

УДК 004.056:061.68

**ОБГРУНТУВАННЯ ПОКАЗНИКА ЯКОСТІ ФУНКЦІОНУВАННЯ
КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ**

*Сташевський З. П., Грицюк Ю. І., д-р техн. наук, професор
Львівський ДУ БЖД, Львів, Україна*

**RATIONALE FOR INDICATOR QUALITY OF INTEGRATED INFORMATION
SECURITY SYSTEM**

*Stashevskiy Z. P., Gricyuk Yu. I., Doctor of Engineering, Professor
Lviv DU BC, Lviv, Ukraine*

Вступ

У статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [1] зазначено: «Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, має оброблятися в системі із застосуванням комплексної системи захисту інформації (КСЗІ)». Наявність конфіденційної та таємної інформації змушує структурні підрозділи Державної служби України з надзвичайних ситуацій (ДСНС України) розробляти та впроваджувати КСЗІ та постійно стежити за її якісною роботою. Для вирішення одного з цих завдань необхідно передусім обґрунтувати математично показник якості функціонування КСЗІ в структурних підрозділах рятувальної служби.

Відповідно до законодавчої та нормативної бази, що регулює діяльність служби порятунку, основна увага посадових осіб акцентується на характері інформації, яка надходить про НС та заходи, які мають бути спрямовані на рятування життя і збереження здоров'я людей, зниження масштабів заподіяння шкоди природному середовищу і скорочення матеріальних збитків. При цьому особливого значення набуває завдання підвищення якості управління силами і засобами ДСНС України шляхом інтеграції інформаційних систем (ІС) управління [2].

Сучасні ІС, які експлуатуються у структурних підрозділах ДСНС України, застосовують інформаційні технології, які містять методи розрахунку найкоротшого шляху до місця виникнення НС, оптимального розташування пожежних депо, кількість підрозділів та чисельність особового складу, які потрібно задіяти у ліквідації НС залежно від її класифікації, застосування системи GPS та навігаційних карт тощо. Актуальними прикладами є розроблені інформаційні системи для диспетчерської служби екстреної допомоги «112», системи оперативно диспетчерської служби (СОДУ). В ін-

формаційних моделях таких систем враховуються різновиди НС; шкідливі речовини, які можуть знаходитись на тому чи іншому об'єкті; параметри пожежі, а також чинники, що впливають на її розвиток; відомості щодо маршруту руху рятувальних підрозділів: напрямки та інтенсивність руху автомобілів на вулицях, перехрестя, світлофори, розміщення вододжерел тощо. Тому будь-яке пошкодження зловмисником ІС може призвести до загибелі людей, матеріальних втрат та забруднення навколишнього середовища.

Ефективна робота КСЗІ в ІС ДСНС України полягає в тому, що вона має унеможливити спотворення інформації, яка надходить, втрату секретної інформації, та забезпечувати збереження державної таємниці. Проте на сьогодні виникає проблема в постановці задачі синтезу ефективних засобів захисту інформації в ІС державної служби. Для розв'язання такої задачі необхідно передусім сформулювати показник якості функціонування КСЗІ в структурних підрозділах ДСНС України.

Мета роботи: провести обґрунтування показника якості КСЗІ в структурних підрозділах ДСНС України як одного із методів розв'язання задачі синтезу ефективних засобів захисту ІС.

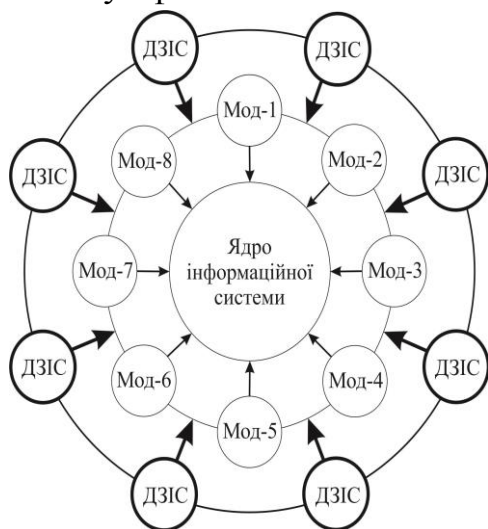


Рис. 1. Узагальнена модель процесу захисту інформації в структурних підрозділах ДСНС України

За визначенням, комплексна система захисту інформації – це взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [3]. У найзагальнішому вигляді модель процесу захисту інформації в ІС структурних підрозділів ДСНС України складається з таких елементів (рис.1): ядро інформаційної системи, модель розподілу інформаційних ресурсів (Мод-1), модель використання інформаційних ресурсів (Мод-2), модель впливу зовнішнього середовища (Мод-3), модель визначення значень керованих параметрів (Мод-4), модель некерованих значень, але таких, що піддаються дії параметрів ІС (Мод-5), модель розподілу засобів поточного управління (Мод-6), модель розподілу засобів дії (Мод-7), модель еволюційного розвитку системи захисту інформації (Мод-8), джерела загроз інформаційній системі (ДЗІС).

Відомо, що інформаційна система (ІС) будь-якого структурного підрозділу може піддаватися різним загрозам, кількість яких нехай буде обмеженою $\tilde{Z}^{dz} = f(\tilde{P}^{zag}, \Delta\tilde{Q}^{zag})$, де: $\tilde{P}^{zag} = \{p_i^{zag}, i = \overline{1, m}\}$ – ймовірністю появи i -ої за-

грози; $\Delta\tilde{Q}^{zag} = \{\Delta q_i^{zag}, i = \overline{1, m}\}$ — обсяг збитку ІС, який наноситься i -ою загрозою. КСЗІ виконує функцію повної або часткової ліквідації загроз для ІС. Основною характеристикою КСЗІ є ймовірність усунення дії i -ої загрози з наявної множини $\tilde{P}^{усун} = \{p_i^{усун}, i = \overline{1, m}\}$. За рахунок функціонування КСЗІ забезпечується зменшення збитку, що наноситься ІС під впливом джерел загроз.

Постановка задачі синтезу системи захисту інформації в ІС має такий вигляд: необхідно вибрати такий варіант реалізації КСЗІ, яка забезпечить максимальне попередження збитку, що може виникнути під впливом різних загроз, при обмежених витратах на її функціонування. Формальна постановка задачі має такий вигляд:

$$\text{знайти } \tilde{T}^0 = \arg \tilde{W}(\tilde{T}) \rightarrow \max : \tilde{T}^0 \in \tilde{T}^+, \text{ при обмеженні } C(\tilde{T}^0) \leq C^{дон}, \quad (1)$$

де: $\tilde{W} = \{\omega_i, i = \overline{1, m}\}$ — попереджений збиток за рахунок ліквідації дії i -ої загрози; $\tilde{T} = \{t_j, j = \overline{1, n}\}$ — множина параметрів технічної реалізації КСЗІ; $\tilde{T}^+ = \{t_j^+, j = \overline{1, n}\}$, $\tilde{T}^0 = \{t_j^0, j = \overline{1, n}\}$ — множина допустимих і оптимальних значень параметрів технічної реалізації КСЗІ; $C^{дон}$ — сума допустимих витрат на функціонування КСЗІ [4].

Для розв'язання цієї задачі необхідно насамперед сформулювати показник якості функціонування КСЗІ, тобто $\tilde{W}(\tilde{T})$. Очевидно, попереджений збиток у загальному вигляді виражатиметься таким співвідношенням:

$$\tilde{W} = F(\tilde{P}^{zag}, \Delta\tilde{Q}^{zag}, \tilde{P}^{усун}) \rightarrow F(p_i^{zag}, \Delta q_i^{zag}, p_i^{усун}, i = \overline{1, m}). \quad (2)$$

Попереджений збиток за рахунок ліквідації дії i -ої загрози:

$$\tilde{W} = \left\{ \omega_i = p_i^{zag} \cdot \Delta q_i^{zag} \cdot p_i^{усун}, i = \overline{1, m} \right\}. \quad (3)$$

За умови незалежності загроз і адитивності їх наслідків отримуємо такий вираз для обчислення ΣW — загального попередженого збитку ІС

$$\Sigma W = \sum_{i=1}^n \omega_i = \sum_{i=1}^m p_i^{zag} \cdot \Delta q_i^{zag} \cdot p_i^{усун}. \quad (4)$$

Ймовірність появи i -ої загрози (p_i^{zag}) визначається статистично і відповідає відносній частоті її появи:

$$\tilde{P}^{zag} = \left\{ p_i^{zag} = \lambda_i / \sum_{j=1}^m \lambda_j = \lambda'_i, i = \overline{1, m} \right\}, \quad (5)$$

де: λ_i — частота появи i -ої загрози; λ'_i — нормоване значення частоти появи i -ої загрози.

Збиток (Δq_i^{zag}), що виникає від впливу i -ої загрози, може визначатися в абсолютних одиницях: фінансових чи матеріальних втратах на відновлення КСЗІ, тимчасових витратах, обсязі знищеної або "зіпсованої" інформації і т.д. Проте, практично це зробити дуже складно, особливо на ранніх етапах функціонування КСЗІ. Тому доцільно замість абсолютного збитку викори-

стовувати відносний збиток, який, по суті, є ступенем небезпеки i -ої загрози для ІС. Ступінь небезпеки здебільшого визначається експертами в припущенні, що усі загрози для ІС становлять повну групу подій [2], тобто:

$$0 \leq \Delta Q^{zaz} \leq 1 \rightarrow \left\{ 0 \leq \Delta q_i^{zaz} \leq 1, i = \overline{1, m} \right\}; \sum_{i=1}^m \Delta q_i^{zaz} = 1.$$

Найбільш складним питанням є визначення ймовірності усунення i -ої загрози $p_i^{усун}$ при функціонуванні КСЗІ. Зробимо звичайне припущення, що ця ймовірність визначається тим, наскільки повно враховані кількісні і якісні вимоги до КСЗІ при її проектуванні, тобто:

$$\tilde{P}^{усун} = \left\{ p_i^{усун} = f_i(\tilde{X}_i), i = \overline{1, m} \right\}, \quad (6)$$

де $\tilde{X} = \left\{ \tilde{X}_i = \{x_{ij}, j = \overline{1, n}\}, i = \overline{1, m} \right\}$ — ступінь виконання j -ої вимоги до КСЗІ при усунення i -ої загрози.

Нехай перші " k " вимог будуть кількісними ($j = \overline{1, k}$) інші $j = \overline{k+1, n}$ — якісними вимогами. Ступінь виконання j -ої кількісної вимоги визначається її наближенням до потрібного (оптимального) значення. Для оцінювання ступеня виконання j -ої кількісної вимоги до КСЗІ найзручніше використовувати її нормоване значення:

$$\tilde{X}' = \left\{ \tilde{X}'_i = \left\{ x'_{ij} = \frac{x_{ij} - x_{ij}^{H2}}{x_{ij}^{HK} - x_{ij}^{H2}}, j = \overline{1, k} \right\}, i = \overline{1, m} : 0 \leq x'_{ij} < 1 \right\}, \quad (7)$$

де: x'_{ij} — нормоване значення j -ої вимоги до КСЗІ для усунення i -ої загрози, визначається за [4]; x_{ij}^{HK} , x_{ij}^{H2} — найкраще і найгірше значення.

З урахуванням формули (7) отримаємо такі співвідношення:

при $x_{ij}^{HK} = x_{ij}^{\max}; x_{ij}^{H2} = x_{ij}^{\min}$, $\tilde{X}' = \left\{ \tilde{X}'_i = \left\{ x'_{ij} = \frac{x_{ij} - x_{ij}^{\min}}{x_{ij}^{\max} - x_{ij}^{\min}}, j = \overline{1, k} \right\}, i = \overline{1, m} \right\}, \quad (8)$

при $x_{ij}^{HK} = x_{ij}^{\min}; x_{ij}^{H2} = x_{ij}^{\max}$, $\tilde{X}' = \left\{ \tilde{X}'_i = \left\{ x'_{ij} = \frac{x_{ij}^{\max} - x_{ij}}{x_{ij}^{\max} - x_{ij}^{\min}}, j = \overline{1, k} \right\}, i = \overline{1, m} \right\}, \quad (9)$

$$x'_{ij} = \begin{cases} 0, & \text{якщо } x_{ij} < x_{ij}^{\min}; x_{ij} > x_{ij}^{\max}; \\ 1, & \text{якщо } x_{ij} = x_{ij}^{opt}; \\ \frac{x_{ij} - x_{ij}^{\min}}{x_{ij}^{opt} - x_{ij}^{\min}}, & \text{якщо } x_{ij}^{\min} \leq x_{ij} \leq x_{ij}^{opt}; \\ \frac{x_{ij}^{\max} - x_{ij}}{x_{ij}^{\max} - x_{ij}^{opt}}, & \text{якщо } x_{ij}^{opt} \leq x_{ij} \leq x_{ij}^{\max}. \end{cases}$$

Ступінь виконання якісної вимоги визначається функцією належності до найкращого значення $\mu(x_{ij})$.

Розклавши функцію (6) в ряд Маклорена і обмежившись тільки першими членами ряду, отримаємо

$$\tilde{P}^{усун} = \left\{ p_i^{усун} = p_i^{усун}(0) + \sum_{j=k+1}^n \frac{\partial p_i^{усун}}{\partial x_{ij}} \cdot x_{ij} + \sum_{j=k+1}^n \frac{\partial^2 p_i^{усун}}{\partial x_{ij}^2} \cdot x_{ij}^2 + \dots, i = \overline{1, m} \right\}, \quad (10)$$

де: $p_i^{усун}(0) = 0$ — ймовірність усунення i -ої загрози при не виконанні вимог до КСЗІ; $\frac{\partial p_i^{усун}}{\partial x_{ij}} = \alpha_{ij}$ — величина, яка характеризує ступінь впливу j -ої вимоги на ймовірність усунення i -ої загрози (важливість виконання j -ої вимоги для усунення i -ої загрози). Очевидно, що $0 \leq \alpha_{ij} \leq 1$; $\sum_{j=k+1}^n \alpha_{ij} = 1, i = \overline{1, m}$.

Після підстановки в (10) відповідних значень отримаємо:

$$\tilde{P}^{усун} = \left\{ p_i^{усун} = \sum_{j=1}^k \alpha_{ij} \cdot x'_{ij} + \sum_{j=k+1}^n \alpha_{ij} \cdot \mu(x_{ij}), i = \overline{1, m} \right\}. \quad (11)$$

Остаточно формула (5) для оцінювання загальної величини ΣW попередженого збитку набуває такого вигляду:

$$\Sigma W = \sum_{i=1}^m \lambda'_i \cdot \Delta q_i^{заг} \left(\sum_{j=1}^k \alpha_{ij} \cdot x'_{ij} + \sum_{j=k+1}^n \alpha_{ij} \cdot \mu(x_{ij}) \right). \quad (12)$$

Таким чином, задача синтезу КСЗІ у вигляді (1) зводиться до оптимального обґрунтування кількісних і якісних вимог до КСЗІ при допустимих витратах на її функціонування, тобто набуває такого вигляду:

знайти
$$\tilde{W}(\tilde{X}') \rightarrow \max, \text{ при обмеженні } C(\tilde{X}') \leq C^{дон}. \quad (13)$$

Згідно з формулюванням задачі (13), основні етапи її розв'язання є:

- збирання та оброблення експертної інформації про характеристики джерела загроз: частоту появи i -ої загрози λ'_i і збитку $\Delta q_i^{заг}, i = \overline{1, m}$;
- збирання та оброблення експертної інформації для визначення важливості виконання j -ої якісної вимоги до КСЗІ при усуненні i -ої загрози α_{ij} і функції належності $\mu(x_{ij}), j = \overline{1, n}; i = \overline{1, m}$;
- оцінювання вартості КСЗІ для конкретного варіанту її реалізації залежно від ступеня виконання вимог $C(x'_{ij}, j = \overline{1, n}; i = \overline{1, m})$;
- розроблення математичної моделі та алгоритму вибору раціонального варіанту побудови КСЗІ (раціонального завдання щодо вимог) відповідно до постановки (15) як задачі нечіткого математичного програмування.

За відсутності інформації про джерела загроз ІС, для розв'язання задачі (13) можна використати показник такого вигляду:

$$\Sigma W = \sum_{i=1}^m \left(\sum_{i=1}^k \alpha_{ij} \cdot x'_{ij} + \sum_{j=k+1}^n \alpha_{ij} \cdot \mu(x_{ij}) \right). \quad (14)$$

Отже, ефективний захист інформації є одним з найголовніших аспектів при побудові надійної ІС будь-яких структурних підрозділів ДСНС України. Наведена математична модель функціонування КСЗІ в ІС структурного підрозділу рятувальної служби дає змогу вибору такого її варіанта реалізації, який може забезпечити максимум попередженого збитку, отриманого внаслідок дії джерела загроз при доступних витратах на цю систему. Це забезпечить безперебійне і вчасне реагування рятувальної служби ДСНС України на будь-які надзвичайні ситуації.

Висновки

Проведено обґрунтування показника якості функціонування КСЗІ в ІС структурних підрозділів ДСНС України та визначено основні етапи розв'язання задачі синтезу ефективних засобів захисту.

Література

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 р., № 80/94, редакція від 30.04.2009 р. [Електронний ресурс]. — Режим доступу: <http://zakon4.rada.gov.ua/laws/show/80/94-вр>
2. Сташевський З. П. Особливості проблеми синтезу систем захисту інформації у структурних підрозділах МНС України / З. П. Сташевський, Ю. І. Грицюк // Науковий вісник НЛТУ України. — 2012. — Вип. 22.10. — С. 79—96.
3. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новіков. — К. : Вид. група BHV, 2009. — 608 с.
4. Анохин А. М. Методы определения коэффициентов важности критериев / А. М. Анохин, В. А. Глотов, В. В. Павельев, А. М. Черкашин // Автоматика и телемеханика. — 1997. — №8. — С. 3—35.
5. Wei T. H. The algebraic foundations of ranking theory, Ph.D. Thesis, Cambridge Univ., 1952.

References

1. Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh" [The Law of Ukraine "Data Protection in the information and telecommunication systems"]. Available at: <http://zakon4.rada.gov.ua/laws/show/80/94-вр> (Accessed 01 Dec 2013)
2. Stashevsky Z.P., Grycyuk Yu.I. (2012) Features of problem of synthesis of systems security of information are in structural subdivisions of ministry of emergency measures of Ukraine. *Naukoviy visnik NLTU Ukrainy*. Vol. 22, No.10. pp. 79–96.
3. Haivoronskyi M.V., Novikov O.M. (2009) Bezpeka informatsiino-komunikatsiinykh system [Security Information and Communication Systems]. Kyiv, BHV Publ., 608 p.
4. Anokhin A.M., Glotov V.A., Paveljev V.V. and Cherkashin A.M. (1997) Metody opredeleniya koeffitsientov vazhnosti kriteriev [Methods for determining the coefficients of the importance of criteria]. *Avtomatika i telemekhanika*. №8, pp. 3–35.
5. Wei T.H. (1952) The algebraic foundations of ranking theory, Ph.D. Thesis, Cambridge Univ.

Сташевський З. П., Грицюк Ю. І. Показник якості функціонування комплексної системи захисту інформації. Проведено обґрунтування показника якості функціонування комплексної системи захисту інформації в ІС структурних підрозділів Державної служби України з надзвичайних ситуацій. Встановлено основні параметри, які впливають на якіс-

ну роботу КСЗІ, визначають її вартість при проектуванні та дають змогу вибору такого її варіанту реалізації, який найкраще забезпечить безперебійну роботу ІС рятувальної служби.

Ключові слова: інформаційна система, комплексна система захисту інформації (КСЗІ), показник якості функціонування, інформаційна загроза.

Сташевский З. П., Грицюк Ю. И. Показатель качества функционирования комплексной системы защиты информации. Проведено обоснование показателя качества функционирования комплексной системы защиты информации в ИС структурных подразделений Государственной службы Украины по чрезвычайным ситуациям. Установлены основные параметры, влияющие на качественную работу КСЗІ, которые определяют ее стоимость при проектировании и позволяют сделать выбор такого ее варианта реализации, который лучшим образом обеспечит бесперебойную работу ИС спасательной службы.

Ключевые слова: информационная система, комплексная система защиты информации (КСЗІ), показатель качества функционирования, информационная угроза.

Stashevskiy Z. P., Gricyuk Yu. I. Rationale for indicator quality of integrated information security system. The justification of functional quality index of the informational security system in Government service structural departments of emergency situations of Ukraine is carried out. Basic parameters which can influence on qualitative work of SSI are determined. These parameters assess the cost of its projecting and allow making such its variant of realization which will be better for constant functioning of is of rescue service.

Keywords: informative system, complex system of informational security (SIS), index of functional quality, informational menace.