ДОПОВІДІ
НАЦІОНАЛЬНОЇ
АКАДЕМІЇ НАУК
УКРАЇНИ

ІНФОРМАТИКА ТА КІБЕРНЕТИКА
INFORMATICS AND CYBERNETICS

https://doi.org/10.15407/dopovidi2023.01.016
УДК 004.047

А.Б. Качинський, https://orcid.org/0000-0001-9642-7006

Рада національної безпеки і оборони України, Київ
E-mail: akachynsky@gmail.com

Структурно-функціональна модель системи забезпечення інформаційної й інформаційно-психологічної безпеки

Представлено академіком НАН України С. І. Пирожковим

Розглядається структурно-функціональна модель системи забезпечення інформаційної й інформаційно-психологічної безпеки, заснованої на багатоешелонній ієрархічній моделі структури складної системи, запропонованої М. Месаровичем, як сукупності відносно незалежних, взаємодіючих між собою підсистем. При цьому деякі (або всі) підсистеми мають право ухвалення рішень, а їх ієрархічне розташування (багатоешелонна структура) визначається тим, що деякі з підсистем знаходяться під впливом або керуються вищими.

Ключові слова: *ієрархічна система, організація, інформаційна, інформаційно-психологічна безпека, багатоешелонна модель структури, інформаційні війни, інформаційна зброя.*

Нині інформація стала критично важливим ресурсом. Підвищення національної безпеки нашої держави потребує розробки як теоретичних основ так і практичних методів державної політики інформаційної безпеки. Це реалізується відповідними організаціями й інституціями держави, заснованими на результатах системних досліджень.

При цьому необхідно знайти компроміс між простотою опису структури системи забезпечення інформаційної й інформаційно-психологічної безпеки (СЗІпБ) S, що дозволить скласти і зберегти цілісні уявлення про неї і детальним описом процесу пропаганди, як форми комунікації. Вона відрізняється як різноманіттям типів елементів, так і різноманіттям типів відношень між ними.

Отже СЗІпБ можна розглядати як цілісний об'єкт, утворений із функціонально різнотипних підсистем, структурно пов'язаних ієрархічною підпорядкованістю і функціонально об'єднаних для досягнення заданих цілей за певних умов

$$S = < A, R, Z > ,$$

Цитування: Качинський А.Б. Структурно-функціональна модель системи забезпечення інформаційної й інформаційно-психологічної безпеки. *Допов. Нац. акад. наук Укр.* 2023. № 1. С. 16—23. https://doi.org/10.15407/dopovidi2023.01.016

де A — множина їх елементів; R — множина відношень між їхніми елементами; Z — множина цілей СЗІПпБ.

Для побудови моделі структури організації протидії дезінформації скористаємося методом структурно-функціонального підходу [1].

Множину властивостей СЗІПпБ зобразимо у вигляді впорядкованої структури класів:

$$B_0 = \{B_\nu \mid \nu = 1, 2, \ldots, m_0\}, \tag{1}$$

де B_0 — множина властивостей системи; B_ν — ν-й клас, який поєднує деяку категорію властивостей, що мають загальні прояви, у нашому випадку — клас цілей і функцій.

Кожний клас B_ν визначає сукупність властивостей як $b_{\nu i}$:

$$B_\nu = \{b_{\nu i} \mid i = 1, 2, \ldots, m_\nu\}. \tag{2}$$

До класу властивостей цілей $b_{\nu i}$ можна включити залежність формування цілей від часу і стадії пізнання об'єкта або процесу, залежність формування від внутрішніх і зовнішніх факторів, зведення задачі формування глобальної цілі до задачі її структурування. Клас функціональних властивостей — це управління, стійкість, адаптованість, керованість, ефективність тощо.

Кожну i-ту властивість $b_{\nu i}$ класу B_ν характеризує множина показників

$$Y_{\nu i} = \{y_{\nu ik} \mid k = 1, 2, \ldots, k_{\nu i}\}, \tag{3}$$

де $y_{\nu ik}$ — k-й показник i-ї властивості ν-го класу B_ν.

Враховуючи важливість показників і порогових значень для систем забезпечення безпеки [2], вимоги до властивостей ν-го класу визначає множина R_ν:

$$R_\nu = \{R_{\nu i} \mid i = 1, 2, \ldots, m_i\}, \tag{4}$$

де $R_{\nu i}$ — множина вимог до i-ї властивості класу B_ν, визначена співвідношенням

$$R_{\nu i} = \{r_{\nu ik} \mid k = 1, 2, \ldots, k_{\nu i}\}, \tag{5}$$

де $r_{\nu ik}$ — вимоги до k-го показника i-ї властивості класу B_ν.

Вимоги до показників зазвичай задають з урахуванням інтервалу допустимих значень або необхідного значення в одній із форм [3]:

$$r^-_{\nu ik} \leqslant r_{\nu ik} \leqslant r^+_{\nu ik}, \quad r_{\nu ik} = r^0_{\nu ik} \pm \Delta r_{\nu ik}, \quad r_{\nu ik} = r^0_{\nu ik}\,(1 \pm \delta r_{\nu ik}),$$

де $\Delta r_{\nu ik}$ — абсолютне значення допуску; $\delta r_{\nu ik}$ — відносне значення допуску, %.

Множина зовнішніх факторів визначає умови функціонування системи і характеризує умови діяльності СЗІПпБ S_e з урахуванням граничних і порогових значень показників безпеки

$$S_e = \{w_{je} \mid w^-_{je} \leqslant w_{je} \leqslant w^+_{je} \mid je = 1, 2, \ldots, Q_e\}, \tag{6}$$

де w_{je} — показник одного з чинників умов діяльності організації; w_{je}^{-}, w_{je}^{+} — відповідно граничні мінімальні і максимальні його значення.

Нехай структура СЗІПпБ відповідає наступній ієрархічній структурі ешелонів [4]: визначення глобальної цілі, декомпозиція цілей за критерієм "кінцевий інформаційний продукт", декомпозиція цілей за критерієм "простір ініціювання цілей", декомпозиція цілей за складом системи забезпечення інформаційної й інформаційно-психологічної безпеки.

Нехай кожен ешелон складається з множини V_q функціональних елементів:

$$V_q = \{V_{qp} \mid q = 1, 2, \ldots, Q,\ p = 1, 2, \ldots, P_0\}, \tag{7}$$

де V_{qp} — p-й функціональний елемент q-го ешелону; Q — загальна кількість ешелонів, $Q = 6$.

Кожний функціональний елемент СЗІПпБ характеризується вектором показників, що для елементів V_{qp} та V_q визначені співвідношенням

$$X_{qp} = \{x_{qpj} \mid j = 1, 2, \ldots, n_{xp}\}, \tag{8}$$

де x_{qpj} — j-й показник p-го функціонального елемента СЗІПпБ q-го ешелону; n_{xp} — загальна кількість показників.

Причому кожний функціональний елемент СЗІПпБ виконує деяку множину функцій, докладний опис яких буде наведено при описі моделі.

Множина функцій елементів V_{qp} та V_q описується виразом

$$\Phi_{qp} = \{f_{qpk} \mid k = 1, 2, \ldots, n_{qp}\}, \tag{9}$$

де f_{qpk} — k-та функція p-го функціонального елемента множини V_q.

Кожна функція залежить від вектора показників X_{qp}^{-}:

$$f_{qpk} = f_{qpk}(X_{qp}^{-}),$$

склад і вигляд функцій визначаються у процесі здійснення системного аналізу.

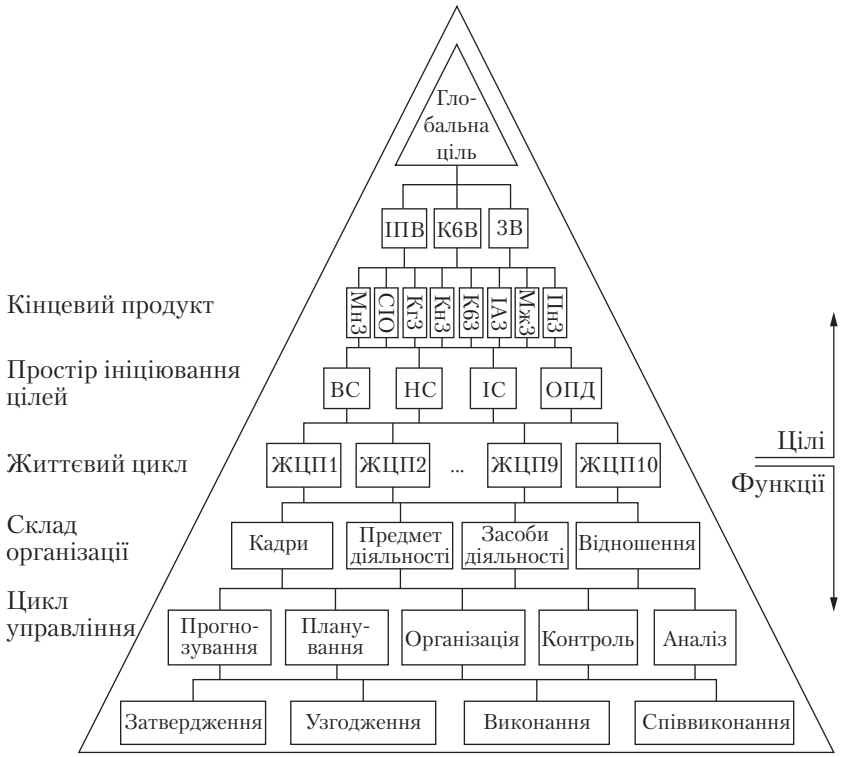
Кожний функціональний елемент впливає на загальні властивості системи. Їх ступінь впливу у загальному випадку описують у вигляді [1]

$$F : X \to Y, \tag{10}$$

де X — множина показників СЗІПпБ; Y — множина показників, які визначають її властивості; F — функціонал, що реалізує перетворення X на Y.

За допомогою структурно-функціонального аналізу можна формалізувати процес розробки математичної моделі СЗІПпБ. При цьому виникає проблема: необхідно знайти компроміс між простотою опису її структури, що дозволяє скласти і зберегти цілісні уявлення про неї, і детальним описом процесу пропаганди, як форми комунікації [5, 6]. Модель вирізняється як різноманіттям типів елементів, так і типів відношень між ними (див. рисунок).

Системний підхід є одним із способів вирішення даної проблеми, що розглядає складну систему як сукупність відносно незалежних, взаємодіючих між собою підсистем; при цьому деякі (або всі) підсистеми мають право ухвалення рішень, а їх ієрархічне розташування ви-



Структурна модель організації протидії дезінформації, що включає цілепокладання та її основні функції

значається тим, що деякі з підсистем знаходяться під впливом або керуються вищими [7]. Рівні такої ієрархії називаються ешелонами [8].

Ешелон 1. Визначення глобальної цілі.

Керівництво організації протидії дезінформації формує глобальну ціль (ГЦ), визначену вищим органом або утворену за допомогою аналізу директивних документів. Воно передає чіткі команди по всій структурі, а також ухвалює рішення для досягнення визначених цілей [9, 10].

Успіх контрпропагандистських кампаній залежить від діяльності сильного централізованого органу, з ієрархією, вбудованою в нього. Це пов'язано з тим [3], що формування і реалізація перетворення (10) — одна з головних цілей структурно-функціонального аналізу складної ієрархічної системи за групою вимог, заданих у формулах (4) — (6). Одначе, враховуючи, що пропаганда — це задумана як сукупність стратегічно розроблених повідомлень, що поширюються серед населення з метою провокації подій і відповідають інтересам їх джерела [11], побудувати функціонал для СЗІпБ вкрай важко.

Глобальна ціль має бути зорієнтована на кінцевий інформаційний продукт.

Ешелон 2. Декомпозиція цілей за критерієм "кінцевий інформаційний продукт".

Посилення інформаційної складової у глобальному протиборстві призводить до повноцінної інформаційної війни. Існує багато класифікацій інформаційних війн. Ми розглядаємо три їх основних види: інформаційно-психологічні війни, кібернетичні війни й інформаційні війни змішаного типу [12, 13].

Водночас новітні інформаційні технології, сучасні інформаційні й психологічні форми та способи впливу на особистість й суспільство породжують велику кількість різних видів інформаційної зброї.

Ми розглядаємо *ментальну зброю*, як зброю спрямовану на зміну ідентичності. В умовах сучасних інформаційних війн особливого значення набуває забезпечення безпеки національного культурного простору, його захист від ментальної зброї.

Спеціальні інформаційні операції — це інформаційна зброя, що використовує не тільки медійні засоби, але й можливості культури й мистецтва, а також психотропні й психотронні методи ураження свідомості, що небезпечніше, — заміщення свідомості.

До інформаційної зброї, спрямованої на ураження свідомості відноситься й *когнітивна зброя*, що здатна заражати масову свідомість когнітивними вірусами на кшталт мемів. Проникаючи у свідомість, "перепрограмовуючи" її, меми-віруси, подібно інформаційній пандемії, поширюються у масовій свідомості.

Контентна зброя — це зброя, що спрямована на зміну властивостей людського інтелекту. Головним її інструментом є зміст інформаційного повідомлення, вибудований спеціальним способом, і який може бути представлений у мультимедійному, текстовому або графічному форматі.

Кібернетична зброя — це зброя, що використовує комп'ютерні мережі для здійснення різних політично орієнтованих кібератак, і застосовується як окремими хакерами, терористичними групами, так і цілими державами. Тут особливу загрозу становлять віруси типу "логічних бомб" і "троянів".

Інформаційно-алгоритмічна зброя — це зброя, яка за допомогою психофізичних методів вражає мозок людини через візуальні образи кіберпростору, перетворює людей у провідників наперед заданих ідей-алгоритмів. Мета застосування даного виду зброї — корекція культурного коду.

Основу *мережевої зброї* становить сукупність дій, спрямованих на формування задуманої моделі поведінки як окремих людей, так і окремих груп спільноти в умовах миру, кризи чи війни. Здійснюється це за допомогою інформаційних технологій (від смартфона до Інтернету).

Поведінкова зброя — це нелетальний тип зброї, метою використання якої є зміна поведінки окремих груп людей або ворога загалом. Вона спрямована на створення спеціальних умов, коли людина віддає перевагу не самостійному ухваленню рішень, а автоматичному наслідуванню чужих звичок, стереотипів тощо.

Ешелон 3: *декомпозиція цілей за критерієм "простір ініціювання цілей"*. Цілепокладання на даному рівні здійснюється в залежності від змін, що відбуваються у зовнішньому інформаційному середовищі, і позначається на кінцевих інформаційних продуктах. Причому всі організовані системи (організації, відомства тощо), з якими взаємодіє система забезпечення інформаційної й інформаційно-психологічної безпеки діляться на чотири класи: вища система (ВС), що визначає головні вимоги до кінцевого інформаційного продукту; нижчі системи (НС), вимоги до яких визначають можливості підготовки якісних інформаційних продуктів, інформаційне середовище (ІС), організації протидії дезінформації (ОПД), яка ініціює власні підцілі, що відповідають стану захищеності держави від інформаційних й інформаційно-психологічних загроз.

Ешелон 4. Декомпозиція цілей за критерієм "простір ініціювання цілей". На даному рівні визначаються послідовні кроки отримання кінцевих інформаційних продуктів — від визначення джерела дезінформації до постановки конкретних завдань: визначення ідеології та мети (ЖЦП1); визначення контексту (ЖЦП2); визначення пропагандиста (ЖЦП3); дослідження структури пропагандистської організації (ЖЦП4); визначення цільової аудиторії (ЖЦП5); розуміння методів використання інструментів пропаганди (ЖЦП6); аналіз спеціальних методів для максимального впливу (ЖЦП7); аналіз реакції аудиторії (ЖЦП8); виявлення й аналіз контрпропаганди (ЖЦП9); завершення оцінки й завдання (ЖЦП10).

Ешелон 5. Декомпозиція цілей за складом системи забезпечення інформаційної й інформаційно-психологічної безпеки, у результаті якої формуються функції щодо вироблення основного інформаційного продукту. Вони випливають із потреб основних елементів організації протидії дезінформації і об'єднуються у три основні групи кадри (К), протидія дезінформації як предмет діяльності (ПД) і засоби діяльності (ЗД).

Ешелон 6. Декомпозиція цілей за критерієм "управлінський цикл". На даному рівні декомпозиції класифікатор включає наступні організаційні заходи системи забезпечення інформаційної й інформаційно-психологічної безпеки: прогнозування (Пр), планування (Пл), організацію (Ор), контроль (Ко) й аналіз результатів її діяльності (Ан). Усі ці заходи передбачають виконання наступних функцій організації протидії дезінформації: затвердження завдань й перевірку їх узгодженості, а також виконання та співвиконання цих завдань.

Вибір багатоешелонної моделі структури пропагандистської організації зумовлений також тим, що кожний рівень ієрархіє формує свої конкретні цілі і засоби їх досягнення. Крім того, для окремих завдань можуть бути як спеціальні цілі, так і засоби їх досягнення, що відповідає основній відмінній рисі багатоешелонної моделі: надання підсистемам усіх рівнів деякої свободи у виборі їх власних рішень. Ці рішення не завжди можуть збігатися з рішеннями вищого органу. Таким чином, надання підсистемам пропагандистської організації свободи дій при ухваленні рішень всім ешелонам ієрархічної структури підвищує ефективність її функціонування.

Висновки. На разі інформацію можна розглядати як критично важливий ресурс, який суттєво позначається на стані національної безпеки держави і потребує розробки як теоретичних засад, так і практичних заходів державної політики інформаційної безпеки. Ця політика реалізується відповідними організаціями й інституціями держави, заснованими на результатах системних досліджень.

Тут важливу роль відіграє структурно-функціональна модель організації, що враховує принципову особливість системного аналізу: розробку та використання засобів для формування й аналізу цілей і функцій організації з забезпечення інформаційної й інформаційно-психологічної безпеки. Такий підхід дає можливість розробити формалізовану модель організації з інформаційного протиборства, визначити її основні цілі і функції, забезпечити цілісність й адаптацію щодо змін, які відбуваються в оточуючому середовищі.

Система забезпечення інформаційної й інформаційно-психологічної безпеки, заснована на структурно-функціональній моделі, — це цілеспрямована система, яка може сприймати виклики, внутрішні і зовнішні загрози та формувати цілі, адекватні інформаційній

безпеці держави, а також ефективно протидіяти деструктивним інформаційним впливам і пропаганді. При чому керівництво організації може змінювати функції, властивості і навіть структуру як функціональних елементів, так і системи загалом, здійснюючи при цьому доцільний вибір альтернативних дій щодо досягнення цілей за наявних умов.

Автор висловлює щиру вдячність акад. НАН України В.П. Горбуліну і чл.-кор. НАН України Н.Д. Панкратовій за консультації і поради під час підготовки даної публікації.

ЦИТОВАНА ЛІТЕРАТУРА

1. Згуровский М.З., Панкратова Н.Д. Системный анализ: проблемы, методология, приложения. Киев: Наук. думка, 2005. 744 с.
2. Качинський А.Б. Індикатори національної безпеки: визначення та застосування їх граничних значень. Київ: НІСД, 2013. 104 с.
3. Згуровский М.З., Панкратова Н.Д. Основи системного аналізу. Київ: Вид. группа BHV, 2007. 544 с.
4. Ильичев А.В. Начала системной безопасности. Москва: Науч. мир, 2003. 456 с.
5. Джоуэт Г., О'Доннел В. Пропаганда и убеждение. Пер. с англ. О.И. Ткаченко. Харьков: "Гумманитарный центр", 2021. 496 с.
6. Лайнбарджер П.М.Э. Психологическая война. Теория и практика обработки массового сознания. Пер. с англ. Е.В. Ламановой. Москва: ЗАО Центрполиграф, 2013. 445 с.
7. Волкова В., Денисов А. Теория систем. Москва: Высш. шк., 2006. 511 с.
8. Мессарович М. Теория иерархических многоуровневых систем. Москва: Мир, 1973. 344 с.
9. Уєбстер Ф. Теория информационного общества. Москва: Аспект Пресс, 2004. 398 с.
10. Бухарин С.Н., Цыганов В.В. Методы и технологии информационных войн. Москва: Академ. Проект, 2007. 382 с.
11. Грант Дж. Не верю. Как увидеть правду в море дезинформации. 12 уроков здорового скепсиса. Пер. с англ. Е. Бакушева. Москва: Альпина Паблишер, 2017. 296 с.
12. Патрикаракос Д. Війна у 140 знаках. Як соціальні медіа змінюють військовий конфлікт XXI століття. Київ: Yakaboo, 2019. 352 с.
13. Сінгер П., Бруклін Е. Війна лайків. Зброя в руках соціальних мереж. Харків: Книжковий клуб "Клуб сімейного дозвілля", 2019. 319 с.

Надійшло до редакції 02.09.2022

REFERENCES

1. Zgurovsky, M. Z. & Pankratova, N. D. (2005). System analysis: problems, methodology, applications. Kyiv: Naukova Dumka (in Russian).
2. Kachynsky, A. B. (2013). Indicators of national security: definition and application of their limit values. Kyiv: NISD (in Ukrainian).
3. Zgurovsky, M. Z. & Pankratova, N. D. (2007). Fundamentals of system analysis. Kyiv: BHV Publishing Group (in Ukrainian).
4. Ilyichev, A. V. (2003). Beginning of system security. Moscow: Nauchny mir (in Russian).
5. Jowett, G. & O'Donnell, V. (2021). Propaganda and persuasion Trans. with English O. I. Tkachenko. Kharkiv: "Humanitarian Center" (in Russian).
6. Linebarger, P. M. E. (2013). Psychological warfare. Theory and practice of processing mass consciousness Trans. with English E. V. Lamanova. Moscow: ZAO Tsentrpoligraf (in Russian).
7. Volkova, V. & Denisov ,A. (2006). Theory of systems. Moscow: Higher School (in Russian).
8. Messarovych, M. (1973). Theory of hierarchical multilevel systems. Moscow: Mir (in Russian).
9. Uyebster, F. (2004). Theory of information society. Moscow: Aspect Press (in Russian).
10. Bukharin, S. N. & Tsyganov, V. V. (2007). Methods and technologies of information wars. Moscow: Academic Project (in Russian).

11. Grant, J. I (2017). Do not believe. How to see the truth in a sea of disinformation. 12 lessons healthy skepticism. Trans. with English E. Bakushev. Moscow: Alpina Publisher (in Russian).
12. Patrikarakos, D. (2019). War in 140 signs. How social media is changing military conflict of the 21st century. Kyiv: Yakaboo (in Ukrainian).
13. Singer, P. & Brooklyn, E. (2019). War of likes. Weapons in the hands of social networks. Kharkiv: Book Club "Family Leisure Club" (in Ukrainian).

Received 02.09.2022

A.B. Kaczynski, https://orcid.org/0000-0001-9642-7006

National Security and Defense Council of Ukraine, Kyiv

E-mail: akachynsky@gmail.com

STRUCTURAL AND FUNCTIONAL MODEL OF THE SYSTEM OF PROVIDING INFORMATION AND INFORMATION-PSYCHOLOGICAL SECURITY

The article considers the structural-functional model of the system of providing information and information-psychological security based on the multi-echelon hierarchical model of the structure of the complex system, proposed by M. Mesarovic as a set of relatively independent interacting subsystems; while some (or all) subsystems have decision-making power, and their hierarchical location (multi-echelon structure) is determined by the fact that some of the subsystems are influenced or controlled by the higher.

Keywords: *hierarchical system, organization, information, information-psychological security, multi-echelon hierarchical model, information warfare, information weapon.*