УДК 354.42

О.М. Косогов, А.О. Сірик

Військова частина А1906, Київ

МЕТОДИКА ВИЗНАЧЕННЯ СТРУКТУРИ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МІНІСТЕРСТВА ОБОРОНИ ТА ЗБРОЙНИХ СИЛ УКРАЇНИ

У статті запропоновано методику обґрунтування раціональної структури системи інформаційної безпеки Міністерства оборони та Збройних Сил України на основі методу кластерного аналізу, метою якого є пошук наявних структур, що виражається в утворенні груп схожих між собою об'єктів – кластерів. На відміну від інших методів, цей метод дає змогу класифікувати об'єкти не за однією, а за декількома ознаками одночасно як сукупність взаємопов'язаних функціональних підсистем із визначенням функцій кожної з них. Наведено варіант дендрограми об'єднання кластерів (структурних підрозділів) за виміром близькості функцій та завдань відповідно до підсистем системи.

Ключові слова: *інформаційна безпека, система інформаційної безпеки, структура, кластерний аналіз, Міністерство оборони, Збройні Сили України.*

Вступ

Постановка проблеми. Аналіз літератури. В умовах перманентного інформаційного протиборства у світі стрімко зростає рівень та значно розширюється спектр інформаційних загроз. Така ситуація становить серйозну небезпеку національній і міжнародній безпеці та призводить до важкопрогнозованих і часом непередбачуваних наслідків у всіх сферах життєдіяльності держави (воєнній, воєнно-політичній, економічній, інформаційній тощо).

Яскравим прикладом цього є потужна інформаційна кампанія Росії проти України, яка проводиться з метою руйнування української державності, і є важливою складовою дій Російської Федерації (РФ) в її гібридній війні.

На заваді цим загрозам може стати лише ефективна система протидії інформаційному впливу, яка забезпечуватиме прийнятний рівень інформаційної безпеки в Україні.

На сьогодні у нашій державі та її Збройних Силах ще не до кінця створено цілісну систему інформаційної безпеки (СІБ), яка б у повному обсязі забезпечувала гарантований захист і надійну протидію інформаційним загрозам. Разом з тим, триває інтенсивний процес її формування, а саме у Міністерстві оборони (МО) України розроблені концептуальні документи та плани щодо розгортання такої системи, у Збройних Силах (ЗС) України створюються відповідні підрозділи [1].

Однак відсутність власного досвіду формування зазначеної системи та різноплановість поглядів на шляхи забезпечення інформаційної безпеки у сфері оборони держави, складність вивчення питань інформаційної безпеки у воєнній сфері, яка полягає у слабко виявлених зв'язках між елементами всієї системи, не дає можливості повною мірою визначити структуру СІБ зазначеної сфери, визначити її завдання та функції.

Аналіз останніх досліджень і публікацій [2–3] щодо визначення різних організаційно-функціональних структур МО та ЗС України показав, що існуючі методичні підходи базуються на використанні ймовірнісних показників статистичних даних та врахуванні досвіду формування військових підрозділів (систем) збройних сил інших держав. Такі підходи визначають структури військових підрозділів (систем) без чіткого розбиття їх на складові відповідно до покладених на них функцій та завдань.

Тому розробка науково обґрунтованих підходів до обґрунтування раціональної структури СІБ держави у сфері оборони є актуальним науково-практичним завданням.

Метою статті є: розробка методики обґрунтування раціональної структури СІБ МО та ЗС України.

Виклад основного матеріалу

Основною метою створення СІБ держави у сфері оборони є попередження та нейтралізація інформаційних загроз їх функціонуванню; створення умов для сталого та гарантованого виконання ЗС та МО України завдань, визначених Конституцією та законами України.

Відповідно до зазначеної мети основними функціями такої системи можуть бути [1]:

1. Створення і забезпечення діяльності організаційних структур та елементів системи, що включає:

– розроблення адміністративно-правових засад для побудови та функціонування системи;

– всебічне забезпечення діяльності елементів системи.

2. Управління Системою, що включає:

– розроблення та введення в дію Керівництва із забезпечення інформаційної безпеки в МО та ЗС Укра-

їни, в якому визначаються єдині підходи до попередження та нейтралізації інформаційних загроз;

– прогнозування, планування, організація, координація та контроль у межах системи та окремих її елементів;

– оцінювання результативності заходів протидії інформаційним загрозам, витрат на їх підготовку та проведення.

3. Проведення планової та оперативної діяльності щодо забезпечення інформаційної безпеки та протидії інформаційним загрозам, що включає:

– визначення та формування моделі потенційних та реальних інформаційних загроз;

– визначення об'єктів критичної інфраструктури, що мають важливе значення для національної безпеки і оборони; виявлення інформаційних загроз, джерел їх виникнення, а також прогнозування можливих наслідків у разі їх реалізації із відпрацюванням відповідних превентивних заходів;

– удосконалення форм, методів і засобів запобігання загрозам інформаційній безпеці та ліквідації наслідків її порушення.

З метою визначення елементів системи, їх завдань, доцільно її розглянути як організовану сукупність взаємопов'язаних функціональних підсистем:

а) підсистеми виявлення інформаційних загроз;

б) підсистеми аналізу і прогнозування загроз та планування заходів інформаційної безпеки;

в) підсистеми протидії інформаційним загрозам;

г) підсистеми захисту від інформаційних загроз;

д) підсистеми наукових досліджень та підготовки спеціалістів з питань інформаційної безпеки.

На ці підсистеми можуть бути покладені такі основні завдання.

На підсистему виявлення інформаційних загроз:

виявлення ознак інформаційно-психологічного впливу на особовий склад Збройних Сил України;

виявлення кібернетичних загроз функціонуванню інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем;

виявлення джерел, які можуть спричинити виток інформації з обмеженим доступом;

виявлення невідповідностей стану та можливостей інформаційно-телекомунікаційних систем та інших інформаційних систем військового призначення сучасним вимогам;

На підсистему аналізу і прогнозування загроз та планування заходів інформаційної безпеки:

збір, узагальнення та систематизація даних про інформаційні загрози, їх оцінювання та прогнозування їх розвитку;

оцінювання джерел інформаційно-психологічного та інформаційно-технічного впливу;

визначення об'єктів критичної інфраструктури;

планування заходів інформаційної боротьби.

На підсистему протидії інформаційним загрозам:

адекватне реагування на кризові ситуації в інформаційному просторі;

підготовка та ведення інформаційних (інформаційно-психологічних) операцій (заходів);

інформаційно-аналітичне забезпечення заходів реагування на кризові ситуації, що спричинюються інформаційними загрозами;

комплектування, забезпечення, підготовка та управління застосуванням сил і засобів захисту інформації та кібернетичної безпеки в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах.

На підсистему захисту від інформаційних загроз:

захист інформаційного простору від кібератак, зокрема захисту об'єктів критичної інфраструктури;

контроль використання інформації з обмеженим доступом;

захист особового складу ЗС та МО України від негативного інформаційно-психологічного впливу.

На підсистему наукових досліджень та підготовки спеціалістів з питань інформаційної безпеки:

замовлення проведення науково-дослідних та дослідно-конструкторських робіт за напрямами інформаційної безпеки;

формування державного замовлення і підготовка відповідних спеціалістів з питань інформаційної безпеки держави у воєнній сфері.

Система інформаційної безпеки МО та ЗС України являє собою сукупність її суб'єктів, що виконують різні завдання інформаційної безпеки за напрямом своєї діяльності. Для створення структури СІБ необхідно об'єднати структурні підрозділи МО України та Генерального штабу (ГШ) ЗС України у вищезазначені функціональні підсистеми за обраним показником. Таким показником може бути близькість функцій із забезпечення інформаційної безпеки, що виконуються цими структурними підрозділами. Для вирішення цього наукового завдання доцільно використати метод кластерного аналізу, метою якого є пошук наявних структур, що виражається в утворенні груп схожих між собою об'єктів – кластерів. На відміну від інших методів, цей метод дає змогу класифікувати об'єкти не за однією, а за декількома ознаками одночасно [4].

Таким чином, методика визначення структури СІБ МО та ЗС України на основі кластерного аналізу призначена для розробки їх структур, виходячи з покладених на них функцій та завдань забезпечення інформаційної безпеки.

Вхідними даними часткової методики є перелік функцій та завдань забезпечення інформаційної

безпеки та відповідних структурних підрозділів МО та ГШ ЗС України.

Вихідними даними часткової методики є структура СІБ МО та ЗС України за належністю до відповідних підсистем.

Використання методики визначення структури СІБ МО та ЗС України, що грунтується на використанні апарату кластерного аналізу, передбачає ряд обмежень та припущень:

– завдання із забезпечення інформаційної безпеки у межах певної підсистеми мають бути одного рівня виконання;

– масив даних до кластерного аналізу встановлюється шляхом проведення експертного оцінювання;

– участь відповідного структурного підрозділу у виконанні поставлених завдань інформаційної безпеки оцінюється експертом у відсотковому відношенні так, щоб сума за всіма завданнями становила 100 %.

У загальному вигляд проведення кластерного аналізу передбачає кілька етапів [5]: підготовка даних до кластерного аналізу; вибір міри відстані між об'єктами та її обчислення; вибір стратегії кластеризації та методу кластерного аналізу; інтерпретація результатів кластеризації.

Дані для проведення кластерного аналізу підготовлюються шляхом формування матриці співвідношень. Вихідна множина складається з m підрозділів, що виконують k завдання щодо забезпечення інформаційної безпеки (табл. 1).

Таблиця 1

Матриця співвідношень

	Завдання k_1	Завдання k_2	...	Завдання kj
Підрозділ m_1	m_1/k_1	m_1/k_2	...	m_1/k_j
Підрозділ m_2	m_2/k_1	m_2/k_2	...	m_2/k_j
...	...	...	...	...
Підрозділ mj	m_j/k_1	m_j/k_2	...	m_j/k_j

При залученні для формування матриці співвідношень X_{mk} групи з Y експертів числове значення судження визначається як середнє арифметичне окремих суджень експертів:

$$\alpha_x = \frac{\sum_{b=1}^{Y} q_b \alpha_b}{Y}, \qquad (1)$$

де α_x – судження b-го експерта;

q_b – вага b-го експерта.

Наступним кроком є вибір міри відстані між об'єктами та її обчислення. В кластерному аналізі існує декілька підходів до визначення міри відстаней: евклідова відстань, квадрат евклідової відстані, відстань Чебишева, відсоток невідповідності, 1-коефіцієнт кореляції Пірсона [6], манхетинівська відстань, метрика Мінковського, відстань Махаланобіса [7]. Для кількісних шкал, якою є матриця співвідношень груп виконавців до завдань, застосовується евклідова відстань [8].

Евклідова відстань між об'єктами являє собою геометричну відстань між ними у багатовимірному просторі і визначається за формулою:

$$l_{rc} = \sqrt{\sum_{i=1}^{k} (y_{ri} - y_{ci})^2}, \qquad (2)$$

де значення $y_{ri} = \frac{\alpha_{xi} - \overline{\alpha_x}}{S_x}$; $y_{ci} = \frac{\alpha_{ix} - \overline{\alpha_x}}{S_x}$

$\overline{\alpha_x}$ – середнє арифметичне значень α_x за завданнями;

S_x – стандартне відхилення значень суджень експертів за завданнями;

k – кількість завдань.

З проведенням послідовних обчислень відстаней між усіма групами виконавців, будується матриця відстаней між ними:

$$L = \begin{pmatrix} 0 & l_{12} & \cdots & l_{1c} \\ l_{21} & 0 & \cdots & l_{2c} \\ \vdots & \vdots & \cdots & \vdots \\ l_{r1} & l_{r2} & \cdots & 0 \end{pmatrix},$$

при $r = c$ $l_{rc} = 0$, $r, c = 1,2,...,m$. Чим менше значення l_{rc}, тим ближче знаходяться між собою групи виконання завдань.

Вибір стратегії кластеризації полягає у визначенні правил об'єднання об'єктів у кластери. Основними правилами кластеризації є [9]:

– стратегія одиночного зв'язку. Стратегія ніби нанизує два кластери разом, і в результаті кластери подаються у вигляді довгих "ланцюжків";

– стратегія повного зв'язку. Стратегія добре працює, коли кластери належать різним класам;

– стратегія незваженого попарного середнього ефективна у випадку реального об'єднання об'єктів як у "кущі", так і в "ланцюжки", що дає змогу показати ієрархічне об'єднання об'єктів;

– стратегія зваженого попарного середнього. Ця стратегія також дає змогу об'єднати об'єкти як у "кущі", так і в "ланцюжки" і використовується тоді, коли передбачають появу кластерів нерівного розміру;

– стратегія Варда. Вона вважається ефективною, але при її використанні створюються кластери малого розміру.

Для визначення структури СІБ МО та ЗС України доцільно обрати стратегію зваженого попарного середнього, яка дає змогу об'єднати групи виконав-

ців з їх ієрархічним поданням і з визначенням їх розміру. Розрахунок проводиться за таким виразом [10]:

$$P(K_s K_t) = \frac{1}{n_s n_t} \sum_{L_r=1}^{K_s} \sum_{L_c=1}^{K_t} d(L_r, L_c), \qquad (3)$$

де $P(K_s K_t)$ – відстань між об'єктами (кластерами) K_s і K_t;

n_s, n_t – кількість елементів в кластерах K_s і K_t відповідно;

L_r, L_c – об'єкти (кластери), за якими відбувається пошук подібності;

d – відстань між L_r та L_c.

Для кінцевої інтерпретації отриманих даних доцільно обрати метод деревоподібної кластеризації [11], що забезпечує побудову ієрархічного кластерного дерева у вигляді дендрограми (рис. 1) [12].

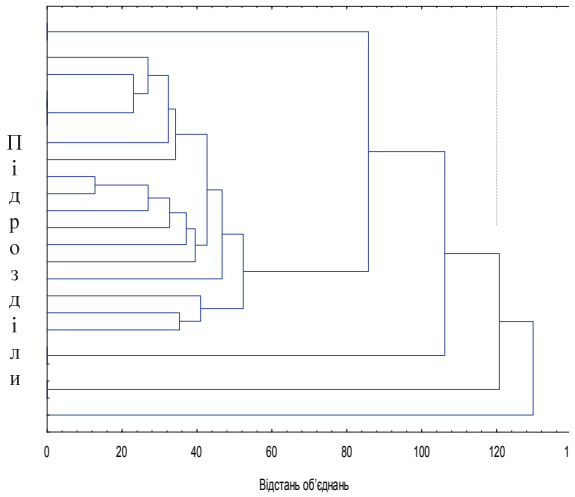

Рис. 1. Приклад дендрограми об'єднання кластерів (варіант)

На підставі наведеного, алгоритм методики визначення структури СІБ МО та ЗС України має вигляд, як показано на рис. 2.

Висновки

Запропонована методика визначення раціональної структури СІБ МО та ЗС України на основі методу кластерного аналізу. Метою кластерного аналізу є пошук наявних структур, що виражається в утворенні груп схожих між собою об'єктів – кластерів. На відміну від інших методів, цей метод дає змогу класифікувати об'єкти не за однією, а за декількома ознаками одночасно як сукупність взаємопов'язаних функціональних підсистем з визначенням функцій кожної з них.

Подальші дослідження слід спрямувати на розробці методів оцінювання ефективності СІБ МО та ЗС України.

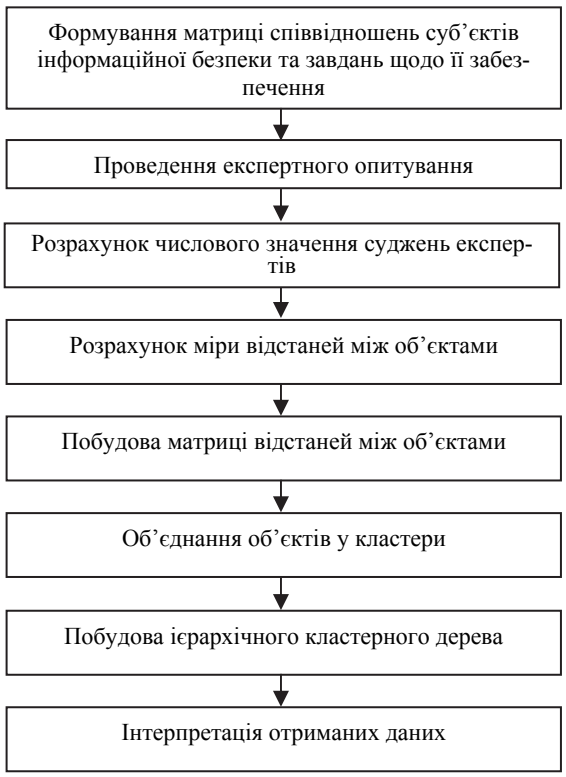

Рис. 2. Алгоритм методики визначення раціональної структури СІБ

Список літератури

1. Радковець Ю.І. Погляди на створення системи інформаційної безпеки України та її Збройних Сил / Ю.І. Радковець, О.В. Левченко, О.М. Косогов // Наука і оборона: щоквартальний науково-теоретичний та науково-практичний журнал. – К.: МО України, 2014. – № 1. – С. 38-42.

2. Гордонов В.П. Моделі визначення ефективності синтезу структури органу інформаційної підтримки рішень у системі управління Збройних Сил / В.П. Гордонов, О.П. Михайленко // Наука і оборона: щоквартальний науково-теоретичний та науково-практичний журнал. – К.: МО України, 2001. – № 2. – С. 39-43.

3. .Гвоздь В.І. Методика обґрунтування раціонального складу та чисельності складної військової системи / В.І. Гвоздь. – К.: ЦНДІ ЗС України, 2013. – 29 с.

4. Факторный дискриминантный и кластерный анализ / [Дж. – О.Ким, Ч.У.Мюллер, У.Р.Клеккандр]; пер. с англ. А.М. Хотинский, С.Б. Королева. – М. : Финансы и статистика, 1989. – 216 с.

5. Кластерний аналіз. Загальне поняття, його математичні основи та завдання. [Електронний ресурс]. – Режим доступу: http:/ib-ko.com/book_346_glava70_ &-2.7_k.

6. Sabine Landau. Cluster Analysis / Sabine Landau, Brians Everitt, Morven Leese, Daniel Stanl. – [5.th Edition]. – gohu Wiley & Sons, Ltd, 2011. – P. 71-110.

7. Методичні вказівки щодо формування структурних підрозділів центрального апарату Міністерства оборони України та визначення їх чисельності. – К.: Мінво оборони України, 2003. – 11 с.

8. Климчук В.О. Кластерний аналіз : використання у психологічних дослідженнях / В.О. Климчук // Практична психологія та соціальна робота. – 2006. – № 4. – С. 30-36.

9. Калинина В.Н. Введение в многомерный статистический анализ : учебник [для студ. высш. учеб. завед.] / В.Н. Калинина, В.И. Соловьев. – М. : ГУУ, 2003. – 66 с.

10. Мандель И.Д. Кластерный анализ / И.Д. Мандель. – М.: Финансы и статистика, 1988. – 176 с.

11. Gower J.C. A comparison of some methods of cluster analysis / J.C. Gower // Biometrics. – 1967. – № 23. – P. 623-628.

12. Дюран Б. Кластерный аналіз / Б. Дюран, П. Оделл; пер. с англ. Е.З. Демиденко. – М. : Статистика, 1977. – 128 с.

13. Classification and Regression. Trees / [Breiman L., Friedman J., Olshen R., Stone C.] – CRC, Boca Raton, FL, 1984.

Надійшла до редколегії 8.06.2017

Рецензент: д-р техн. наук проф. О.Б. Леонтьєв, Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОДИКА ОПРЕДЕЛЕНИЯ СТРУКТУРЫ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МИНИСТЕРСТВА ОБОРОНЫ И ВООРУЖЕННЫХ СИЛ УКРАИНЫ

А.Н. Косогов, А.А. Сирык

В статье предложена методика обоснования рациональной структуры системы информационной безопасности Министерства обороны и Вооруженных Сил Украины на основе метода кластерного анализа, целью которого является поиск имеющихся структур, который выражается в образовании групп похожих между собой объектов-кластеров. В отличие от других методов, этот метод дает возможность классифицировать объекты не за одной, а за несколькими признаками одновременно как совокупность взаимосвязанных функциональных подсистем с определением функций каждой из них. Приведен вариант дендрограми объединение кластеров (структурных подразделений) за измерением близости функций и задач соответственно подсистемам системы.

Ключевые слова: *информационная безопасность, система информационной безопасности, структура, кластерной анализ, Министерство обороны, Вооруженные Силы Украины.*

METHODOLOGY FOR DETERMINING THE STRUCTURE OF THE INFORMATION SECURITY SYSTEM OF THE MINISTRY OF DEFENSE AND ARMED FORCES OF UKRAINE

O. Kosogov, A. Siryk

The article proposes a technique for substantiating the rational structure of the information security system of the Ministry of Defense and the Armed Forces of Ukraine on the basis of the cluster analysis method, whose goal is to search for existing structures, which is expressed in the formation of groups of similar clusters. Unlike other methods, this method makes it possible to classify objects not just one but several attributes simultaneously as a set of interrelated functional subsystems with the definition of the functions of each of them. A variant of dendrographs is given for the integration of clusters (structural units) for measuring the proximity of functions and tasks, respectively, to the subsystems of the system.

Keywords: *information security, information security system, structure, cluster analysis, the Ministry of Defense, the Armed Forces of Ukraine.*