УДК 621.384

Толюпа С.В., Борисов І.В.

МЕТОДИКА ОЦІНКИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Для вирішення задачі оцінки КСЗІ запропонований підхід, який ґрунтується на використанні принципів і правил системного аналізу, експертно-аналітичного методу вирішення складних слабоструктурованих завдань та теорії нечітких мір.

Ключові слова: комплексна система захисту, інформація, об'єкт, теорія нечітких мір, нечітка логіка.

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 [1,2]. 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 [3].

Перспективність даного напряму досліджень будь-якої галузі за сучасних умов полягає в перевагах ТНМ, так як використання Fuzzy-технологій дозволяє:

– формалізувати в єдиній формі вхідні дані, що не формалізуються іншими методами. Фактично ТНМ дозволяє об'єднати формалізовані і неформалізовані методи аналізу КСЗІ;

– описати, за відсутності достатньої інформаційної бази (навіть якщо статистична інформація спотворена, недостатня або не викликає довіри), невизначеності будь-яких видів;

– провести прогнозовані розрахунки в умовах невизначеності, кількісно оцінити ризики будь-яких рішень (дій) та управляти ними, долаючи при цьому недоліки та обмеження існуючих методів оцінки можливих ризиків (наприклад, імовірнісного і мінімаксного підходів);

– швидко моделювати складні динамічні системи, економлячи час на з'ясуванні точних значень змінних і складанні рівнянь, що їх описують, порівнювати їх із заданою мірою точності, оцінюючи різні варіанти вхідних значень;

– враховувати при побудові моделей і визначенні інтегральних показників логіку посадової особи, що приймає рішення щодо введення КСЗІ в експлуатацію, ідеально описуючи його суб'єктну активність;

– отримувати, на відміну від імовірнісних методів, навіть у реальних умовах низької якості вхідної інформації результат, що характеризується низькою чутливістю (високою стійкістю) до зміни вигляду функцій приналежності вхідних нечітких чисел;

– досить просто виявляти експертні знання.

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 об'єктів інформаційної діяльносі (ОІД), дозволяють підвищити наукову обґрунтованість, 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 ОІД [4].

Математичні моделі на основі Fuzzy-технологій набули широкого розповсюдження для вирішення задач в електроніці, кібернетиці, управлінні складними інтелектуальними системами. Більшість з таких завдань відносяться до класу експертно-аналітичних завдань (ЕАЗ) оцінки і прогнозу стану КСЗІ, вирішення яких повинне базуватися на методах системного аналізу, експертній методології і перспективних математичних методах обробки даних.

До цього ж класу й належать задачі оцінки рівня захищеності інформації КСЗІ на ОІД та ефективності рекомендацій щодо її підвищення. Ці задачі є взаємопов'язаними, комплексними, складними та вимагають всебічного залучення спеціалістів-експертів, здатних вирішувати такого роду аналітичні задачі. При вирішенні подібного класу задач основною проблемою є формалізація об'єкту оцінки в слабко структурованих (що погано формалізуються) ситуаціях та умовах невизначеності.

Вибір або формулювання показників, які характеризують рівень захищеності інформації КСЗІ є досить складним теоретичним і практичним завданням. Основні принципи вибору показників оцінки КСЗІ, як правило, можна конкретизувати таким чином:

– наявність одного узагальненого показника, відповідного основній меті оцінки рівня захищеності інформації КСЗІ на ОІД;

– можливість розкладання узагальненого показника на безліч показників, що відображають окремі приватні властивості, які різною мірою і часто протилежно впливають на цей узагальнений показник оцінки;

– урахування того, що в КСЗІ вирішується безліч завдань і реалізується безліч функцій, які на різних етапах функціонування мають різну значущість і тому по-різному впливають на узагальнений показник.

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 ОІД.

У даній статті при створенні ієрархічної структури показників оцінки та виборі інтегральних і часткових показників рівня захищеності інформації будемо враховувати:

– методологію та принципи системного аналізу;

– загальні принципи вибору показників ефективності;

– особливості та вимоги до КСЗІ;

– аналіз загроз інформації, які визначають порядок створення та функціонування КСЗІ й впливають на забезпечення захисту інформації на ОІД;

– місце КСЗІ в забезпеченні функціонування ОІД;

– можливі канали витоку інформації на ОІД.

Загальна модель визначення рівня захищеності інформації КСЗІ наведена на рис. 1.

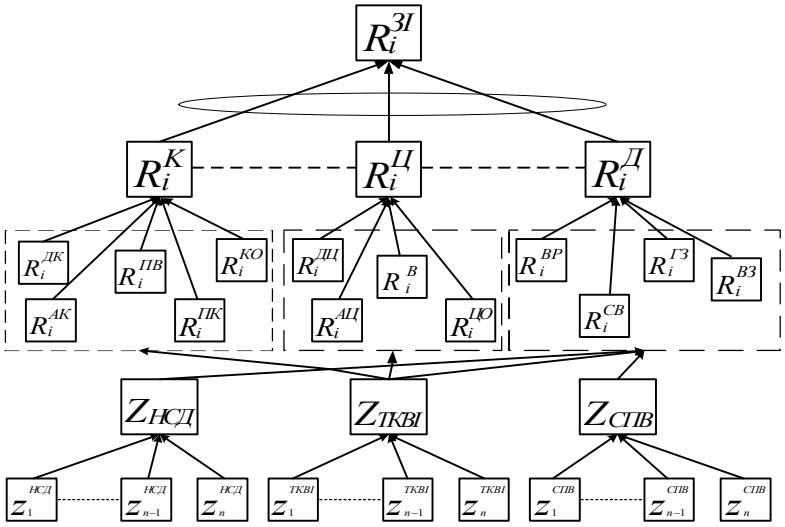

Рис. 1. Модель визначення рівня захищеності інформації КСЗІ

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 ОІД, 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 ОІД та складових КСЗІ на ОІД.

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. Комплексний показник першого рівня визначається наступним чином:

$$R_i^{\text{ЗІ}} = R_i^{\text{К}} \bigcap R_i^{\text{Ц}} \bigcap R_i^{\text{Д}}, \tag{1}$$

де $\bigcap$ і $\bigcup$ - знаки логічних операцій "І" та "АБО", відповідно;

Для другого рівня використовуються такі вирази:

$$R_i^{\text{К}} = R_i^{\text{ДК}} \bigcap R_i^{\text{АК}} \bigcap R_i^{\text{ПВ}} \bigcap R_i^{\text{ПК}} R_i^{\text{КО}} \text{ та /або}$$
$$R_i^{\text{ДК(АК,ПВ,ПК,КО)}} = \bigcap_{i=1}^{N} \left(R_i^{\text{ДК(АК,ПВ,ПК,КО)}} \right); \quad (2)$$

де $R_i^{\text{ДК}}$ - показники рівня довірчої конфіденційності інформації; $R_i^{\text{АК}}$ - показник адміністративної конфіденційності; $R_i^{\text{ПВ}}$ - показник повторного використання; $R_i^{\text{ПК}}$ - показник прихованих каналів; $R_i^{\text{КО}}$ - показник конфіденційності при обміні.

$$R_i^{\text{Ц}} = R_i^{\text{ДЦ}} \bigcap R_i^{\text{АЦ}} \bigcap R_i^{\text{В}} \bigcap R_i^{\text{ЦО}} \text{ та /або}$$
$$R_i^{\text{ДЦ(АЦ,В,ЦО)}} = \bigcap_{i=1}^{N} \left(R_i^{\text{ДЦ(АЦ,В,ЦО)}} \right); \quad (3)$$

де $R_i^{\text{ДЦ}}$ - показник довірчої цілісності; $R_i^{\text{АЦ}}$ - показник адміністративної цілісності; $R_i^{\text{В}}$ - показник відкату; $R_i^{\text{ЦО}}$ - показник цілісності при обміні.

$$R_i^{\text{Д}} = R_i^{\text{ВР}} \bigcap R_i^{\text{СВ}} \bigcap R_i^{\text{ГЗ}} \bigcap R_i^{\text{ВЗ}} \text{ та /або}$$
$$R_i^{\text{ВР(СВ,ІЗ,ВЗ)}} = \bigcap_{i=1}^{N} \left(R_i^{\text{ВР(СВ,ГЗ,ВЗ)}} \right). \quad (4)$$

де $R_i^{\text{ВР}}$ - показник використання ресурсів; $R_i^{\text{СВ}}$ - показник стійкості до відмов; $R_i^{\text{ГЗ}}$ - показник гарячої заміни; $R_i^{\text{ВЗ}}$ - показник відновлення після збоїв.

Знак $\bigcap$ може бути не тільки “І”, як і знак $\bigcup$ - не тільки “АБО”. Семантичний відтінок операцій може змінюватися від “І” до “АБО” та навпаки, що породжує семантичний спектр відповідних оцінок [4].

Процедура згортки у кожному випадку здійснюється за різними правилами: від простого арифметичного сумування до використання методів нечіткої логіки за допомогою ТНМ. В останньому випадку визначення інтегральних оцінок виконується на основі відповідних нечітких логічних операцій.

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 викладеного підходу створена чітка ієрархічна сукупність показників, яка характеризує рівень захищеності інформації КСЗІ на ОІД. 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. У відповідності з цим при створенні методики оцінки рівня захищеності інформації КСЗІ на ОІД були визначені вимоги до:

– методів і процедур організації та математичного забезпечення проведення оцінки КСЗІ, формалізації та оброблення отриманих даних;

– програмних засобів, які реалізують математичне забезпечення та підтримують процедури проведення зазначених оцінок.

Метою оцінки КСЗІ є визначення здатності КСЗІ (її елементів) забезпечити захист інформації на ОІД, а також вироблення пропозицій щодо проведення необхідних підготовчих заходів.

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 ОІД. 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.

В якості особливостей зазначеної задачі слід вказати:

– на рівні цільових умов моделювання – багатокритеріальність, наявність складних психологічних аспектів формулювання, прийняття рішення та цілей визначених на якісному рівні;

– на рівні моделювання об'єктів предметної області – наявність лінгвістичних описів стану об'єктів (як окремих елементів, так і КСЗІ взагалі, а також загроз інформації, що циркулює на ОІД), відсутність, як правило, можливості статистичного опису;

– на рівні вихідної інформації для моделювання – суперечливість, нечіткість, неоднозначність та інші види невизначеності.

Методика оцінки КСЗІ, що пропонується, спрямована на вирішення двох взаємопов'язаних завдань.

Перше (основне) – оцінки потенційного рівня захищеності інформації КСЗІ на ОІД взагалі та її складових зокрема. Вона вирішується за типових умов.

Критерії та показники, що визначаються у ході зазначених процедур як і додаткові характеристики, за допомогою яких здійснюється згортка, становлять основу так званої бази знань (якісні та кількісні зв'язки між елементами ієрархічної структури). Наповнення бази знань здійснюється на основі досліджень під час виконання заходів забезпечення захисту інформації та за результатами експертного опитування із застосуванням відповідних методів отримання знань [6]. При цьому можуть використовуватися такі методи отримання знань:

– для уточнення КМ ПО – текстологічні методи (аналіз документів, літератури, довідників тощо) і пасивний комунікативний метод (спостереження за ходом навчань і застосування);

– для встановлення зв'язків між елементами КМ – активний комунікативний метод (експертне анкетування).

Таким чином, у процесі розробки методики оцінки КСЗІ, виконано таке:

– розроблено чітку ієрархічну структуру показників захищеності інформації з визначенням інтегральних (загальних) і часткових показників різного рівня, принципів згортання часткових показників (у тому числі, різного типу) в інтегральні;

– враховані особливості впливу загроз інформації на рівень її захищеності;

– забезпечено можливість згортки числових та нормативних показників за різними контекстами, враховано стохастичні, у тому числі нечіткі, фактори впливу на рівень захищеності інформації КСЗІ на ОІД;

– запропоновано покласти в основу математичного забезпечення оцінки КСЗІ теорію нечітких множин (мір) та інтегралів для забезпечення можливості адекватного виявлення нечіткої слабоструктурованої лінгвістичної інформації.

Фактично розроблено нову методику, 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.

Результати розрахунків порівнювались з вимогами щодо рівнів захищеності інформації, які викладені в НД ТЗІ 2.5-004-99 [7], що дозволяє оцінити можливий рівень захищеності інформації в заданих умовах (табл. 1).

Вимоги щодо рівня захищеності інформації КСЗІ Таблиця 1

Оцінка рівня захищеності інформації КСЗІ		**Можлива оцінка функціонування КСЗІ**
Числова	***Лінгвістична***	
>0,8	Абсолютно достатній	Забезпечення гарантованого захисту інформації
0,6-0,8	Достатній	
0,2-0,5	Недостатній	Створення умов для витоку інформації
< 0,2	Абсолютно недостатній	Витік інформації

Висновки:

1. Для вирішення задачі оцінки КСЗІ запропонований підхід, який ґрунтується на використанні принципів і правил системного аналізу, експертно-аналітичного методу вирішення складних слабоструктурованих завдань та ТНМ.

2. Структура оцінки рівня захищеності інформації КСЗІ на ОІД ґрунтується 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.

3. Методика та ММ оцінки КСЗІ розроблені на основі ієрархічної сукупності показників захищеності, принципах побудови ММ оцінки рівня захищеності КСЗІ, визначенні 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.

У процесі розробки методики оцінки рівня захищеності інформації КСЗІ забезпечена можливість згортки числових (імовірних) та нормативних (лінгвістичних) показників за різними контекстами, враховані нечіткі фактори впливу на рівень захищеності інформації КСЗІ на ОІД.

Як результат, розроблена ММ оцінки рівня захищеності інформації КСЗІ, є - оціночною та прогнозованою за цільовою спрямованістю;багаторівневою за ієрархічною структурою; за характером вихідної інформації такою, що використовує методи обробки нечітких даних.

ЛІТЕРАТУРА

1. 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.

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

3. Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений / Л. Заде. - М.: Мир, 1976. - 165 с.

4. Модели принятия решений на основе лингвистической переменной / [А.Н. Борисов, А.В. Алексеев, О.А. Крумберг и др.] – Рига: Зинатне, 1982. – 256 с.

5. Толюпа С.В. Метод багатокритеріального аналізу ефективності функціонування та забезпечення інформаційної безпеки інфокомунікаційних систем / С.В. Толюпа // Науково-технічний журнал „Захист інформації”. - 2012. - №3 (54). с. 80-86.

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

7. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, НД ТЗІ 2.5-004-99 – 58 с.

Надійшла: 24.02.2013 р.

Рецензент: д.т.н., проф. Розорінов Г.М.