УДК 004.413.4

О.А. Замула[1], В.І. Черниш[1], О.І. Аніщенко[2]

[1] *Харківський національний університет радіоелектроніки, Харків*
[2] *Центральне казенне конструкторське бюро «Протон», Харків*

ЗАСТОСУВАННЯ ТЕОРІЇ НЕЧІТКИХ МНОЖИН ТА ЛІНГВІСТИЧНОЇ НЕВИЗНАЧЕНОСТІ ПРИ ОЦІНЮВАННІ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянуті основи теорії нечітких множин та лінгвістичної невизначеності. Запропоновано використання методу нечіткого виводу при оцінюванні ризиків інформаційної безпеки.

Ключові слова: *інформаційна безпека, інформаційний ризик, нечітка множина, оцінка ризиків.*

Вступ

Інформаційна безпека (ІБ) в даний час стає необхідною умовою успішного розвитку господарюючого суб'єкта (ГС). Ризик компрометації інформації впливає на матеріальні і нематеріальні активи організації і, в кінцевому рахунку, на результати її виробничо-економічної діяльності.

У зв'язку з великим числом інформаційних ризиків (ІР), широким різноманіттям значень збитку при їх реалізації та обмеженістю бюджету на ІБ ГС виникає завдання раціонального фінансування витрат на захист інформації. Можлива інша постановка завдання: при фіксованому обсязі фінансових вкладень необхідно знизити рівень ризику компрометації інформації на максимальну величину [1 – 3].

В даний час оцінка ризиків ІБ проводиться методами, що вимагають статичних даних по інцидентам, або використовують деякі вразливості інформаційної системи. Недоліком таких методів є той факт, що ризики ІБ мають найчастіше суб'єктивні значення, що вносить суттєву похибку в результати їх оцінювання. З іншого боку, оцінка ризиків за допомогою експертних методів вносить перешкоду у вигляді неточності експертної оцінки [1 – 3].

Ще одним фактором, що ускладнює прийняття рішення з обробки виявленого ризику – мала кількість параметрів, якими він характеризується. Більшість оцінок ІР спираються на два показники – величину можливого збитку ризику та імовірність його виникнення.

Однак дуже часто потрібно також знання величини витрат на зниження ризику до прийнятного рівня. Можуть використовуватися інші показники: характер ризику (періодичний, випадковий або одноразовий), метод фінансування програм по зниженню ризику (одноразові або регулярні витрати на зменшення ризику). Введення все нових і нових елементів ускладнює модель оцінки ризику ІБ і створює певні труднощі її практичного використання.

У статті розглядаються моделі оцінки ризиків ІБ на основі теорії нечітких множин.

Основний матеріал

Застосування теорії нечітких множин та лінгвістичної невизначеності

При оцінюванні ризиків ІБ корпорацій аналітик збирає відомості про інформаційну систему (ІС), будує її модель і потім аналізує (виходячи з власного професійного досвіду) отриману модель з точки зору предметної області.

Особливості даного підходу можна визначити наступними пунктами:

1. Предметна область ІБ складається переважно з сутностей, виражених не в строгому, формалізованому вигляді, а у вигляді тверджень на мові оригіналу. Таким твердженням властива лінгвістична невизначеність. Під лінгвістичною невизначеністю в даному випадку розуміються якісні оцінки мови оригіналу для тих чи інших кількісних або якісних характеристик, а також для логічного висновку, прийняття рішень та планування [4].

2. Професійний досвід експерта складається з сутності, що в силу особливостей мозку виражені у формі вербальних і невербальних когнітивних образів. Когнітивний образ являє собою суб'єктивну репрезентацію досвіду і не має чітких, визначених меж [4, 5].

3. У зв'язку з цим, звичні математично точні логічні зв'язки і відносини рівності та включення або втрачають сенс, або неприпустимо спотворюють логічні висновки.

Основи теорії нечітких множин та лінгвістичних змінних при оцінюванні ризиків ІБ, поняття «нечітка множина» введено Л.А. Заде в 1965 р. [4]. У той же час він випустив перші праці з теорії нечітких множин.

Теорія являє собою апарат формалізації невизначеностей, що виникають при моделюванні реальних об'єктів, а саме, при використанні природних слів для опису об'єкту.

Для вираження ризику нечіткими числами необхідно знайти основні параметри, що його характеризують (початкові та центральні моменти) за допомогою функції приналежності.

В основі концепції оцінювання ризиків ІБ за допомогою використання апарату теорії нечіткої логіки лежить логіко-лінгвістична модель, що базується на теорії нечітких множин та лінгвістичних підставних.

Нечіткою множиною в деякому непустому просторі U називається множина впорядкованих пар

$$\{x_i / \mu_A(x_i)\},$$

де $\mu_A(x)$: U → [0, 1] – функція приналежності x до A, що додається до кожного елемента x ∈ U ступінь його належності до нечіткої підмножини A. Функція μA(x) приймає свої значення в цілком упорядкованій безлічі множин M = [0, 1], називається безліччю приладдя [3, 4].

Лінгвістична змінна характеризується набором (L, T (L), U, G, M), в якому L – назва змінної; T (L) – терм-множина змінної L, U – універсальна множина базових значень (область, в якій визначені значення лінгвістичної змінної); G – синтаксичне правило; M – семантичне правило [6].

Терм-множина T (L) являє собою сукупність термів – назв лінгвістичних значень змінної L. Кожному терму відповідає нечітка підмножина безлічі U, визначальне лінгвістичне значення терма.

Іншими словами, зміст терма характеризується функцією належності μ: U → [0, 1], яка кожному елементу u ∈ U ставить у відповідність значення приналежності цього елементу терму. Синтаксичне правило G має зазвичай форму граматики, що породжує терми. Терм, що складається з одного або більше атомарних термів, називається складовим термом. Семантичне правило M ставить у відповідність кожному атомарному терму його зміст у вигляді нечіткої множини. Крім того, семантичне правило M пов'язує приналежності атомарних термів в складені лінгвістичні значення з приналежністю складеного значення.

Некласичні лінгвістичні підставні

Некласичні лінгвістичні підставні, що визначенні на множині чисельних вимірних показників, можливо вважати класичним випадком. Наведемо приклади лінгвістичних підставних, визначених на деяких інших шкалах, та які цілком можна застосувати для оцінювання подій безпеки.

У випадку, коли немає можливості заснувати лінгвістичну підставну на чисельних показниках, можна використовувати в якості універсальної множини порядкову шкалу деяких вражень та образів, позначених абстрактними символами [6, 7]. Таку шкалу можна скласти з кінцевої множини прийнятих за еталон об'єктів, що мають спільну природу, але різну інтенсивність. Досліджуючи інші об'єкти, експерт на основі своїх вражень порівнює їх з еталонною шкалою і визначає нечітку множину, що описує схожість досліджуваного об'єкта з об'єктами, що належать еталонній шкалі.

Можна виділити єдиний еталонний складний об'єкт з низкою властивостей, які складають номінальну (невпорядковану) шкалу. У такому випадку експерт, визначаючи нечітку множину на номінальній шкалі, задає певний рівень входження об'єкта в еталон на основі комбінацій властивостей.

Лінгвістична змінна ймовірності – це лінгвістична змінна, визначена в універсальній множині значень ймовірності P = [0, 1]. Відповідно до класичної теорії ймовірностей, подія A визначається як елемент поля підмножини F, що належать простору елементарних подій Ω. Класична ймовірність події A визначається як невід'ємне дійсне число P (A).

Існує багато реальних проблем, в яких порушуються ці гіпотези, котрі приведені в неявній системі аксіом. По-перше, подія A часто буває нечіткою в тому сенсі, що не існує достатньої межі між її появленням та непоявленням. Таку подію можна охарактеризувати як нечітку підмножину простору елементарних подій Ω з вимірною функцією приналежності μA. По-друге, навіть якщо A – цілком певна звичайна (не нечітка) подія, її ймовірність P (A) може бути визначена виключно лінгвістично. В даному випадку можна зробити припущення того, що ймовірність P є лінгвістичною змінною. Це дозволяє застосовувати класичну теорію ймовірності до певних ситуацій [6].

Лінгвістична змінна істинності – це лінгвістична змінна, визначена в універсальній множині значень істинності V = [0, 1]. Позначимо терміном «висловлення» твердження виду «u є A», де u – назва деякого предмета, а A – назва нечіткої підмножини універсальної множини U. В даному випадку висловлюванню типу «u є A» відповідають дві нечітких підмножини. Перше з них – M (A) – сенс A, тобто нечітка підмножина з назвою A універсальної множини U. Друге – значення істинності твердження «u є A» (або просто значення істинності A), що позначається як v(A) і визначається як можливо нечітка підмножина універсальної множини значень істинності V [6 – 8].

Агрегація та узагальнення значень лінгвістичної змінної. Застосування механізму нечіткого виводу

Особливість будь-якої експертної системи, що основана на лінгвістичних підставних, полягає в тому, що вона має можливість будувати алгоритм вирішення задачі за допомогою міркувань. Основними логічними прийомами, використовуваними в міркуваннях, є узагальнення і агрегація понять [7, 8].

Узагальнення понять – це форма зв'язку понять, при якій на основі вихідних понять P та Q утворюються узагальнююче поняття K більш високого рівня. Поняття K зберігає загальні ознаки вихідних понять P та Q, але ігнорує їх більш чіткі різноманітні ознаки.

Агрегація понять – це форма зв'язку понять, при якій на основі вихідних понять P і Q утворюється поняття-агрегат R більш високого рівня і який успадковує всі ознаки входять до понять P і Q. Поняття R має ознаки як поняття P, так і поняття Q. Для теоретико-множинної форми представлення понять узагальнення відповідає операції перетину нечітких множин, а агрегація операції – об'єднання нечітких множин.

Перетин двох нечітких множин в загальному вигляді являє собою бінарну операцію

$$\mu_{A\cap B}(x) = t(\mu_A, \mu_B),$$

де функція t – так звана t-норма. Об'єднання двох нечітких множин в загальному вигляді являє собою бінарну операцію

$$\mu_{A\cup B}(x) = s(\mu_A, \mu_B),$$

де функція s – s-норма, що є доповнення норми щодо t-норми. Опції t і s задовольняють таким умовам при a, b, c $\in$ [0, 1]: умова монотонності t(a, b) $\leq$ t(b, c) для b $\leq$ c; умова комутативності t (a, b) = t (b, a); умова асоціативності t(t(a, b), c) = t(a, t(b, c)).

Крім того, t-норма задовольняє граничним умовам t(a, 0) = 0, t(a, 1) = a. s-норма задовольняє граничним умовам s(a, 0) = a, s(a, 1) = 1 [6].

Розглянемо механізм нечіткого виводу, що є основною ланкою в методиці отримання оцінки ризику ІБ. Він перетворює вхідні дані у вихідну підставну, тобто в оцінку ризику.

Механізм нечіткого виводу є послідовність операцій над вхідними даними відповідно до параметрів, що використовується в наборі продукційних правил (рис. 1) [8].

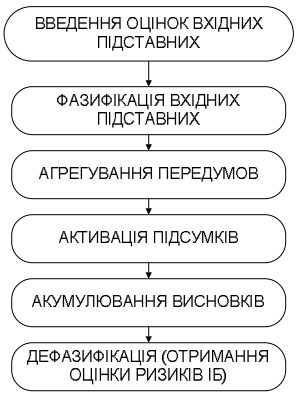

Рис. 1. Механізм системи нечіткого виводу

Основними етапами нечіткого виводу є:

- *введення експертних оцінок,* що забезпечує механізм виводу необхідної інформації;
- *фазифікація* – являє собою процедуру знаходження функцій приналежності використаних термів вхідних підставних на основі вхідних даних;
- *агрегація* – є процедурою визначення ступеня істинності умов по кожному з правил системи нечіткого виводу;
- *активація* – являє собою процедуру знаходження ступеня істинності кожного з підсумків правил нечітких висновків;
- *акумуція* – являє собою процедуру знаходження функції приналежності для кожної з вихідних лінгвістичних змінних заданої сукупності правил нечіткого виводу [8].

Дефазифікацією є процедура знаходження чітких значень вихідних змінних, що найбільшою мірою відповідають вхідним даним та базі продукційних правил. Реалізація механізму нечіткого виводу полягає у використанні відомого або в розробці нового алгоритму обробки даних. Розглянемо приклади практичного використання механізму нечіткого виводу для отримання оцінки ризику ІБ [9].

Припустимо, що за допомогою продукційних правил нечіткої логіки необхідно відтворити механізм оцінки ризику, представлений в табл. 1 та рис. 2 (рекомендації стандарту NIST800-30).

Таблиця 1

Залежність ризиків від ймовірності та збитків

ймовірність (P)	збиток (D)		
	великий	середній	низький
велика	В	С	Н
середня	С	С	Н
низька	Н	Н	Н

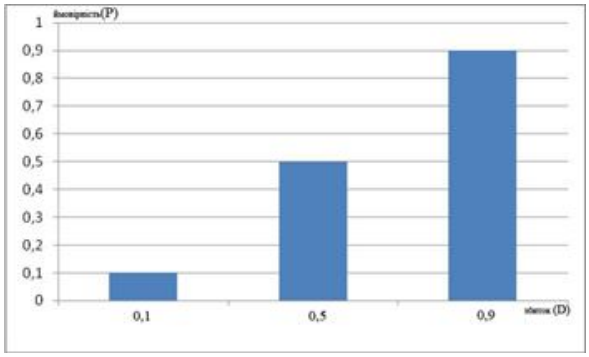

Рис. 2. Залежність ризиків від ймовірності та збитків

1. ЯКЩО Ймовірність – Велика ТА Збиток – Великий, ТО Ризик = В (великий);
2. ЯКЩО Ймовірність – Велика ТА Збиток – Середній, ТО Ризик = С (середній);
3. ЯКЩО Ймовірність – Велика ТА Збиток – Низький, ТО Ризик = Н (низький);
4. ЯКЩО Ймовірність – Середня ТА Збиток – Великий, ТО Ризик = С (середній);
5. ЯКЩО Ймовірність – Середня ТА Збиток – Середній, ТО Ризик = С(середній);
6. ЯКЩО Ймовірність – Середня ТА Збиток – Низький, ТО Ризик = Н (низький);

7. ЯКЩО Ймовірність – Низька ТА Збиток – Великий, ТО Ризик = Н (низький);

8. ЯКЩО Ймовірність – Низька ТА Збиток – Середній, ТО Ризик = Н (низький);

9. ЯКЩО Ймовірність – Низька ТА Збиток – Низький, ТО Ризик = Н (низький).

Механізм виводу буде мати два входу: один – для введення оцінки ймовірності, другий – для введення оцінки збитку (рис. 3).

Висновки

Теорія нечітких множин може буди застосована для оцінювання ризиків ІБ в умовах невизначеності значень показників ризиків, а також при виборі з групи ризиків.

Недоліком використання нечітких множин є суб'єктивність оцінки ризиків ІБ в нечітких термінах та суб'єктивність правил виводу.

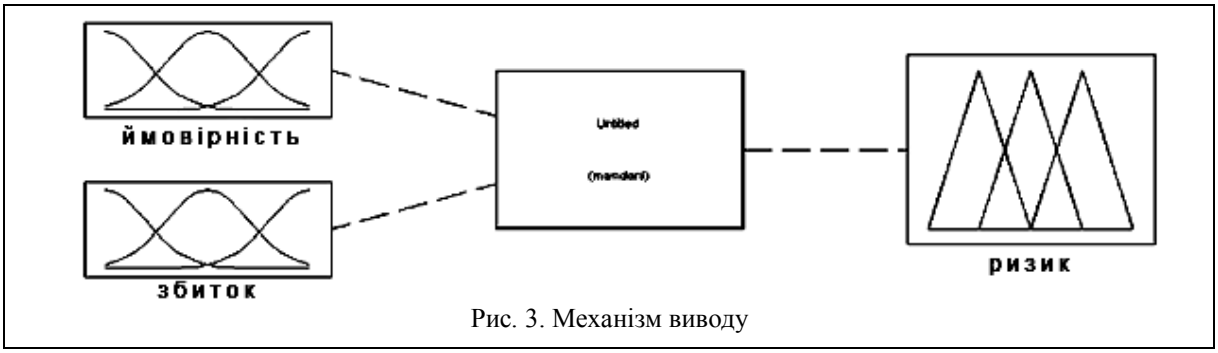

Рис. 3. Механізм виводу

Список літератури

1. Черныш В.И. Методы оценивания информационных рисков компании / В.И. Черныш // Материалы XV Международного юбилейного молодёжного форума «Радиоэлектроника и молодежь в XXI веке»: Сб. тезисов, 18-20 апреля 2011 р., Т.5. – Х.: ХНУРЭ. 2011. – С. 195.

2. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації . – Х.: ХУ ПС, 2011. – Вип. 2(92). – С. 53-56.

3. Замула А.А. Оценивание рисков информационной безопасности в современных информационных системах / А.А. Замула, В.И. Черныш, К.И. Иванов // XIV Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах»: тезисы докладов. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2011. – С. 31.

4. Zadeh L. A. Fuzzy sets. Information and Control. – 1965. – Vol. 8, № 3. – P. 338-353.

5. Замула А.А. Математические методы оценивания информационных рисков компании / А.А. Замула, В.И. Черныш, Ю.В. Землянко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. – Том 9, №1. – С. 123-127.

6. Круглов В.В. Нечёткая логика и искусственные нейронные сети. Учеб. пособие / В.В. Круглов, М.И. Дли,

7. Р.Ю. Голунов. – М.: Издательство Физико-математической литературы, 2001. – С. 224.

8. Леоненков А.В. Нечёткое моделирование в среде MATLAB и FuzzyTech / А.В. Леоненков. – СПб.: БХВ - Петербург, 2005. – С. 739.

9. Сидоров А.О. Разработка методики структурированной оценки риска / А.О. Сидоров, Ю.А. Торшенко, А.А. Павлютенков, Л.Г. Осовецкий // Научно-технический вестник СПбГУ ИТМО Системы: управление, моделирование, безопасность. – СПб., 2008. – № 55. – С. 108-110.

10. Шубин Ю.М. Метод формирования профиля защиты автоматизированной банковской системы / Ю.М. Шубин, А.О. Сидоров // Научно-технический вестник СПбГУ ИТМО Системы: управление, моделирование, безопасность. – СПб., 2008. – № 55. – С. 113-116.

Надійшла до редколегії 15.07.2011

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Харківський національний технічний університет сільського господарства ім. П. Василенка, Харків.

ПРИМЕНЕНИЕ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ И ЛИНГВИСТИЧЕСКОЙ НЕОПРЕДЕЛЕННОСТИ ПРИ ОЦЕНИВАНИИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Замула, В.И. Черныш, А.И. Анищенко

Рассмотрены основы теории нечетких множеств и лингвистической неопределенности. Предложено использование метода нечеткого вывода при оценке рисков информационной безопасности.

***Ключевые слова**: информационная безопасность, информационный риск, нечеткое множество, оценка рисков*

APPLICATION OF THE THEORY OF FUZZY SETS AND LINGUISTIC UNCERTAINTY IN ESTIMATION RISK INFORMATION SAFETY

A.A. Zamula, V.I. Chernish, A.I. Anishenko

The basics of the theory of fuzzy sets and linguistic uncertainty. Proposed use of the method of fuzzy inference in assessing information security risks.

***Keywords:** information security, information risk, fuzzy set, risk assessment.*