвих невідповідностей у визначенні цих загроз. Тому в статті під загрозою інформаційній безпеці у воєнній сфері розуміється здатність заподіяння будь-якого інформаційного впливу. Інформаційна безпека держави визначається можливістю нейтралізувати такий вплив.

Постановка проблеми. На сьогоднішній день у воєнній сфері розглядають такі загрози: посягання на державний суверенітет та територіальну цілісність держави; нарощування поблизу кордонів держави угруповань військ та озброєнь, які порушують співвідношення сил, що склалося; воєнно-політична нестабільність та конфлікти в сусідніх країнах; можливість застосування проти держави ядерної зброї та інших видів зброї масового знищення; зниження рівня боєздатності воєнної організації держави; політизація силових структур держави; створення та функціонування незаконних збройних формувань [4]. Посилення нестабільності інформаційного середовища є передумовою виникнення нових загроз інформаційній безпеці у воєнній сфері.

Існування інформаційних систем, що інтегровані до інформаційного суспільства, є зміна в своїх інтересах поведінки інших інформаційних систем або ж підтримання їх поведінки незмінною. Кожна інформаційна система може розглядатися як об'єкт інформаційного впливу, який реалізується цілеспрямованою передачею інформації, що включає як змістову (сутнісний бік, пов'язаний із відображенням реальної діяльності), так і представницьку складову (форму представлення інформації для передачі та забезпечення адекватного засвоєння) [5].

Аналіз останніх досліджень і публікацій. Аналіз публікацій [1-5] показав, що загрози інформаційній безпеці у воєнній сфері розроблені станом на 2017 рік. Але на сьогоднішній день джерела загроз змінилися [6, 7]. Це спричинило появу інших загроз інформаційної безпеки у воєнній сфері.

Мета статті полягає у викладенні моделі оцінки джерел загроз інформаційній безпеці у воєнній сфері яка, на відміну від існуючих, ураховує інформаційні можливості.

Виклад основного матеріалу дослідження

Аналіз джерел загроз інформаційній безпеці табл.1 свідчить про наявність у кожному джерелі воєнної складової, яка формує джерело загрози інформаційній безпеці у воєнній сфері.

Таблиця 1

Джерела загроз інформаційної безпеки

Зовнішні джерела загроз інформаційної безпеки	Внутрішні джерела загроз інформаційної безпеки
Вплив технічних засобів іноземної розвідки на політичні, економічні, військові структури	Маніпулювання суспільною свідомістю і політичною орієнтацією груп населення держави

Концепції окремих держав щодо інформаційної та психологічної війни	Дестабілізація політичних відносин між органами державної влади
Міжнародні терористичні організації та комп'ютерна злочинність	Дезорганізація діяльності управлінських структур
Міжнародна конкуренція за володіння інформацією	Блокування інформаційного ресурсу

Порівнюючи воєнну та інформаційну сферу можна окреслити варіанти джерел загроз інформаційній безпеці у воєнній сфері: дискредитація органів управління; провокування сутичок між органами управління воєнної організації держави; утруднення прийняття органами управління воєнної організації держави важливих рішень; підрив авторитету воєнної організації держави; нанесення втрат життєво важливим інтересам держави в оборонній сфері.

До джерел загроз інформаційній безпеці у воєнній сфері відносяться також прояви у вигляді отримання протиправного доступу до відомостей, що складають державну таємницю, та іншої конфіденційної інформації, розкриття якої може нанести загрозу національній безпеці. Проте найбільш небезпечним джерелом загроз інформаційній безпеці у воєнній сфері є неконтрольоване розповсюдження інформації про наявність хімічної та бактеорологічної зброї.

За класифікацією [8] джерела загроз інформаційній безпеці у воєнній сфері по рівнях ієрархії можна поділити на регіональні джерела загроз (стратегічний рівень), які стосуються діяльності всієї воєнної організації та локальні джерела загроз (тактичний рівень) за напрямком діяльності окремих її структур. Оцінки регіональних джерел загроз здійснюється на основі сукупності комбінацій локальних джерел загроз інформаційній безпеці у воєнній сфері.

Вибір локальних джерел загроз є основою для формування можливої загрози інформаційній безпеці у воєнній сфері, тому що вони, по-перше, визначають характер впливу на кожну структуру воєнної організації держави, а по-друге, задають напрям розвитку ситуації в національній безпеці.

Методологічною основою для розробки моделі оцінки джерел загроз інформаційній безпеці у воєнній сфері став інструментарій системи підтримки ухвалення стратегічних рішень, у якій була запропонована теоретико-множинна формалізація загроз інформаційній безпеці у воєнній сфері $b_{i\,заг}$:

$$b_{i\,заг} = \{S_{мм}, S_{ма}, S, h_{джер}\}, \qquad (1)$$

де $S_{мм}$ - модель оцінки воєнної могутності;

$S_{ма}$ - модель оцінки потенційної агресивності;

S - множина джерел загроз інформаційній безпеці;

$h_{джер}$ - модель оцінки джерел загрози інформаційній безпеці у воєнній сфері.

Оскільки зовнішнім середовищем для інформаційної безпеки у воєнній сфері є інформація про воєнно-політичну обстановку, прогноз її визначається темпом зростання інформаційної агресивності будь-якої держави у порівнянні з Україною G. Тоді зміна темпу зростання інформаційної агресивності держави $G_{інф_{агр}}$ буде характеризуватися станом інформації про воєнно-політичну обстановку $STAN$, а її постійність $POST$ (поточним рівнем інформації M і тенденцією до зміни (Mt) $POST = \{M, Mt\}$, що відображає інформаційну насиченість середовища. Інформаційну можливість воєнної організації держави IFM пропонується оцінювати по займаній нею частці інформації про воєнно-політичну обстановку D, а тенденцію зміни – по інформаційній активності воєнної організації, яка є часткою інформаційного середовища, що характеризується загальним об'ємом отриманої інформації I та імовірністю зміни цієї частки It. Тому модель оцінки воєнної могутності $S_{мм}$ містить взаємозв'язані показники, які характеризують стан інформації про воєнно-політичну обстановку та кількість інформації $STAN = \{G, G_{інф_{агр}}\}$, інформаційну активність воєнної організації $INF = \{D, I, It\}$:

$$S_{мм} = \{STAN, POST, INF\}. \qquad (2)$$

Розгляд кожного локального джерела загрози інформаційній безпеці у воєнній сфері, вимагає врахування внутрішніх інформаційних можливостей відповідної структури воєнної організації. На підставі цього в моделі оцінки потенційної агресивності $S_{ма}$ поєднані показники управління інформацією UIF, інформаційні можливості однієї зі структур воєнної організації $IFM_{струк}$ та рівень насиченості інформацією в кожній структурі воєнної організації $IRNIF$:

$$S_{ма} = \{UIF, IFM_{струк}, IRNIF\}. \qquad (3)$$

Ефективність управління інформаційною сферою воєнної організації UIF пропонується оцінювати як частку втрат інформаційного ресурсу A за певний проміжок часу $Про_t$, $MAR = \{A, Про_t\}$. Інформаційні можливості однієї зі структур воєнної організації держави $IFM_{струк}$ оцінюються часткою витрат на формування інформаційного простору IFP кожної структури воєнної організації N. Звідси $IFM_{струк} = \{N, P\}$. Тоді рівень насиченості інформацією $IRNIF$ пропонується оцінювати поточним її об'ємом Z у відповідній інформаційній сфері Z^*. Отримаємо вираз $IFM_{струк} = \{Z, Z^*\}$.

Стан джерела загрози інформаційній безпеці у воєнній сфері в будь-який момент часу може бути описаний сукупністю конкретних значень кількісних і якісних показників. Перехід від кількісної шкали до дискретної здійснюється шляхом розбиття діапазону зміни значення

параметра на непересічні інтервали. При цьому J - ий інтервал позначається як ξ_j^1. Якщо параметр x_1 вимірюється за шкалою найменувань, то ξ_j^1 - приймаємо за лінгвістичне поняття відповідного джерела загрози.

Наприклад, показник насиченості інформаційного середовища Z розраховується відповідно до рівнів, які мають значення: ("вища інформаційна безпека", "стала інформаційна безпека", "нижча інформаційна безпека".

Використання наведених дискретних шкал дозволяє побудувати модель оцінки джерел загроз інформаційній безпеці у воєнній сфері $h_{джер}$ рис. 1.

Рис. 1. Модель оцінки джерел загроз інформаційній безпеці у воєнній сфері

Порядок використання моделі складається із таких етапів:

- ідентифікація інформаційної ситуації S_i відобразимо вектором стану

$$\vec{P}=\begin{cases} G,Gt,M,Mt,D,Dt,I,It,A, \\ O,N,P,Z,Z^* \end{cases}, P\in X \quad (4)$$

Тоді представлений вираз $Par(x_1, w_k^1)$ може бути описаний залежностями:

$$S_i : Par\left(G,\xi_{kG}^{G}\right)\&\,Par\left(Gt,\xi_{kGt}^{Gt}\right)\&\,Par\left(M,\xi_{kM}^{M}\right)\&\,Par\left(Mt,\xi_{kMt}^{Mt}\right)$$
$$Par\left(D,\xi_{kD}^{D}\right)\&\,Par\left(Dt,\xi_{kDt}^{D}\right)\&\,Par\left(I,\xi_{kI}^{I}\right)\&\,Par\left(It,\xi_{kIt}^{I}\right)\&\,Par\left(A,\xi_{kA}^{A}\right)\& \quad (5)$$
$$Par\left(O,\xi_{kO}^{O}\right)\&\,Par\left(N,\xi_{kN}^{N}\right)\&\,Par\left(P,\xi_{kP}^{P}\right)\&\,Par\left(Z,\xi_{kZ}^{Z}\right)\&\,Par\left(Z^*,\xi_{kZ}^{Z^*}\right);$$

- виявлення відносин переваг $Best$ (ξ_i^0, ξ_j^0), що приймає істинне значення в тому випадку, якщо одне значення критерію $x_o = \xi_i^o$ переважно іншого x_o для ідентифікації інформаційної ситуації S_i;

- оцінки обмежень за параметрами Bel $(x_o \;\; w^1(s_i)$, якщо параметр x_1 відповідає допустимому або нормативному показнику множини; виявлення залежності між параметрами x_1 і x_j та значеннями Dep (x_1, x_j), для обліку взаємозв'язаних параметрів між собою. Залежність між параметрами, що описують ситуацію, встановлюється безліччю правил z, складених у вигляді логічних формул:

$$z = Dep(x^o, x_1)\&\,Dep(x^0, x_2)\&...\&\,Dep(x^o, x_1)\vee Dep(x_1, x_2)\& \quad (6)$$
$$Dep(x_1, x_3)\&...\&\,Dep(x_1, x_k)\vee...$$

За допомогою правил L об'єднуються у відносини:

$$L = Par(x_1, \xi_{kL}^1)\&\,Best(\xi_i^1, \xi_j^1)\&\,Bel(x_1, w^1(s))\&\,Dep(x_1, x_m) \quad (7)$$

- рішення $h_{джер_i}$ по вибору джерела загрози S_{ir} ухвалюється, якщо визначена ситуація S_1, при якій виявлена залежність між параметрами z_1 та співвідношення L_1.

Запропонована модель оцінки джерел загроз інформаційній безпеці у воєнній сфері становить теоретико-множинну форму взаємозв'язків між чинниками зовнішнього середовища і внутрішніми можливостями воєнної організації. Врахування зазначених взаємозв'язків дозволяє окреслити правила формування логічних виразів, які надалі стануть основою методології забезпечення інформаційної безпеки у воєнній сфері рис. 2.

Наведена методологія описує взаємозв'язки між ієрархією інформаційного середовища та інформаційними можливостями кожної структури воєнної організації у вигляді графів з вершинами P_{f_1} та P_{f_2}. Значення цих вершин будуть характеризувати мету якою є виявлення на ранніх стадіях загроз інформаційній безпеці у воєнній сфері.

Для формування загроз інформаційній безпеці у воєнній сфері в наведеній методології використовуються як кількісні, так і якісні показники значення яких можна подати виразом:

$$G = \langle \{f\}, \{m\}, \{b\}, \{h_{джер}\} \rangle, \quad (9)$$

де f - оцінка загроз національній безпеці;

m - оцінка загроз інформаційній безпеці;

b - оцінка загроз інформаційній безпеці у воєнній сфері;

$h_{джер}$ - оцінка джерел загроз інформаційній безпеці у воєнній сфері на основі запропонованої на основі запропонованої моделі рис.1.

Поряд з цим, якісний аналіз впливу характеристик на вагу часткових критеріїв відносної пріоритетності загроз інформаційної безпеки у воєнній сфері показує, що вони

характеризуються значною кількістю нерівнозначних, суб'єктивних і об'єктивних факторів. Це не дозволяє тільки шляхом логічного аналізу встановити прийнятну за всіма ознаками, з певним ступенем компромісу, пріоритетність часткових критеріїв відносної пріоритетності.

Вирішальною перевагою у порівнянні з іншими існуючими методами оцінювання альтернатив (у тому числі з методами безпосереднього експертного оцінювання) є чіткий вираз суджень.

Інформаційні загрози національним інтересам в усіх сферах діяльності постійно кількісно та якісно змінюються. Ці загрози, реалізація яких шляхом інформаційного впливу призводить до реальних негативних наслідків, потребують прийняття спеціальних заходів щодо їх відвернення або мінімізації. Комплексне вирішення проблем інформаційної безпеки військ, їх захист від деструктивного інформаційного впливу потребує урахування наступних початкових умов.

1. Система забезпечення інформаційної безпеки воєнної сфери є частиною (підсистемою) складної системи військового призначення – системи військового управління. Головне завдання системи забезпечення ІБ, це безперервна оцінка стану ІБ та доповідь керівництву відповідних показників.

2. Це завдання може бути виконано, якщо в системі ІБ буде здійснюватися моніторинг інформаційних загроз.

3. Для оцінки впливу інформаційних загроз на якість військового управління треба будувати надійну систему моніторингу.

Створення такої системи базується на різних методичних підходах, деякі з них розглянемо у цьому розділі. Під складною системою розуміється система зі слабко передбачуваними властивостями, що схильні до схованих чи самостійних тенденцій поводження. У військовій системотехніці під складними системами розуміються угруповання військ (оперативно – тактичні системи) і комплекси озброєння [5]. Систему військового управління можна розглядати як складну систему військового призначення організаційного типу, що дає можливість під час дослідження застосовувати принципи системного підходу, який припускає декомпозицію системи на складові. Так із системи управління для подальших досліджень доцільно виділити систему забезпечення інформаційної безпеки.

Сутність оцінки інформаційного впливу (конструктивного та деструктивного) на систему військового управління полягає у знаходженні таких співвідношень між відповідними показниками інформаційного впливу та функціонування системи управління, які можуть забезпечити виконання бойових завдань. Це є головною вимогою до методу досліджень, який буде застосований.

Вибір можливого методичного підходу до оцінки інформаційного впливу на систему військового управління визначається багатьма умовами, які впливають на кінцевий результат інформаційного протиборства, але цей підхід доцільно вибирати з методів порівняльного оцінювання варіантів системи.

Порівняльний аналіз методичних підходів [37] показує, що більш простим і прийнятним для порівняльного оцінювання ефективності системи забезпечення інформаційної безпеки є метод аналізу ієрархій (МАІ). Цей метод являє собою систематичну процедуру ієрархічного представлення елементів які визначають сутність задачі, що розв'язується. Метод передбачає декомпозицію задачі (її ієрархічне зображення) на більш прості складові частини і подальшу обробку послідовності суджень експертів попарним порівнянням, починаючи від вихідних елементів і переходячи від рівня до рівня, поки не буде отримана кінцева оцінка розв'язання задачі.

На основі МАІ розроблений метод експертної оцінки загроз інформаційній безпеці держави, у якому використовується ідентифікація та квантифікація реальних і потенційних загроз інформаційній безпеці в усіх сферах національної безпеки. У подальших дослідженнях цей метод доцільно взяти за основу для оцінки впливу інформаційних загроз на інформаційну безпеку системи військового управління.

Ідентифікація загроз інформаційній безпеці розглядається як процес розпізнавання таких їхніх ознак, які характеризують небажані наслідки їхнього прояву і можуть адекватно сприйматися системою моніторингу цих загроз. Ідентифікація інформаційних загроз у системі моніторингу безпосередньо визначається їхньою структуризацією за всіма сферами національної безпеки відповідно до Доктрини інформаційної безпеки України. Для воєнної сфери інформаційні загрози структуровані у двох варіантах (табл. 1) відповідно до джерел [7, 8]. При необхідності ці загрози можна доповнювати та трансформувати.

Квантифікація є процесом надання кількісної оцінки якісним ознакам певного процесу або явища. Для структурованих ознак інформаційних загроз у воєнній сфері практичне (емпіричне) їхнє оцінювання можливе за показниками, наведеними у рис.1. Після здійснення емпіричних оцінок показників вони мають бути співставленні з їхніми критичними значеннями у різних сферах національної безпеки. Критичні значення представляють граничні межі, перевищення яких призводить до деградації чи суттєвого послаблення безпеки об'єктів захисту. У результаті цього можливі значні матеріальні, моральні та інші втрати. Тому головним завданням системи моніторингу інформаційних загроз має бути контроль і збереження такого стану інформаційної безпеки, за якого забезпечується перебування її показників у допустимих межах.

Враховуючи ці закономірності моніторингу загроз інформаційній безпеці, пропонується в якості граничних значень показників цих загроз визначити 1/3 для їхніх абсолютних значень.

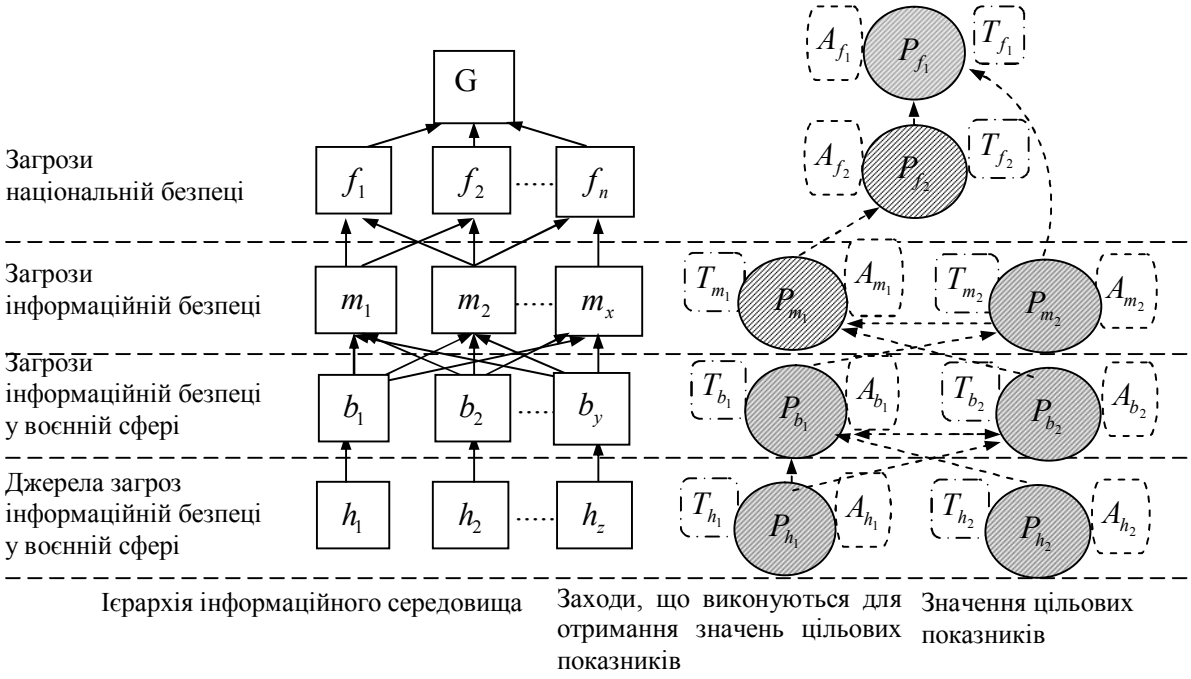

Рис. 2. Методологія забезпечення інформаційної безпеки у воєнній сфері

Варіант якісної оцінки впливу характеристик на вагу часткових критеріїв відносної пріоритетності загроз інформаційної безпеки у воєнній сфері наведена у табл. 1. Відповідно до наведених характеристик (рис.1) загальними позитивними факторами часткових критеріїв відносної пріоритетності загроз інформаційній безпеці у воєнній сфері для таких кризових ситуацій застосування Збройних Сил.

Висновки й перспективи подальших досліджень

Підводячи підсумок, можна стверджувати, що заздалегідь визначена загроза інформаційній безпеці у воєнній сфері дасть можливість передбачити її реалізацію в умовах існування інформаційних технологій, які включають питання захисту інформації, як такої інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів.

Зробити висновок щодо переваги одного часткового критерію загроз інформаційній безпеці відносної відносно іншого можна за результатами співставлення певних характеристик, таких як: час появи загрози; втрати; сфера впливу; простота у діях; сил і засобів, які залучаються для локалізації.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть вчинити збиток чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян.

Література

1. Левченко О.В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки/ О.В. Левченко // Наука і техніка Повітряних Сил Збройних Сил України. – 2015.№3(20). – С.47–50. **2. Косогов О.М.** Методика визначення заходів протидії інформаційним загрозам державі у воєнній сфері // Системи обробки інформації. – 2016, №3(140). С.25–29. **3. Балуев Д. Г.** Информационная революция и современные международные отношения: Учебное пособие. – Нижний Новгород: ННГУ, 2000. – 107 с. **4. Бусленко Н. П.** Моделирование сложных систем. – М.: Наука, 1978. - 399 с. **5. Венцель Е. С.** Исследование операций. – М.: Знание, 1976. – 64 с. **6. Концепція** інформаційної безпеки держав-учасників Співдружність Незалежних Держав у військовій сфері, 1993. – 14 с. **7. Морозов О.** Інформаційна безпека в умовах сучасного стану і перспективи розвитку державності //Віче. – 2007. – № 12. – Спецвипуск. – С. 23–25. **6. Крюков О. І.** Інформаційна безпека держави в умовах глобалізації / О. І. Крюков. // Державне будівництво. - 2007. – № 2. – Режим доступу: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12.

МЕТОДИЧЕСКИЙ ПОДХОД К ОПРЕДЕЛЕНИЮ ИСТОЧНИКОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВОЕННОЙ СФЕРЕ

Виталий Александрович Кацалап *(кандидат военных наук)* [1]
Александр Владимирович Войтко *(кандидат военных наук)* [1]
Юрий Владимирович Цурко [2]

[1] ***Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина***

[2] Центральный научно-исследовательский институт Вооруженных Сил Украины

Предложен методический подход к определению источников угроз информационной безопасности в военной сфере, которая в отличие от существующих учитывает информационную возможность каждой составляющей военной организации. Использование такого подхода даст возможность предусмотреть возможные изменения в информационном пространстве. В соответствии с разработанной методикой проведена качественная оценка характеристик, которые влияют на вес частичных критериев относительной приоритетности угроз информационной безопасности государства в военной сфер. Особенности квантификации комплексных информационных угроз позволяет: практически оценивать состояние информационной безопасности за каждой сферой национальной безопасности; целеустремленно формировать и развивать мониторинг внешних и внутренних угроз информационной безопасности на основе системы показателей этих угроз; более обоснованно принимать решение относительно повышения уровня информационной безопасности за всеми сферами национальной безопасности.

Ключевые слова: *Угрозы, информационная безопасность, военная организация государства*

METHODICAL GOING NEAR DETERMINATION OF SOURCES OF THREATS TO INFORMATIVE SAFETY IN MILITARY SPHERE

Vitaliy Katsalap *(Candidate of military sciences)* [1]
Oleksandr Voitko *(Candidate of military sciences)* [1]
Yurii Tsurko [2]

[1] ***National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine***
[1] ***Central research institute of Military Powers of Ukraine***

The methodical going is offered near determination of sources of threats to informative safety in a military sphere, that unlike existing takes into account informative possibility of every constituent of military organization. The use of such approach will give an opportunity to foresee possible changes in informative space. In accordance with the worked out methodology the quality estimation of descriptions that influence by weight of partial criteria of relative priority of threats of informative safety of the state in military spheres is conducted. Allows the features of квантифікації of complex informative threats : practically to estimate the state of informative safety after every sphere of national safety; purposefully to form and develop monitoring of external and internal threats to informative safety on the basis of the system of indexes of these threats; more reasonably to make decision in relation to the increase of informative strength security after all spheres of national safety.

Key words: *Threats, information security, hierarchical structure.*

References

1. Levchenko O.V. (2015), The conceptual approach of assessing the state of information security [Konceptualjnyj pidkhid do kompleksnoji ocinky stanu informacijnoji bezpeky], Nauka i tekhnika Povitrjanykh Syl Zbrojnykh Syl Ukrajiny, №3(20). – pp. 47–50. **2. Kosogov O.M.** (2016), Methods of the determination information threats reluctances actions to state in military sphere [Metodyka vyznachennia zakhodiv protydii informatsiinym zahrozam derzhavi u voiennii sferi], Systemy obrobky informatsii, №3 (140). – pp. 25–29. **3. Baluev D.H.** (2000), Informatsionnaya revolyutsiya i sovremennyie mezhdunarodnyie otnosheniya: Uchebnoe posobie. – Nizhniy Novgorod: NNGU, 107 p. **4. Buslenko N.P.** (1978), The Modeling of Complex Systems [Modelirovanie slozhnyih system], Moscow: Nauka, 399 p. **5. Ventsel E.S.** (1976), The Operations Research [Issledovanie operatsiy], Moscow: Znanie, 64 p. **6. Kontseptsiia** informatsiinoi bezpeky derzhav-uchasnykiv Spivdruzhnist Nezalezhnykh Derzhav u viiskovii sferi (1993), – 14 p. **7. Morozov O.** (2007), Informatsiina bezpeka v umovakh suchasnoho stanu i perspektyvy rozvytku derzhavnosti, Viche, № 12. – pp. 23–25. **8. Kriukov O.I.** (2007), Informatsiina bezpeka derzhavy v umovakh hlobalizatsii, Derzhavne budivnytstvo, №2.