УДК 621.384 **С.В. Толюпа, Ю.Я. Самохвалов, Н.В. Цьопа**

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ СПЕЦІАЛЬНИХ ОБ'ЄКТІВ ТА МЕТОДИКА ЇХ ОЦІНКИ

В статті показано, що структура оцінки рівня захищеності інформації на спеціальних об'єктах повинна ґрунтуватися на відповідній ієрархічній сукупності показників, яка складається з ряду окремих показників різного рівня та інтегрального загального критерію – рівня, який характеризує ступінь виконання функціонування комплексних систем захисту інформації власної цільової функції. Для оцінки систем захисту інформації запропоновано підхід, який ґрунтується на використанні принципів і правил системного аналізу, експертно-аналітичного методу вирішення складних слабоструктурованих завдань та теорії нечітких мір. Також показано, що реальною альтернативою та доповненням до базових методів оцінки рівня захисту інформації комплексних систем захисту інформації є застосування у дослідженнях Fuzzy-технологій, які дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різнорідності.

Ключові слова: комплексна система захисту інформації, теорія нечітких мір, нечітка логіка, об'єкт інформаційної діяльності, показник якості, методика оцінки.

Світова економічна криза призвела до загострення конкурентної боротьби на світових ринках. В умовах глобалізації та наростаючої конкурентної боротьби комплексні системи захисту інформації (КСЗІ) як в комерційних організаціях так і в державних підприємствах та корпораціях України є досить пріоритетним питанням інформаційної безпеки держави. Все частіше виникає потреба створення надійного захисту та збереження інформаційних ресурсів, як на рівні всієї організації взагалі так і на рівні окремих її підрозділів. І часто в тому наскільки ефективним є КСЗІ залежить загальна конкурентоздатність всієї організації. Підвищення вимог до ефективності захисту інформації (СЗІ) супроводжується підвищенням вимог щодо ефективності використання фінансових ресурсів, що виділяються на захист інформації (ЗІ).

На теперішній час, найбільше розповсюдження отримали два підходи до визначення оптимального варіанту побудови КСЗІ організацій. Перший з них ґрунтується на перевірці відповідності рівня захищеності інформації в організації вимогам одного зі стандартів (законодавчих актів) у галузі інформаційної безпеки. Основний недолік першого підходу полягає в тому, що коли рівень захищеності інформації чітко не визначений визначити найбільш ефективний варіант побудови КСЗІ організації достатньо складно. Другий підхід пов'язаний з використанням методів та моделей оптимізації складних систем для визначення оптимального варіанту побудови КСЗІ. У зв'язку з цим розробка відповідних методів та моделей оптимізації показників СЗІ отримує особливу актуальність.

Кінцевою метою при оптимізації показників КСЗІ є забезпечення необхідного рівня інформаційної безпеки організації за різних умов конкурентної боротьби. Завдання ускладнюється тим, що пошук доводиться вести в умовах невизначеності, коли дії суперника нам не відомі і, в кращому разі, можуть бути оцінені з певною долею ймовірності. При відсутності статистичних даних, що характерно для комерційних структур, вибір параметрів розрахунку і функціональних залежностей, які входять в математичну модель, ведеться на основі експертних оцінок і вимагає розробки відповідних методів та методик.

Рішення зазначених задач потребує включення до складу процедур спеціальних оптимізаційних моделей котрі встановлюють залежність між показниками кінцевого ефекту функціонування системи і сукупністю її параметрів. Саме такий підхід може бути покладено в основу оптимізації систем захисту інформації в умовах інформаційного протиборства. Таким чином, задача побудови оптимальної комплексної системи захисту інформації може бути вирішена на основі теоретичного (системного) підходу котрий використовує усесторонній розгляд та врахування основних факторів які впливають на ефективність системи. Під дослідженням операцій розуміють застосування математичних кількісних методів для обґрунтування рішень у всіх областях цілеспрямованої людської діяльності [1].

При дослідженні операцій ключову роль відіграє математична модель - умовний образ деякої системи інформаційної безпеки, який з допомогою математичних методів відображає властивості об'єктів, їх взаємозв'язків і процесів, котрі виникають при їх взаємодії. При цьому важливо дотримуватись також системного підходу, який в задачах оптимізації показників систем інформаційної безпеки проявляється в тому, що система „напад-захист" розглядається у взаємодії (протидії) її складових з врахуванням їх параметрів і характеристик. Оптимізація показників ведеться в двох напрямках - відносно загальної вартості ресурсів захисту (порівняно за вартістю інформації) і відносно розподілу цих ресурсів захисту між об'єктами, котрі відрізняються вразливістю, кількістю інформації, імовірністю нападу.

Вирішення цих питань, що досягається на основі математичної моделі, являє собою доволі складну задачу, обумовлену складністю встановлення функціональної залежності між показниками системи та її параметрами і характеристиками, а також відсутність усталеної методики розрахунку цих величин. Цільова функція може включати декілька показників - таких, як частка втраченої інформації, прибуток від інвестиції в захист інформації, їх рентабельність. Пошук вирішення ускладнюється тим, що протистояння в інформаційній сфері ведеться в умовах невизначеності, коли дії суперника невідомі і можуть бути передбачені лише з певною імовірністю на основі статистичних даних або з допомогою експертної оцінки. Таким чином, оптимізація показників складних багато рубіжних систем, якими є сучасні системи захисту інформації, є водночас важливою і складною задачею вирішення якої можливе лише шляхом розробки математичних моделей на основі системного підходу та методів дослідження операцій.

Реальною альтернативою та доповненням до базових методів оцінки рівня захисту інформації комплексних систем захисту інформації (КСЗІ) є застосування у дослідженнях Fuzzy-технологій, які дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різнорідності. Вони уможливлюють аналіз значної кількості якісної інформації, отриманої від експертів та доповненої кількісними даними. Fuzzy-технології є сукупністю теоретичних основ, методів, алгоритмів, процедур і програмних засобів, що базуються на використанні теорії нечітких мір (ТНМ) і оцінок експертів для вирішення широкого класу задач з самих різних областей [2,3]. Теорія нечітких мір, нечіткої логіки або *Fuzzy Logic* – новий підхід до опису процесів, в яких присутня невизначеність, що ускладнює і навіть виключає вживання точних кількісних методів і підходів. Основна відзнака методу – введення лінгвістичних змінних (суб'єктивних категорій) і методів їх обробки. Ця теорія може виступати як інструмент моделювання невизначеності, який базується на відомій розумовій здатності людини оперувати якісними категоріями і оформляти свої логічні висновки також в якісній формі.

Застосування даної технології підвищує достовірність і якість рішень, що приймаються, при суттєвому зниженні вимоги до вхідних даних (їх якості, кількості, достовірності), формалізація яких виконується настільки точно, наскільки дозволяє їх обсяг і якість. Розроблені моделі і методи вирішення задач нечіткого математичного програмування, які адекватні сучасним умовам функціонування спеціальних об'єктів інформаційної діяльносі (СОІД), дозволяють підвищити наукову обгрунтованість, ефективність рішення, що формулюється та приймається при нечіткій вхідній інформації, збільшують аналітичну базу, надають можливість формалізації різних параметрів задачі та різноманітних цільових установок.

Необхідно відзначити, що нечіткі числа багато в чому аналогічні розподілам теорії імовірності, але вільні від властивих останнім недоліків, а нечіткі описи є моделлю згортки окремих сценаріїв розвитку подій з одночасним зважуванням цих сценаріїв за рівнем можливості (аналогічну функцію виконує і щільність імовірнісного розподілу).

Крім того, існує ще декілька причин використання ТНМ. По-перше, нечіткі множини ідеально описують суб'єктну активність посадової особи, що приймає рішення щодо введення КСЗІ в експлуатацію. По-друге, нечіткі числа ідеально підходять для планування

факторів у часі, коли їх майбутня оцінка ускладнена (розмита, не має достатніх імовірнісних умов). Таким чином, всі сценарії за тими чи іншими окремими факторами можуть бути зведені в один сценарій у формі трикутного числа, де відокремлюють три позиції: мінімально можливе, найбільш очікуване та максимально можливе значення фактору. Причому ваги окремих сценаріїв у структурі зведеного сценарію формалізуються як трикутна функція приналежності рівня фактора нечіткій множині "приблизного рівняння середньому". По-третє, при використанні нечітких множин ми можемо в межах однієї моделі формалізувати особливості застосування СОІД [4].

Жоден окремо вибраний засіб захисту інформації не може захистити від різноманіття існуючих загроз безпеці, а проста комбінація різноманітних засобів захисту призводить до зниження рівня захисту в цілому із-за можливої конфліктності розрізнених засобів захисту. Тому останнім часом намітилася тенденція до побудови складних комплексних систем інформаційної безпеки. Ефективність КСЗІ можна охарактеризувати як здатність системи протистояти несанкціонованим діям порушника в рамках проектної загрози. Існують якісні і кількісні методи аналізу ефективності КСЗІ.

У багатьох випадках якісних оцінок не досить, щоб відповісти на питання, наскільки надійний захист інформації. Найбільш точніші кількісні методи. Проте для того, щоб "зміряти" ефективність, необхідно мати обґрунтований критерій (показник оцінки ефективності КСЗІ).

Ефективність функціонування КСЗІ залежить від безлічі взаємопов'язаних між собою елементів, що діють, і, як правило, оцінюється сукупністю критеріїв, що знаходяться в складних конфліктних взаєминах. Відсутність на сьогоднішній день загального підходу до вирішення завдань даного класу закономірно спричиняє за собою різноманіття різних не взаємопов'язаних методів оцінки рівня захисту інформації. Процес визначення ефективності систем захисту починають з вибору і обґрунтування показників (критеріїв) оцінки ефективності системи захисту, а потім переходять до підбору або розробки методик розрахунку цих показників.

У таблиці 1 приведені умовні назви підходу, що використовуються для вибору критеріїв і оцінки параметрів, показники ефективності систем захисту і методики їх розрахунку.

Найбільш поширеними методами оцінки ефективності КСЗІ, які використовуються при так званому оптимізаційному або комбінаторному підході, є адитивний метод Балаша і метод гілок і меж, що відноситься до класу завдань дискретного програмування з булевими змінними. Вказані методи використовуються як для побудови нової КСЗІ, так і для оцінки якісних характеристик існуючої КСЗІ.

Аналіз викладених підходів до оцінки рівня захищеності інформації показав, що вони мають низку проблемних питань, до основних з яких слід віднести:

- відсутність чіткої ієрархічної структури рівня захищеності інформації КСЗІ з визначенням інтегральних (загальних) і часткових показників різного рівня, принципів згортання часткових показників (у тому числі, різного типу) в інтегральні;
- складність комплексної оцінки рівня захищеності інформації КСЗІ на основі наведених в методиках часткових показників та способів їх згортки у інтегральний показник;
- відсутність можливості вирішення оптимізаційних завдань, важливих при формулюванні та прийнятті рішення на впровадження комплексу заходів з забезпечення захисту інформації на СОІД;
- неврахування у методиках оцінки ефективності КСЗІ зв'язків між показниками, що використовувалися як основними так і імовірними показниками;
- неврахування нестохастичних, у тому числі нечітких, факторів впливу на рівень захищеності інформації КСЗІ на СОІД;
- фактична відсутність інтегральної оцінки рівня захищеності інформації за умов впливу загроз на інформацію що циркулює на СОІД.

Таблиця 1

Показники оцінки ефективності комплексних систем захисту і методики їх розрахунку

№ п/п	Підхід до оцінки КСЗІ	Показники оцінки ефективності	Спосіб розрахунку показників
1	**2**	**3**	**4**
1.	Статистичний	Загроза *i*-го типу виникає в середньому за період часу T_i.	Статистична обробка потенційних загроз і їх наслідків.
2.	Імовірнісний	Сумарні середні втрати $R=\sum_{i=1}^{2^n}\sum_{j=1}^{2^n}P(\vec{\gamma}/\vec{x},)P(\vec{s})\Pi(\vec{\gamma}/\vec{s})+m$, $P(\vec{\gamma}/\vec{m}\,\vec{s})$ - вірогідність усунення; $P(\vec{s})$ - апріорна вірогідність стану об'єкту контролю; $\Pi(\vec{\gamma}/\vec{s})$ - втрати прийняття рішення *s* при стані об'єкту s; m - кількість розпізнаваних погроз.	Визначається імовірність відмови системи від обробки даних в результаті реалізації загроз.
3.	Частотний	Очікуваний збиток від і-ї загрози: $R_i=F(S,V)$, де S - показник частоти виникнення загрози; V - умовний показник збитку.	На підставі аналізу статистичного матеріалу задається значення *S*, величина V вибирається рівною від 1 до max можливої суми збитку, розраховується значення показника R_i як функції параметрів *V* і *S*.
4.	Експертне оцінювання	Ступінь забезпечення безпеки *SR* системи *S* $SR_{(s,r)}=\frac{1}{n_{i=1}^{n}}W_iG_i.$	Визначається кількість (n) і перелік параметрів (i), які характерезують КСЗІ. Задаються значення суб'єктивних коефіцієнтів важливості (W_i) кожній з характеристик G_i, призначених експертним шляхом. Розраховуються значення параметра *SR*.
5.	Інформационно -ентропійний	Величина інформаційної ентропії Шенона: $\psi(t)=(\int_0^t s_n(t-\tau)...(\int^t s_3(\int_0^t s_1(\tau)s_2(t-\tau)d\tau...)d\tau$ $s_1 \ldots . s_n$ - значення інформаційної ентропії різних підсистем.	Проводиться аналітичне обчислення інформаційної ентропії системи, використовуючи поняття згортки функції. При лінійній залежності ефективність інтеграції підсистем в інформаційному плані вважають задовільною. Інакше – неефективною.
6.	Нейромережевий підхід (багатокритерійна оцінка)	Нечіткі показники захисту інформаційної системи у вигляді лінгвістичних змінних, таких як: “абсолютно незахищена”, “недостатньо захищена”, “захищена”, “достатньо захищена”, “абсолютно захищена” $A=\sum_{i=1}^{n}\frac{\mu^A(x_i)}{x_i}.$	Приналежність певного рівня безпеки визначається на проміжку [0, 1], показники надійності являються функцією приналежності $\mu^A(x_i)$, де – є елемент множини *X* – вимог безпеки, *A* – безліч значень, що визначають виконання вимог безпеки. Оцінка ефективності проводиться по чітко визначених критеріях.

Продовження таблиці 1

1	2	3	4
7.	Метод мінімізації ризиків.	Показник економічного ефекту від управління ризиками розраховується по формулі, що враховує Мо – сумарні вірогідні втрати без обробки ідентифікованих ризиків; сумарні вірогідні втрати після обробки ризиків М; сумарні фактичні втрати від прояву ризиків Іф; сумарні фактичні витрати на обробку ідентифікованих ризиків (Н = Нф); сумарні фактичні втрати від прояву ризиків Іфн; сумарні фактичні витрати на обробку ризиків Нфн: $E = (\sum_{i=1}^{N} M_{oi} - \sum_{i=1}^{N} M_i) - ((\sum_{i=1}^{N} I_{фi} + \sum_{i=1}^{N} H_{фi}) + (\sum_{j=1}^{K} I_{фнj} + \sum_{j=1}^{K} H_{фнj}))$.	1. Провести фіксацію ризиків. 2. Визначити індекс ризику (може бути виражений відносним або абсолютним рівнем витрат і вимірюється вірогідністю виникнення ризику і ступенем впливу ризику при його виникненні). 3. Класифікація ризиків за ступенем дії і по рівню впливу. 4. Визначення способів обробки ризику. 5. Розрахунок показників, що характеризують ризики. 6. Розрахунок показника економічного ефекту від управління ризиками.
8.	Матричний (формальні моделі захисту).	Стан системи захисту описується трійкою параметрів, наприклад: (*S, O, M*) – множини *S* – суб'єктів, *O* – об'єктів, *M* – прав доступу; Або (*O, H, M*) - *O* - основи і складові частини системи (нормативно-правова, організаційна, інформаційна і так далі), *H* – напрями захисту, *M* – етапи створення КСЗІ.	1. Визначення параметрів. 2. Складання тривимірної матриці відносин. 3. Перетворення матриці відносин в двовимірну таблицю. 4. Визначення якісних і кількісних значень показників.
9.	Багаторівневий підхід.	Стан системи захисту описується сукупністю рівнів конфіденційності і набору категорій конфіденційності.	Модель кінцевих станів Бела Ла-Падули. Гратчаста модель Д. Деннінга.
10.	Оптимізаційний (комбінаторний).	Вирішується завдання дискретного програмування вигляду: максимізувати $\sum_{j=1}^{n} c_j x_j$ за умов $\sum_{j=1}^{n} a_{ij} x_j \le b_i, i = \overline{1,m};$ $x_j \in \{0,1\}, j = \overline{1,n}.$	Методи Балаша для цілочисельних змінних, гілок і меж, виключення групи невідомих, елементи теорії подвійності, інструментарій лінійного, опуклого і параметричного програмування.

Аналіз підходів до оцінки ефективності КСЗІ, дозволяє зробити висновок, що в основі практично всіх відомих методик оцінки ефективності КСЗІ лежать такі математичні моделі (ММ): оціночні – за цільовою спрямованістю; однорівневі – за ієрархічною структурою; аналітичні – за способом опису функціональних зв’язків; комбіновані – за способом урахування випадкових факторів; імовірностні – з точки зору врахування стохастичної невизначеності [5].

Але при такому підході практично не враховується той факт, що будь-який СОІД діє за умов істотної невизначеності внутрішнього і зовнішнього середовищ та описується на основі інформації, що має неповний, неточний або не повністю визначений характер.

Існуючі підходи або зовсім виключають невизначеність зі своїх ММ, або нездібні формально описати і врахувати всю можливу її різноманітність. Отже, необхідні нові, додаткові, аналітичні підходи й інструменти для вирішення завдань щодо оцінки рівня захищеності інформації КСЗІ на СОІД.

Аналіз існуючих методик показав, що цілком вірно пропонується оцінювати ефективність КСЗІ, як складну систему і характеризувати декількома частковими показниками, на підставі яких формується загальний критерій.

Усі зазначені підходи правомірні. Проте, їх реалізація не відображає у повній мірі суті захисту інформації на СОІД і не дозволяє однозначно визначити запропоновані дослідниками показники ефективності КСЗІ, як адекватний процесу інтегральний показник, з точки зору реалізації можливостей КСЗІ щодо вирішення покладених на неї завдань.

Також існуючі методики оцінки ефективності КСЗІ, мають суттєві недоліки, а саме:

- методики спрямовані на оцінку й дослідження окремих показників, не дозволяють комплексно оцінити рівень захищеності інформації КСЗІ взагалі та її окремих елементів;
- методики не адаптовані до змін, які відбулися у можливостях розвідки щодо комплексного застосування технічних засобів розвідки (ТЗР), підвищення їх технічних та оперативних характеристик, що особливо впливає на забезпечення захисту інформації на СОІД;
- відсутність підходу щодо визначення складових КСЗІ з точки зору оцінки захищеності інформації її окремих елементів.

Неврахування зазначених недоліків не дозволяє з достатньою достовірністю і точністю оцінити рівень захищеності інформації для подальшого обґрунтування рекомендацій щодо удосконалення КСЗІ в зазначених умовах. В наявному вигляді ці методики не можуть бути застосовані для проведення дослідження за обраною темою і потребують удосконалення.

Об’єктивні труднощі, пов’язані з вибором і формулюванням одного, єдиного, основного і повного показника оцінки КСЗІ, призводять до того, що на практиці широко використовують не один узагальнений, а безліч часткових показників [5]. Використання сукупності показників іноді дозволяє з достатньою, для практичних завдань проектування, повнотою і точністю оцінити загальний рівень захищеності інформації КСЗІ на СОІД.

Оцінювання КСЗІ є класичною задачею, в якій оцінюються підсистеми, окремі елементи та вся система взагалі. Це передбачає вибір сукупності показників, яка дозволить оцінити ефективність функціонування її підсистем (елементів) та їх внесок до ефективності функціонування підсистем і системи в цілому.

Такий підхід дозволить врахувати те, що виконання КСЗІ – це, в основному, ймовірний процес (значна кількість показників має імовірнісний характер), також поєднати ці показники оцінки з показниками іншого типу та вжити заходів щодо зменшення ступеня невизначеності системи (як стохастичної, так і нестохастичної).

Центральною ланкою розв’язання ЕАЗ оцінювання рівня захищеності КСЗІ є розробка КМ ПО (концептуальної моделі предметної області), яка формалізує структуру оцінки, що складається з сукупності показників оцінки та зв’язків між ними. Враховуючи зазначене, в основу створення КМ (концептуальної моделі) оцінки рівня захищеності КСЗІ було покладено її розподіл на ієрархічні рівні, які описують процес самого забезпечення захисту інформації на СОІД, процес оцінки способів забезпечення захисту інформації елементів КСЗІ та встановлення зв’язків між цими рівнями за допомогою експертно-аналітичних методів. При цьому ієрархічна сукупність показників оцінки ефективності КСЗІ побудована на двох рівнях оцінки: рівень захищеності інформації КСЗІ на СОІД та складових КСЗІ на СОІД [6].

Для реалізації цього підходу як комплексний показник оцінки на кожному ієрархічному рівні приймаємо рівень захищеності інформації:

- комплексної системи захисту інформації - $R_i^{\text{ЗІ}}$;
- складових комплексної системи захисту інформації - конфіденційності інформації $\left(R_i^{\text{К}}\right)$, цілісності інформації $\left(R_i^{\text{Ц}}\right)$, доступності інформації $\left(R_i^{\text{Д}}\right)$.

Ці показники для кожного рівня є інтегральними, тобто визначаються послідовною згорткою часткових для нього показників нижнього рівня. Але по відношенню до показників верхнього рівня він сам буде частковим. Так, показники верхнього рівня визначаються послідовною згорткою часткових для нього показників нижнього рівня з використанням математичного апарату нечітких множин.

Часткові показники, на основі яких будуть визначатися інтегральні показники нижнього рівня, можуть бути як у числовому, так і в номінальному (лінгвістичному) вигляді. Ці характеристики надаються за спеціальною шкалою методом експертної оцінки.

Таким чином, на основі такого підходу створена чітка ієрархічна сукупність показників, яка характеризує рівень захищеності інформації КСЗІ на ССОІД. Вона складається з ряду окремих показників (простих і узагальнених) різного рівня (елемент, система) та інтегрального загального показника – рівня захищеності інформації КСЗІ.

Ця сукупність показників спільно з КМ ПО (загальною та частковими) є основою методики оцінки КСЗІ. Під методикою оцінки КСЗІ розуміється комплекс організаційних заходів і методів, програмних засобів, побудованих на єдиній теоретичній та інструментальній основі, які забезпечують комплексне вирішення питань організації та проведення такої оцінки, адекватної обробки, аналізу та видачі результатів.

Проведений аналіз показав, що за своєю суттю задача оцінки рівня захищеності інформації КСЗІ спрямована на одержання оцінок КСЗІ (елементів) по різноманітних показниках та прийняття рішення щодо додаткових заходів забезпечення захисту інформації на СОІД. Ця задача є комплексною, складною й вимагає всебічного притягнення спеціалістів-експертів, які здатні вирішувати такого роду аналітичні задачі. При вирішенні подібних задач, основною проблемою є формалізація об’єкту оцінки в слабкоструктурованих (що погано формалізуються) ситуаціях [7].

Фактично методика, яка ґрунтується на новій сукупності показників, принципах побудови математичної моделі (ММ) оцінки КСЗІ, визначення інтегральних показників на основі часткових. У той же час методика, що пропонується, використовує як окремі елементи положення всіх раніше відомих підходів та сумісна з ними.

Як результат, ММ оцінки КСЗІ, яка запропонована в статті є оціночною та прогнозованою за цільовою спрямованістю; багаторівневою за ієрархічною структурою; аналітичною за способом опису функціональних зв’язків; імовірнісною з точки зору врахування стохастичної невизначеності; комбінованою за способом урахування випадкових факторів (реалізовані детермінований та стохастичний підходи з урахуванням нестохастичної невизначеності); за характером вихідної інформації такою, що використовує методи обробки нечітких даних.

Висновки

Таким чином для вирішення задачі оцінки КСЗІ необхідно застосовувати такий підхід, який ґрунтується на використанні принципів і правил системного аналізу, експертно-аналітичного методу вирішення складних слабоструктурованих завдань та ТНМ. Структура оцінки рівня захищеності інформації КСЗІ на СОІД повинна ґрунтуватися на відповідній ієрархічній сукупності показників, яка складається з ряду окремих показників (простих і узагальнених) різного рівня (складова, система) та інтегрального загального критерію – рівня, який характеризує ступінь виконання функціонування КСЗІ власної цільової функції. Обрані показники захищеності інформації КСЗІ побудовані на двох рівнях оцінки: рівня захищеності інформації комплексною системою захисту інформації; рівня захищеності інформації складових комплексної системи захисту інформації. Для реалізації цього підходу

як комплексний показник на кожному ієрархічному рівні прийнято рівень захищеності КСЗІ та складових КСЗІ.

ЛІТЕРАТУРА

1. Левченко Е.Г. Показники багатоступінчатих систем захисту інформації / Е.Г. Левченко, Р.Б. Прус, А.О. Рабчун // Вісник Інженерної академії України. – 2009. – №1. - С. 61-65.

2. Бочарников В.П. Fuzzy - технология: Математические основы. Практика моделирования в экономике / В.П. Бочарников. - СПб.: “Наука” РАН, 2001. - 328 с.

3. Бочарников В.П. Fuzzy - технология: Основы моделирования и решения експертно-аналитических задач / В.П. Бочарников, С.В. Свєшников. - К.: Эльга, Ника-Центр, 2003, - 296 с.

4. Алексеев А.В. Интерпретация и определение функций принадлежности нечетких множеств / А.В. Алексеев // Методы и системы принятия решений. - Рига: Риж. политехн. ин-т, 1979. - С. 42 - 50.

5. Толюпа С.В., Підходи до проектування та оцінки ефективності системи захисту інформації в автоматизованих системах обробки та передачі даних / С.В. Толюпа, О.М. Іванова, І.О. Демченко // Науково-технічний журнал “Сучасний захист інформації”. – 2013. - №1. – С. 25-30.

6. Толюпа С.В. Методика оцінки комплексної системи захисту інформації на об’єкті інформаційної діяльності / С.В. Толюпа, І.В. Борисов // Науково-технічний журнал “Сучасний захист інформації”. – 2013. - №2. – С. 43-49.

7. Бусленко Н. П. Моделирование сложных систем / Н.П. Бусленко. - М. : Главная ред. физ-мат лит-ры изд-ва “Наука”, 1968. - 356 с.

Надійшла: 03.03.2014 р. Рецензент: д.т.н., проф. Бурячок В.Л.