УДК 303.131.7

Г. В. Мельник, асистент кафедри прикладної математики,
Чернівецький національний університет
ім. Юрія Федьковича

ОЦІНЮВАННЯ ВЕЛИЧИНИ МОЖЛИВИХ ВТРАТ ІНФОРМАЦІЙНИХ АКТИВІВ

АНОТАЦІЯ. У даній статті запропоновано лінгвістичний підхід до моделювання величини можливих втрат інформаційних активів. Побудовано формалізований опис моделі визначення можливих втрат активів інформаційної системи на підґрунті нечіткої логіки.

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

КЛЮЧОВІ СЛОВА. Інформаційні ризики, інформаційний актив, рівень загроз, рівень вразливості системи, форми втрат інформаційних активів, фактори втрат інформаційних активів, лінгвістичний критерій, функція належності, нечіткі терми, нечітка множина.

Вступ. Питання визначення величини можливих втрат внаслідок впливу агента ризику на інформаційну систему є найскладнішим в аналізі ризиків. У низці випадків системні аналітики або виключають з розгляду втрати загалом і беруть до уваги тільки можливість найгірших наслідків дії загрози, або намагаються проводити точні розрахунки та обчислення величини можливих втрат. Виключення втрат з аналізу взагалі означає, що аналітики уникають розгляду ризиків, оскільки, за означенням, інформаційний ризик містить компоненту втрат. Позиціонування уваги тільки на найгірших наслідках дії агенту загрози усуває з аналізу елементи імовірності, оскільки, зокрема, ризик є результатом імовірності за означенням. З іншого боку, особи, що приймають рішення в загальному вимагають тільки імовірну величину втрат. Досвід аналізу інших видів ризиків (інвестиційний, маркетинговий та ін..) привчив їх, що фактичні втрати не можуть бути передбачені жодними точними розрахунками. [3].

Є кілька причин, які викликають труднощі вимірювання можливих втрат:

— складність встановлення точної оцінки вартості інформаційного активу;

— активи в загальному мають більше ніж одну характеристику для оцінювання;

— втрати можуть набувати різних форм;

— єдина подія може мати наслідки в кількох формах втрат;

— між різними формами втрат існує комплексний та систематичний взаємозв'язок;

— величину можливих втрат визначає множина факторів.

Вивчення оточення інформаційних ризиків ускладнюється недостатнім накопиченням історичних даних про величину втрат. Більшість організацій не проводять аналіз втрат після настання події та обмежуються «легким заповненням» метрик ризику (людино-години, втрати апаратного чи програмного забезпечення). До того ж, без стандартного підходу до вимірювання та оцінювання важко нормалізувати дані, що були отримані від різних організацій.

Втрати активів потенційно походять від тих вартості та зобов'язань, які вони мають в організації. Наприклад, інформація про покупця забезпечується оцінкою її ролі в отриманні доходу для комерційної організації. Та ж сама інформація також може бути цінною для організації, що законно захищає її, або покупець очікує, що інформація про нього буде належним чином захищена [3].

Факторний аналіз інформаційних ризиків визначає шість форм втрат:

1) *продуктивність* — зниження спроможності організації генерувати первинну пропозицію (прибуток, товари, послуги та ін.);

2) *реакція* – витрати, що пов'язані з управлінням подіями втрат (можлива відповідь на дії агенту загрози);

3) *заміна* — внутрішня оцінка активу. Типово представлена у вигляді капітальних витрат, що пов'язані з заміною втрачених або пошкоджених активів (відновлення обладнання, придбання та заміна комп'ютера та ін.);

4) *штрафи* та *покарання* — карні та адміністративні стягнення щодо організації;

5) *перевага конкурентів* — втрати, що призводять до зниження конкурентоспроможності організації. Це втрати активів, які забезпечують стійкість організації серед конкурентів — комерційні таємниці, плани та ін.;

6) *репутація* — втрати, що пов'язані із зовнішнім сприйняттям організації, як некомпетентної, кримінальної чи неетичної.

Всі фактори втрат мають зони впливу в межах однієї з наступних трьох категорій – активи, організація та оточення. Активи відносяться до первинних категорій, організація та оточення — до вторинних [1—3].

При розгляді власне втрат активів ключову роль як у походженні, так і у величині втрати відіграють вартість/відповідальність активу. Надалі визначимо вартість/відповідальність як:

— критична — характеристики активу стосуються продуктивності організації. Наприклад, знищення бази даних організації ведуть до значної втрати прибутку;

— вартісна — стосується внутрішньої вартості активу, тобто вартість заміни на подібний актив;

— чутлива — збитки, що можуть бути заподіяні ненавмисним розголошенням комерційної таємниці організації.

Обсяг активу визначається з тієї умови, що чим більше активів підлягатимуть під впливу ризику, тим більша величина можливих втрат для всієї організації.

Нагадаємо, що вторинними факторами втрат є організаційні та зовнішні характеристики оточення, що впливають на природу та рівень втрат.

Виділяють наступні основні організаційні фактори втрат [3—5]: *час* виникнення події; *належна старанність* характеризується рівнем відповідальності організації у випадку виникнення події загрози; *реакція* демонструє наскільки ефективно організація відповідає на подію загрози.

Зовнішні фактори втрат розкладаються на категорії: виявлення події загрози ззовні; юридичний базис – адміністративна, кримінальна та господарська відповідальність; конкуренти; засоби масової інформації; зовнішні учасники капіталу [3].

Постановка завдання. Вичерпний кількісний аналіз можливих втрат не завжди можливий через нестачу інформації про систему або діяльність, що аналізується, відсутність або нестачу даних про відмови, впливи людського фактора. За таких обставин може виявитися ефективним порівняльне кількісне або якісне ранжування ризику фахівцями, які є добре інформованими в даній області і системах.

Автор пропонує розглянути задачу побудови математичної моделі оцінювання можливих втрат інформаційних активів на етапі створення інформаційної системи. У цьому випадку можливо визначитися з факторами та формами втрат інформаційних активів внаслідок впливу інформаційних ризиків на підставі вищенаведеного факторного аналізу можливих втрат. Автор пропонує застосувати нечіткий лінгвістичний підхід до моделювання оцінювання можливих втрат інформаційних активів.

Результати. Для моделювання оцінювання можливої величини втрат унаслідок дії агента загрози розглянемо тільки первинні фактори втрат, що лежать у площині вартості та обсягу інформаційного активу. Сформулюємо формалізований підхід до аналізу рівня загроз і вразливості інформаційної системи з використанням нечітких описів [6, 7].

Система містить набір інформаційних активів:

$$S = s(C_1, C_2, ..., C_n), \tag{1}$$

де C_i — *i*-тий інформаційний актив. Величину втрати P_i, $i = \overline{1, n}$, *i*-го інформаційного активу пропонується характеризувати за факторами [3]: X_{i1} — продуктивність, X_{i2} — внутрішні витрати (реакція), X_{i3} — вартість заміни активу, X_{i4} — штрафи та санкції, X_{i5} — втрати, що призводять до зниження конкурентоспроможності організації, X_{i6} — репутація організації.

Оцінювання фактору X_{ij}, $j = \overline{1, 6}$, проводиться експертом за шкалою: *VH* — «втрата дуже велика», *H* — «втрата велика», *M* — «втрата середня», *L* — «втрата мала», *VL* — «втрата дуже мала». Тобто, терм-множина вхідних змінних у загальному вигляді представляється у вигляді:

$$A = \{ VH, H, M, L, VL \}. \tag{2}$$

Для того, щоб мати змогу оцінювати та обробляти лінгвістичні показники X_i формуємо шкалу з шести якісних термів [6, 7]: *Sv* — «сувора», *H* — «висока», *Sg* — «суттєва», *M* — «середня», *L* — «низька», *VL* — «дуже низька» величина втрати у відповідних грошових одиницях відносно бюджету проекту інформаційної системи. А терм-множина вихідної змінної P_i записується у вигляді:

$$D = \{ Sv, H, Sg, M, L, VL \}. \tag{3}$$

Базу нечітких знань стосовно величини втрати *i*-го інформаційного активу можна подати у вигляді (табл. 1).

Таблиця 1

Номер вхідної комбінації	Вхідні змінні						Вагові коефіцієнти w_i	Вихідна змінна P_i
	X_{i1}	X_{i2}	X_{i3}	X_{i4}	X_{i5}	X_{i6}		
11	*VH*	*VH*	*VH*	*VH*	*VH*	*VH*	w_{i11}	*Sv*
12	*VH*	*VH*	*VH*	*VH*	*VH*	*H*	w_{i12}	
13	*VH*	*VH*	*VH*	*VH*	*H*	*VH*	w_{i13}	
14	*VH*	*VH*	*VH*	*VH*	*H*	*H*	w_{i14}	
15	*VH*	*VH*	*VH*	*H*	*VH*	*VH*	w_{i15}	
…								
$1k_{Sv}$	*VH*	*VH*	*VH*	*H*	*H*	*H*	$w_{i1k_{Sv}}$	
21	*VH*	*VH*	*H*	*VH*	*VH*	*VH*	w_{i21}	*H*
22	*VH*	*VH*	*H*	*VH*	*VH*	*H*	w_{i22}	
…								
$2k_H$	*H*	*H*	*H*	*M*	*M*	*M*	w_{i2k_H}	
31	*H*	*H*	*M*	*H*	*H*	*H*	w_{i31}	*M*
…								
$6k_{VL}$	*VL*	*VL*	*VL*	*VL*	*VL*	*VL*	$w_{i6k_{VL}}$	*VL*

Номер вхідної комбінації змінних $X_{i1}, X_{i2},\ldots,X_{i6}$ подається у вигляді $n_l n_j$, де n_l відповідає номеру вихідної змінної $P_i = d_i$ з множини (3), $n_l = \overline{1,5}$; n_j — номер комбінації вхідних змінних $X_{i1}, X_{i2},\ldots,X_{i6}$ для відповідного значення вихідної змінної $P_i = d_i$ з множини (3), $n_j = \overline{1,k_{d_i}}$.

Систему нечітких знань для опису моделі оцінювання величини втрат *і-го* інформаційного активу можна записати у вигляді:

$$\mu_i^{d_l}(X_{i1},X_{i2},\ldots,X_{i6}) = \bigvee_{k_{d_l}} \left(w_{im} \left[\bigwedge_{j=1}^{6} \mu_i^{a_q}(X_{ij}) \right] \right), \qquad (4)$$

де $\mu_i^{d_l}(X_{i1},X_{i2},\ldots,X_{i6})$ — функція належності вектора вхідних змінних $(X_{i1},X_{i2},\ldots,X_{i6})$ значенню вихідної змінної $P_i = d_l$ з

множини (3); k_{d_l} — кількість комбінацій значень змінних $(X_{i1}, X_{i2}, \ldots, X_{i6})$, для яких вихідна змінна приймає значення d_l; w_{im} — ваговий коефіцієнт для відповідної m-ї комбінації; $\mu_i^{a_q}(X_{ij})$ — функція належності вхідної змінної X_{ij} до нечіткого терму a_q з множини (2).

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

Спираючись на результати проведеного факторного аналізу величини втрат інформаційного активу внаслідок дії загрози активу можна реалізувати систему побудови функцій належності термів лінгвістичних змінних (критеріїв, альтернатив та наслідків) та застосувати апарат нечіткого математичного програмування.

Таким чином, ми формуємо базу знань з використанням експертних даних та виводимо систему нечітких логічних рівнянь. Даний підхід дозволяє формувати модель оцінювання величини втрат інформаційних активів у системі внаслідок впливу чи дії порушників безпеки інформаційної системи.

Результат аналізу величини можливих втрат та частоти подій виникнення загрози інформаційному активу та виникнення подій втрат внаслідок дії інформаційних ризиків системи зводиться до таблиці відповідно по кожному з можливих ризиків:

Ризик

Величина можливих втрат						
	Sv	*H*	*H*	*C*	*C*	*C*
	H	*M*	*H*	*H*	*C*	*C*
	Sg	*M*	*M*	*H*	*H*	*C*
	M	*L*	*M*	*M*	*H*	*H*
	L	*L*	*L*	*M*	*M*	*H*
	VL	*L*	*L*	*L*	*M*	*M*
		VL	*L*	*M*	*H*	*VH*

Частота події втрат

де *C* — «критичний», *H* — «високий», *M* — «середній», *L* — «низький».

Подібним чином формується база знань з використанням експертних даних та виводиться система нечітких логічних рівнянь. Такий підхід дозволяє формувати модель аналізу інформаційних ризиків із врахуванням специфіки конкретного підприємства, для якого проектується інформаційна система.

Висновки. Результатом представленої технології оцінювання можливих втрат інформаційних активів унаслідок дії інформаційних ризиків на систему є лінгвістичний опис величини втрат активів унаслідок впливу агентів загрози. Розроблено підхід до аналізу та оцінки величини втрат інформаційних активів із використанням апарату нечіткої логіки, що дозволяє формувати модель не тільки з можливістю адаптації її до конкретної інформаційної системи, але й з урахуванням переоцінки ризику надалі. Подібна модель має властивості гнучкості та адаптивності, тонкого налаштування у відповідності до одержаної бази знань.

Література

1. *Липаев В. В.* Методы обеспечение качества крупномасштабных программных средств. — М.: РФФИ. СИНТЕГ, 2003.
2. *Липаев В. В.* Функциональная безопасность программных средств. — М.: СИНТЕГ, 2004.
3. *Jack A.* Jones. An Introduction to FAIR. — Trustees of Norwich University, 2005.
4. Computer Security Handbook, 4th Edition Editors: Seymour Bosworth, M. E. Kabay ISBN: 0-471-41258-9, 1224 Pages, March 2002.
5. Information Systems Security Association на сайте http://www.issa.org/.
6. *Заде Л.* Понятие лингвистической переменной и ее применение к принятию приближенных решений. — М.: Мир, 1976.
7. *Матвійчук А. В.* Моделювання економічних процесів із застосуванням методів нечіткої логіки: Монографія. — К.: КНЕУ, 2007. — 264 с.
8. *Вітлінський В. В., Великоіваненко Г. І.* Ризикологія в економіці та підприємництві: Монографія. — К.: КНЕУ, 2004. — 480 с.

Статтю подано до редакції 30.06.10 р.