

4. Національні рахунки України за 2007 рік: Стат. зб. — К.: Держкомстат України, 2008. — 149 с.
5. *Маничуров І.Г.* Статистика економічного зростання та конкурентоспроможності країни. — К.: КНЕУ, 2006. — 388 с.
6. *McArthur J. W., Sachs J. D.* The Growth Competitiveness Index: Measuring Technological Advancement and the Stages of Development // The Global Competitiveness Report 2001—2002. — New York: Oxford University Press for the World Economic Forum, 2002. — 897 с.
7. <http://www.bank.org> // Офіційний сайт Всесвітнього банку.
8. <http://www.bank.gov.ua> // Офіційний сайт Національного банку України.
9. <http://www.bizpro.org.ua> // Проект БІЗПРО, Американська торговельна палата в Україні.
10. <http://www.imf.org> // Офіційний сайт Міжнародного валютного фонду.
11. <http://www.weforum.org> // The Global Competitiveness Report.
12. <http://www.ukrstat.gov.ua> // Офіційний сайт Держкомстату України.
13. <http://www.zakon.rada.gov.ua>

Стаття надійшла до редакції 12.01.09 р.

УДК 303.131.7

В. В. Вітлінський, д-р екон. наук, проф.,
ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»

Г. В. Мельник, Чернівецький національний університет
ім. Юрія Федьковича

МОДЕЛЮВАННЯ ЗАГРОЗ ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ПІДГРУНТІ ІНСТРУМЕНТАРІЮ НЕЧІТКОЇ ЛОГІКИ

АНОТАЦІЯ. В даній статті запропоновано лінгвістичний підхід до моделювання загроз активам інформаційної системи. Побудовано формалізований опис моделі загроз активам інформаційної системи на підґрунті нечіткої логіки.

ANNOTATION. The linguistic approach to the design of threats in the informative system is considered in this article. The formalized description of model of threats to the assets of the informative system is built with application of methods of fuzzy logic.

КЛЮЧОВІ СЛОВА. Інформаційні ризики, інформаційний актив, рівень загроз, порушник безпеки інформаційної системи, рівень вразливості системи, лінгвістичний критерій, функція належності, нечіткі терми, нечітка множина.

I. Вступ

Для оцінювання інформаційних ризиків необхідно виявити загрози активам інформаційної системи (ІС), тобто чинники ризику. Ґрунтуючись на класифікації чинників ризику, необхідно для кожного з прийнятих до розгляду елементів інформаційного активу виявити потенційні ризикові події, що можуть бути реалізовані. На нашу думку, вдалою концепцією щодо побудови моделей загроз ефективного функціонування інформаційних систем є методичні положення, які викладені, зокрема, в [5, 6].

Методологічні положення щодо аналізу та оцінювання ступеня загроз та ризиків ефективного функціонування інформаційної системи ґрунтуються, зокрема, на описі джерел загроз, вразливості, методів і об'єктів можливих нападів (наприклад, конфіденційності, цілісності, доступності активів), обсягів потенційного збитку [1]. По суті, необхідно розробити на основі сценарного аналізу адекватну модель ризику щодо ефективного функціонування інформаційної системи. Необхідно наголосити, що така модель має характеризуватись прогностичною силою і давати змогу здійснювати зіставлення кожному елементу активу ІС певних джерел загроз (чинників ризику), які можуть нанести збитків ІС на підґрунті ідентифікації системи джерел можливих загроз, існуючої стосовно відповідного елементу вразливості. Джерело загрози (чинник ризику) визначається, зокрема, як намір і спосіб умисної чи ненавмисної дії на вразливий актив, тобто це сукупність мотивів і умов, які можуть стати причиною порушення цілісності, доступності та конфіденційності інформації. Цілісність, доступність і конфіденційність інформації є вираженням вартості чи важливості інформаційного активу, який розглядається як об'єкт ризику, про що йдеться в низці праць, зокрема в [2].

Цілісність відображає необхідність захисту інформації від несанкціонованої зміни і зумовлені цим можливі збитки. Цілісність порушується в разі недозволених дій над даними або системами незалежно від того, були вони умисними чи випадковими.

Доступність — це забезпечення отримання необхідної інформаційної послуги (інформації) в потрібний час. ІС впроваджуються для надання певних інформаційних послуг внутрішнім і

зовнішнім користувачам. Якщо надати ці послуги в прийнятний термін неможливо, це тягне за собою відповідні збитки.

Конфіденційність — це забезпечення захисту від несанкціонованого доступу до інформації, її несанкціонованого використання, відтворення і розповсюдження.

Джерела загроз, які можуть призвести до порушення цілісності, доступності і конфіденційності інформації, повинні бути виявлені та описані з рівнем деталізації, який визначається реальними потребами та можливостями в захисті, тобто залежно від співвідношення між вартістю захисту ІС шляхом зниження ступеня ризику і вартістю можливої реалізації ризику. Зазначимо, що процес ідентифікації ризику є циклічним.

На частоту виникнення загрози інформаційному активу впливають два ключові чинники: контакт порушника з активом і дія порушника на цей актив [3].

Контакт у даному аспекті — це вірогідна частота, в межах певного часового інтервалу отримання порушником доступу до активу. Контакт може бути як фізичний, так і «логічний». Незалежно від методу, контакт може бути випадковим (не сфокусована або недостатньо орієнтована активність порушника), регулярним (контакт здійснюється через постійні дії порушника), а також навмисним (порушник має конкретну мету).

Дія (як наслідок контакту) — це вірогідність впливу порушника на інформаційний актив у разі здійснення контакту [3].

На підставі цього оцінювання виокремлюються найбільш значущі чинники ризику, а вже на підґрунті цього будуються детальні моделі оцінювання можливих загроз інформаційній безпеці ІС.

II. Постановка завдання

Для вибору математичної моделі поведінки потенційного порушника доцільніше використовувати деталізований кількісний підхід, який буде враховувати, зокрема, гриф інформації, що підлягає захисту. Оскільки кваліфікація порушника — поняття досить відносне і приблизне, доцільно прийняти за основу такі чотири рівні стійкості захисту або класи безпеки стосовно можливих порушників, про що йдеться, зокрема в [2]:

1-й клас рекомендується для захисту суттєво важливої інформації, витік, порушення або модифікація якої можуть призвести до великих збитків для санкціонованого користувача. Стійкість захисту має бути розрахована на порушника-професіонала;

2-й клас рекомендується використовувати для захисту важливої інформації в роботі кількох санкціонованих користувачів, які мають доступ до різних масивів даних або які формують свої файли, що недоступні іншим санкціонованим користувачам. Стійкість захисту має бути розрахована на порушника високої кваліфікації;

3-й клас рекомендується для захисту відносно цінної інформації, постійний несанкціонований доступ до якої, шляхом її накопичення, може призвести до витоку і більш цінної інформації. Стійкість захисту має бути розрахована на відносно кваліфікованого порушника-професіонала;

4-й клас рекомендується для захисту іншої інформації, яка для серйозних порушників не має цінності. Такий клас потрібний для дотримання технологічної дисципліни обліку та обробки; контролю інформації службового користування і відкритої інформації, з метою захисту її від випадкових порушень унаслідок помилок санкціонованих користувачів і часткового попередження випадків цілеспрямованих загроз.

Автори пропонують розглянути задачу побудови математичної моделі загроз інформаційній безпеці на етапі створення ІС. У цьому випадку важливо визначитися з чинниками інформаційних ризиків майбутнього проекту. На підставі вищевказаної класифікації рівнів необхідного ступеня безпеки ІС щодо загрози зі сторони порушника. Автори пропонують застосувати нечіткий лінгвістичний підхід до моделювання можливих загроз активам ІС.

III. Результати

Сформулюємо концептуальний підхід до аналізу та оцінювання рівня загроз і вразливості інформаційної системи з використанням нечітких описів [4, 7].

Для кожного класу безпеки (рівня стійкості захисту ІС) поставимо у відповідність лінгвістичні показники X_1, X_2, X_3, X_4 , а потім проведемо оцінювання ІС за відповідним набором із вищезазначених показників:

Для оцінювання рівня загроз стійкості захисту 1-го класу:

$$X_1 = f_1(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}), \quad (1)$$

для оцінювання рівня загроз стійкості захисту 2-го класу:

$$X_2 = f_2(x_1, x_2, x_3, x_4, x_5, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}), \quad (2)$$

для оцінювання рівня загроз стійкості захисту 3-го класу:

$$X_3 = f_3(x_1, x_2, x_3, x_4, x_5, x_9, x_{10}, x_{11}), \quad (3)$$

для оцінювання рівня загроз стійкості захисту 4-го класу:

$$X_4 = f_4(x_1, x_3, x_4, x_5). \quad (4)$$

Оцінювання здійснюється за показниками x_j (j — індекс показника $j=\overline{1,12}$), які характеризують рівень доступу до елементів інформаційної системи. За приклад можна взяти: x_1 — доступ до персональних ЕОМ, робочих станцій, терміналів користувачів; x_2 — до апаратури документування інформації; x_3 — до носіїв інформації, які переміщуються в межах зони ІС; x_4 — до документів; x_5 — до носіїв програмного забезпечення (ПЗ); x_6 — до носіїв залишків інформації; x_7 — до засобів завантаження ПЗ; x_8 — до апаратури передачі даних у зовнішні канали зв'язку; x_9 — до технологічних пультів і органів управління; x_{10} — до внутрішнього монтажу апаратури; x_{11} — до внутрішніх ліній зв'язку між апаратними засобами ІС; x_{12} — до зовнішніх ліній зв'язку ІС.

Оцінювання x_j проводиться відповідними експертними методами за шкалою: *IP* — «доступ неможливий», *LP* — «доступ малоймовірний», *MP* — «доступ імовірний», *HP* — «доступ відкритий повністю». Тобто, терм-множину вихідних змінних, у загальному випадку, можна подати у такому вигляді:

$$A = \{IP, LP, MP, HP\}. \quad (5)$$

Для того, щоб мати змогу оцінювати та обробляти лінгвістичні показники X_1, X_2, X_3, X_4 , формуємо шкалу з п'яти якісних термів [4, 7]. Терм-множина результату X_i записується у вигляді:

$$D = \{VH, H, M, L, VL\}, \quad (6)$$

де *VH* — «дуже високий» рівень загрози, *H* — «високий», *M* — «середній», *L* — «низький», *VL* — «дуже низький» рівень загрози.

Базу нечітких знань стосовно оцінювання рівня загрози стійкості захисту 1-го класу можна подати у вигляді:

Таблиця 1

Номер вихідної комбінації	Вихідні змінні												Вагові коефіцієнти w_l	Кінцеві змінні X_l
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}		
11	HP	HP	HP	HP	HP	HP	HP	HP	HP	HP	HP	HP	w_{111}	VH
12	HP	HP	HP	HP	HP	HP	HP	HP	HP	HP	HP	MP	w_{112}	
13	HP	HP	HP	HP	HP	HP	HP	HP	HP	HP	MP	HP	w_{113}	
14	HP	HP	HP	HP	HP	HP	HP	HP	HP	HP	MP	MP	w_{114}	
15	HP	HP	HP	HP	HP	HP	HP	HP	HP	MP	HP	HP	w_{115}	
...														
1k _{VH}	HP	HP	HP	HP	HP	HP	MP	MP	MP	MP	MP	MP	$w_{11k_{VH}}$	H
21	HP	HP	HP	HP	HP	MP	HP	HP	HP	HP	HP	HP	w_{121}	
22	HP	HP	HP	HP	HP	MP	HP	HP	HP	HP	HP	MP	w_{122}	
...														
2k _H	MP	MP	MP	MP	MP	MP	LP	LP	LP	LP	LP	LP	w_{12k_H}	H
31	MP	MP	MP	MP	MP	LP	MP	MP	MP	MP	MP	MP	w_{131}	M
...														
5k _{VL}	IP	IP	IP	IP	IP	IP	IP	IP	IP	IP	IP	IP	$w_{15k_{VL}}$	VL

Номер вихідної комбінації змінних $x_1, x_2, \dots, x_{12}$ подається у вигляді $n_i n_j$, де n_i відповідає номеру кінцевої змінної $X_i = d_i$ з множини (6), $n_i = \overline{1, 5}$; n_j — номер комбінації вихідних змінних $x_1, x_2, \dots, x_{12}$ для відповідного значення кінцевої змінної $X_i = d_i$ з множини (6), $n_j = \overline{1, k_{d_i}}$.

Систему нечітких знань для опису моделі оцінювання рівня загрози стійкості захисту 1-го класу можна записати у вигляді:

$$\mu_1^{d_l}(x_1, x_2, \dots, x_{12}) = \bigvee_{k_{d_l}} \left(w_{1m} \left[\bigwedge_{j=1}^{12} \mu_1^{a_p}(x_j) \right] \right), \quad (7)$$

де $\mu_1^{d_l}(x_1, x_2, \dots, x_{12})$ — функція належності вектора вихідних змінних $(x_1, x_2, \dots, x_{12})$ значенню кінцевої змінної $X_1 = d_l$ з множини (6); k_{d_l} — кількість комбінацій значень змінних, для яких кінцева змінна приймає значення d_l ; w_{1m} — ваговий коефіцієнт

для відповідної m -ї комбінації; $\mu_1^{a_p}(x_j)$ — функція належності вихідної змінної x_j до нечіткого терму a_p ($a_p \in A$ за (5)).

Систему нечітких знань для опису моделі оцінювання рівня загрози стійкості захисту i -го класу можна записати у вигляді:

$$\mu_i^{d_l}(x_{ij}) = \bigvee_{k_{d_l}} \left(w_{im} \left[\bigwedge_{j=1}^{12} \mu_i^{a_p}(x_{ij}) \right] \right). \quad (8)$$

Матимемо на увазі, що для кожного з класів стійкості захисту ІС формується власний набір показників (1) — (4). Тобто, для опису рівнів загрози стійкості захисту ІС певного класу певні показники X_j можуть бути відсутні.

Вагові коефіцієнти w_{im} характеризують впевненість експертів у кожному вибраному ними для прийняття рішень конкретному правилі [7]. Для узгодження та агрегації вагових коефіцієнтів на підставі оцінок експертів можна використовувати метод відшукування матриці порівнянь (медіани Кемені) або метод аналізу ієрархій за Сааті [8].

Для опису загального рівня загрози інформаційній системі сформуємо базу нечітких знань:

Таблиця 2

Номер вихідної комбінації	Вихідні змінні				Вагові коефіцієнти v	Кінцева змінна Y
	X_1	X_2	X_3	X_4		
11	VH	VH	VH	VH	v_{11}	VH
12	VH	VH	VH	H	v_{12}	
13	VH	VH	H	VH	v_{13}	
14	VH	VH	H	H	v_{14}	
...						
$4n$	VL	VL	VL	VL	v_{4n}	VL

Математична форма запису вирішального правила для визначення загрози рівня d_l інформаційній системі матиме вигляд:

$$\mu^{f_l}(X_1, X_2, X_3, X_4) = \bigvee_{k_{f_l}} \left(v_{s_{f_l}m} \left[\bigwedge_{j=1}^4 \mu_j^{d_{p_j}}(X_j) \right] \right), \quad (9)$$

де $\mu^{f_l}(X_1, X_2, X_3, X_4)$ — функція належності вектора вихідних змінних (X_1, X_2, X_3, X_4) значенню кінцевої змінної $Y=f_l$ з множини $F = \{VH, H, M, L, VL\}$; k_{f_l} — кількість комбінацій значень змінних (X_1, X_2, X_3, X_4) , для яких кінцева змінна приймає значення f_l ; $v_{s_{f_l}m}$ — ваговий коефіцієнт для відповідної m -ї комбінації; $\mu_{f_l}^{d_{p_j}}(X_j)$ — функція належності вихідної змінної X_j до нечіткого терму d_{p_j} ($d_{p_j} \in D$ за (6)) і вона подається в (8).

IV. Висновки

Грунтуючись на результатах проведеної класифікації загроз активам інформаційної системи, можна реалізувати систему побудови функцій належності термів лінгвістичних змінних (критеріїв, альтернатив та наслідків) та застосувати апарат нечіткого математичного програмування.

Отже, ми формуємо необхідну базу знань з використанням експертних даних та виводимо систему нечітких логічних рівнянь. Даний підхід дозволяє формувати модель оцінювання рівня загроз інформаційній системі внаслідок впливу чи дії порушників безпеки інформаційної системи.

Література

1. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник / За ред. С.Г.Лаптева. — К.: Європ. ун-т, 2001. — 321 с.
2. Jack A. Jones. An Introduction to FAIR. — Trustees of Norwich University, 2005.
3. Л. Заде. Понятие лингвистической переменной и ее применение к принятию приближенных решений. — М.: Мир, 1976.
4. Лунаев В.В. Методы обеспечения качества крупномасштабных программных средств. — М.: РФФИ; СИНТЕГ, 2003.
5. Лунаев В.В. Функциональная безопасность программных средств. — М.: СИНТЕГ, 2004.
6. Матвійчук А.В. Моделювання економічних процесів із застосування методів нечіткої логіки: Монографія. — К.: КНЕУ, 2007. — 264 с.
7. Вітлінський В.В., Великоіваненко Г.І. Ризикологія в економіці та підприємстві: Монографія. — К.: КНЕУ, 2004. — 480 с.

Стаття надійшла до редакції 29.12.08 р.