УДК004.413.4

Д. О. Сікорський,
аспірант, Київський національний університет імені Тараса Шевченка, м. Київ

ХАРАКТЕРИСТИКА МЕТОДІВ І ЗАСОБІВ АНАЛІЗУ Й УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

D. Sikorskyi,
post-graduate student, Department of Economic Cybernetics, Taras Shevchenko Kyiv National University, Kyiv

METHODS AND TOOLS OF INFORMATION RISKS ANALYSIS

У статті розглянуто існуючі методики аналізу та управління інформаційними ризиками. Визначено необхідність проведення оцінки інформаційних ризиків у корпоративних інформаційних системах підприємств. Розроблено концептуальні положення щодо формування системи математичних моделей і методів управління інформаційними ризиками.

The paper studies methods of analysis and management of information risks. The necessity of evaluation of information risks in corporate information systems is defined. The study proposes conceptual principles as to formation of mathematic model system and methods of information risks management.

Ключові слова: інформаційна безпека, інформаційний ризик, корпоративна інформаційна система, лінгвістична змінна, лінгвістичний критерій, функція належності, нечітка множина.
Key words: information security, information risk, corporate information system, linguistic variable, linguistic criteria, membership function, fuzzy set.

ПОСТАНОВКА ПРОБЛЕМИ

У сучасних умовах господарювання вітчизняні підприємства приділяють значну увагу питанням інформаційної безпеки. Основою для побудови системи управління інформаційною безпекоюєаналіз інформаційних ризиків, що на практиці зводиться до опису загроз та вразливостей корпоративної інформаційної системи (КІС). Розповсюдженість такого підходу зумовлена, перш за все, тим, що підприємства мають схожі загрози безпеці, оскільки у своїй діяльності використовують однакові операційні системи і системні механізми, а їх бізнес-додатки побудовані на принципах подібності. Проте аналіз ризиків для кожного підприємства має бути індивідуальним та визначати розмір можливих збитків від інформаційних ризиків.

Чіткої методики кількісного аналізу інформаційних ризиків поки ще не вироблено. Це пов'язано з відсутністю достатнього об'єму статистичних даних. На жаль, більшість довідкових даних спирається на закордонний досвід і тому не завжди вони можуть бути застосовані до українських реалій. Тому поширеним залишається якісний аналіз інформаційних ризиків, коли за відсутності точних даних, значення параметрів встановлює експерт.

Зазвичайоцінюються такі фактори, якімовірність виникнення події та величини можливих збитків. Вважається, що ризик тим більший, чим більша ймовірність виникнення події та величина збитків. Якщо змінні є кількісними величинами, величина ризику — це оцінювання математичного очікування втрат. Однак дослідження проблеми показують, що більшість з описаних параметрів оцінюється на основі думки експерта. Це пов'язано з тим, що кількісна оцінка імовірності реалізації загрози ускладнена, зважаючи на відносну новизну інформаційних технологій, і, як наслідок, відсутність достатньої кількості статистичних даних.

АНАЛІЗОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Управлінню ризиками приділяється достатньо уваги в закордонних і вітчизняних публікаціях, зокрема в теорію управління ризиками значний внесок зробили такі вчені: В. Вітлінський, П. Верченко, В. Завгородний, Л. Заде, В. Кульба, В. Ліпаєв, А. Матвійчук, А. Ротштейнта інші. Проте залишається невирішеними проблеми, пов'язані з відсутністю чітких методик кількісного оцінювання інформаційних ризиків, що забезпечували б системний підхід до управління інформаційною безпекою підприємств.

МЕТА СТАТТІ

Метою статті є теоретичне дослідження основних методів і засобів аналізу й управління інформаційними ризиками вітчизняних підприємств.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Управлінням інформаційними ризиками — це система узгоджених дій, операцій та процедур, що виконуються персоналом КІС з метою мінімізації витрат на протидію інформаційним ризикам та усунення їх наслідків [2]. Метою управління інформаційними ризиками є зниження обсягів можливих збитків внаслідок реалізації цих ризиків та мінімізація суми витрат підприємства спрямованих на протидію інформаційним ризикам.

Управління інформаційними ризиками передбачає розв'язання таких задач [2, 4]: 1) аналіз та оцінювання величини ризиків; 2) вироблення політики управління інформаційними ризиками; 3) створення системи управління інформаційними ризиками; 4) уникнення причин і зменшення впливу чинників значущих ризиків; 5) створення механізмів своєчасного виявлення та зниження обсягів збитків; 6) зменшення негативного впливу від ризиків; 7) оцінювання обсягів можливих збитків; 8) своєчасна ліквідація наслідків несприятливих подій; 9) аналіз дієвості системи управління інформаційними ризиками; 10) вдосконалення системи управління інформаційними ризиками.

На рисунку 1наведено спрощену структурну схему управління інформаційними ризиками КІС, на якій стрілками показані інформаційні та фінансові потоки.

Найважливіший елемент управління інформаційними ризиками — аудит безпеки, що включає в себе аналіз та оцінювання інформаційних ризиків. Слід зазначити, що на сьогоднішній день існують різноманітні та складні за своєю структурою КІС, для яких неможливо дібрати конкретну методику оцінювання ризиків. Тому для отримання точних задовільних результатів оцінювання необхідно використовувати комплексний підхід до аналізу та управління інформаційними ризиками.

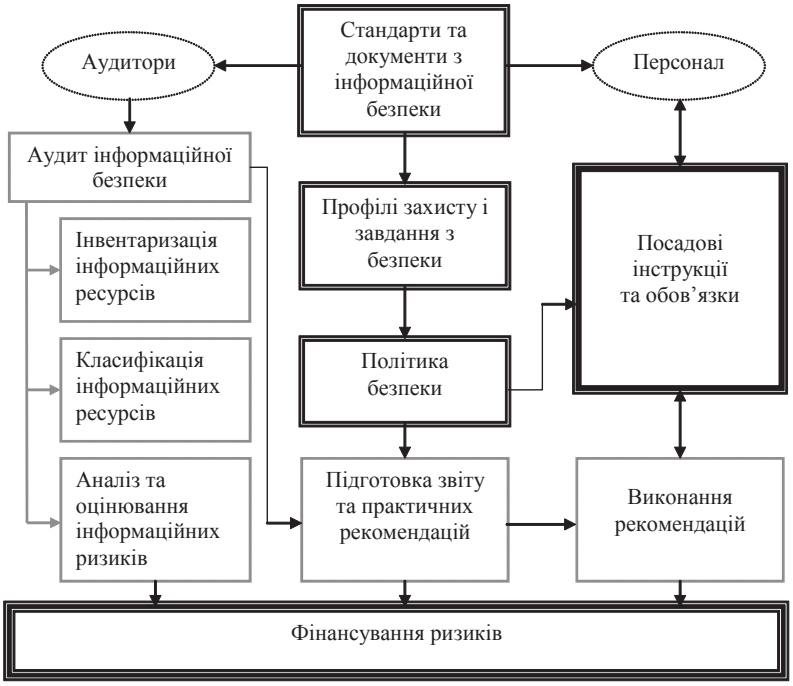

Рис. 1. Структурна схема управління інформаційнимиризиками

КІС є складною людино-машинною чи соціотехнічною системою, що включає в себе інформаційну систему підприємства. Для дослідження таких систем використовуються різні типи моделей.

Функціонування КІС здійснюється в умовах протиборства підприємства як соціотехнічної системи, з одного боку, і конкурентів, зловмисників, негативних впливів природи та інших об'єктів і явищ, з іншого боку. Моделювання таких конфліктних ситуацій за участю людини здійснюється за допомогою теорії ігор. Теорія ігор досить широко використовується при моделюванні економічних процесів і систем [1].

Одним з розділів математики, що знайшов широке застосування в моделюванні складних систем, є теорія множин. Розширити можливості класичної теорії множин дозволяє теорія нечітких множин [7]. При моделюванні складних систем доцільно використовувати апарат нечітких множин для розподілу об'єктів за підмножинами в умовах недостатньої інформації та випадковості процесів. Методи нечітких множин та нечіткої логіки дозволяють використовувати як кількісні, так і якісні оцінки, отримувати інтегральні показники. Вони найбільшою мірою підходять для роботи з експертними оцінками.

Великі можливості досліднику складних систем надає теорія графів [2]. Графи використовуються для опису структури системи, взаємодії об'єктів системи. Вони мають цілу низку переваг. Властивості графів можуть описуватися як в матричній формі, так і аналітичними виразами. Графи дозволяють досить просто масштабувати рівні розгляду об'єктів і процесів та моделювати не тільки статичні системи, але й динамічні процеси.

Мережі Петрі є одним з найбільш перспективних розділів теорії графів. Вони володіють низкою властивостей, що дозволяють вважати мережі Петрі придатними для моделювання процесу управління інформаційними ризиками. Поряд з класичними мережами Петрі розроблені різні модифікації мереж [3]: мережі Петрі з інгібіторними зв'язками, імовірнісні, тимчасові та комбіновані.

Доведено, що мережі Петрі з інгібіторними зв'язками еквівалентні машині Тьюрінга, і з їх допомогою можна задати довільний алгоритм [3]. Головною перевагою імовірнісних мереж Петрі є можливість моделювання як технічних, так і людино-машинних (соціотехнічних) систем. З їх допомогою досить просто моделювати як процес передачі інформації по каналах зв'язку, так і процес подолання зловмисником системи захисту комп'ютерної системи [2]. У мережах Петрі допускається агрегування об'єктів і процесів. Це дозволяє за необхідності в рамках однієї моделі описувати різні об'єкти або процеси в різних масштабах.

При роботі з нестатистичною інформацією можуть використовуватися нечіткі мережі Петрі [3]. Поширення набули нечіткі часові мережі Петрі для аналізу динамічних процесів, а також нечіткі мережі Петрі, що адаптовані до отримання нечітких висновків.

Пропонуємо розробити механізм отримання оцінок ризиків, який дозволяв би замінити наближені табличні методи грубої оцінки ризиків сучасним математичним інструментарієм. Формування системи математичних моделей і методів управління інформаційними ризиками грунтується на таких концептуальних положеннях:

— розроблення і застосування методів ідентифікації інформаційних ресурсів (активів) підприємства, які можуть стати об'єктами інформаційних ризиків та загроз цим ресурсам;

— розроблення і застосування моделей кількісного аналізу й оцінювання чинників (вразливості, дієвості засобів захисту тощо) та загального рівня інформаційних ризиків із застосуванням інструментарію нечіткої логіки;

— розроблення математичних моделей щодо економічного обгрунтування ефективності використання механізмів (засобів) для зниження ступеня інформаційних ризиків, забезпечення відповідності функціональним критеріям захищеності інформації (конфіденційності, цілісності, доступності, спостережності) та зниження пов'язаних з цим втрат (збитків, шкоди) підприємству на основі нечітких ієрархічних систем та нечітких часових мереж Петрі з інгібіторними зв'язками.

Розглянемо більш детально питання побудови моделей кількісного аналізу й оцінювання чинників та загального рівня інформаційних ризиків із застосуванням інструментарію нечіткої логіки. Лінгвістичні (нечіткі) описи в структурі методу аналізу складних систем з'являються в зв'язку із невпевненістю експерта, що виникає в ході різного роду оцінювання чи класифікацій. Наприклад, експерт не може чітко провести межу між високим чи середнім, середнім чи низьким значенням параметру [5].

Експерт утворює лінгвістичну змінну зі своєю терм-множиною значень. Так, для лінгвістичної змінної "Рівень інформаційного ризику" множина значень може бути сформована з термів ("Критичний", "Високий", "Середній", "Низький"). Щоб конструктивно описати лінгвістичну змінну, експерт вибирає відповідну їй кількісну ознаку — функцію належності — сконструйований визначеним чином показник зростання рівня інформаційного ризику, що приймає значення від 0 до 1. Таким чином, зміст лінгвістичної змінної χ характеризується обраною мірою — так званою функцією належності $\mu : U \to [0, 1]$, що кожному елементу u універсальної множини U ставить у відповідність значення сумісності цього елемента з χ [5]. Метою такого опису є введення основних формалізмів, необхідних для визначення нечітких баз знань, які є носієм експертної інформації [6].

Розглядається об'єкт з входами та одним виходом виду:

$$y = f_y(x_1, x_2, ..., x_n) \quad (1),$$

де y — вихідна змінна; $x_1, x_2, ..., x_n$ — вхідні змінні.

Змінні $x_1, x_2, ..., x_n$ і y можуть бути як кількісним, так і якісними. Для кількісних змінних покладають відомими області зміни:

$$U_i = \left[\underline{x_i}, \overline{x_i}\right],\ i = \overline{1,n} \quad (2),$$

$$Y = \left[\underline{y}, \overline{y}\right] \quad (3),$$

де $\underline{x_i}, (\overline{x_i})$ — нижнє (верхнє) значення вхідних змінних $x_i,\ i = \overline{1,n}$; $\underline{y}\ (\overline{y})$ — нижнє (верхнє) значення вихідної змінної y.

Для якісних змінних $x_1, x_2, ..., x_n$ і y покладають відомими множини всіх можливих значень:

$$U_i = \left\{v_i^1, v_i^2, ..., v_i^{q_i}\right\},\ i = \overline{1,n} \quad (4),$$

$$Y = \left\{y^1, y^2, ..., y^{q_m}\right\} \quad (5),$$

де $v_i^1\ (v_i^{q_i})$ — бальна оцінка, що відповідає найменшому (найбільшому) значенню вхідної змінної x_i ; $y^1\ (y^{q_m})$ — бальна оцінка, що відповідає найменшому (найбільшому) значенню вихідної змінної y ; $q_i,\ i = \overline{1,n}$ і q_m — потужності множин (4) та (5) відповідно, причому в загальному випадку $q_1 \neq q_2 \neq ... \neq q_n \neq q_m$.

Нехай $X^* = \langle x_1^*, x_2^*, ..., x_n^* \rangle$ — вектор фіксованих значень вхідних змінних об'єкту, який розглядається, де $x_i^* \in U_i,\ i = 1,n$. Задача прийняття рішення полягає в тому, щоб на основі інформації про вектор входів X^* визначити вихід $y^* \in Y$. Необхідною умовою формального розв'язку такої задачі є наявність залежності (1). Для встановлення такої залежності розглядають вхідні змінні $x_i,\ i = \overline{1,n}$ та вихідну змінну y як лінгвістичні змінні, що задані на універсальних множинах (2), (3) або (4), (5).

Для оцінювання лінгвістичних змінних $x_i,\ i = \overline{1,n}$ та y використовують якісні терми з наступних терм-множин:

$A_i = \left\{a_i^1, a_i^2, ..., a_i^{l_i}\right\}$ — терм-множина змінної $x_i,\ i = \overline{1,n}$;

$D = \{d_1, d_2, ..., d_m\}$ — терм-множина змінної y;

де a_i^p — p-й лінгвістичний терм змінної $x_i,\ i = \overline{1,n},\ p = \overline{1,l_i}$; d_j — j -й лінгвістичний терм змінної y ; m — кількість різних рішень в області, що розглядається.

Потужності терм-множини $A_i,\ i = \overline{1,n}$ в загальному випадку можуть бути різними, тобто $l_1 \neq l_2 \neq ... \neq l_n$. Назви окремих термів $a_i^1, a_i^2, ..., a_i^{l_i}$ можуть відрізнятися для різних лінгвістичних змінних $x_i,\ i = \overline{1,n}$.

Лінгвістичні терми $a_i^p \in A_i$ та $d_j \in D,\ p = \overline{1,l_i},\ i = \overline{1,n},\ j = \overline{1,m}$ розглядають як нечіткі множини, що задані на універсальних множинах U_i та Y та визначені співвідношеннями (2) — (5).

У випадку кількісних змінних $x_i,\ i = \overline{1,n}$ та y , нечіткі множини a_i^p та d_j визначають співвідношеннями:

$$a_i^p = \int_{\underline{x_i}}^{\overline{x_i}} \mu^{a_i^p}(x_i) / x_i \quad (6),$$

$$d_j = \int_{\underline{d}}^{d} \mu^{d_j}(d) / d \quad (7),$$

де $\mu^{a_i^p}(x_i)$ — функція належності значення вхідної змінної $x_i \in \left[\underline{x_i}, \overline{x_i}\right]$ до терму $a_i^p \in A_i,\ p = \overline{1,l_i},\ i = \overline{1,n}$; $\mu^{d_j}(d)$ — функція належності значення вихідної змінної $y \in \left[\underline{y}, \overline{y}\right]$ до терму-рішення $d_j \in D$, $j = \overline{1,m}$.

У випадку якісних $x_i,\ i = \overline{1,n}$ та y , нечіткі множини a_i^p та d_j визначають наступним чином:

$$a_i^p = \sum_{k=1}^{q_i} \mu^{a_i^p}(v_i^k) / v_i^k \quad (8),$$

$$d_j = \sum_{r=1}^{q_m} \mu^{d_j}(y^r) / y^r \quad (9),$$

де $\mu^{a_i^p}(v_i^k)$ — ступінь належності елемента $v_i^k \in U_i$ до терму $a_i^p \in A_i$, $p = \overline{1,l_i}$, $k = \overline{1,q_i}$, $i = \overline{1,n}$; $\mu^{d_j}(y^r)$ — ступінь належності елемента $y^r \in Y$ до терму-рішенню $d_j \in D$, $j = \overline{1,m}$.

U_i та Y визначаються співвідношеннями (4) та (5).

Слід зазначити, що у співвідношеннях (6) — (9) знаки інтегралу і суми означають об'єднання пар $\mu(u) / u$.

Даний етап побудови нечіткої моделі, на якому визначаються лінгвістичні оцінки змінних та необхідні для їх формалізації функції належності, отримав у літературі з нечіткої логіки назву "фазифікація змінних".

ВИСНОВКИ

Невід'ємною частиною ефективного управління будь-яким підприємством є управління інформаційними ризиками, що здійснюється не тільки за наявності статистичної інформації, але і в умовах застосування нестатистичної інформації. Управління інформаційними ризиками має здійснюватися на основі розроблення та застосування: методів ідентифікації інформаційних ресурсів підприємства; моделей кількісного аналізу й оцінювання чинників та загального рівня інформаційних ризиків із застосуванням інструментарію нечіткої логіки; математичних моделей щодо економічного обгрунтування ефективності використання механізмів для зниження ступеня інформаційних ризиків, забезпечення відповідності функціональним критеріям захищеності інформації та зниження пов'язаних з цим збитків підприємству на основі нечітких ієрархічних систем та нечітких часових мереж Петрі з інгібіторними зв'язками.

Література:

1. Вітлінський В.В. Економічний ризик: ігрові моделі: навч. посібник / В.В. Вітлінський, П.І. Верченко, А.В. Сігал, Я.С. Наконечний. — К.: КНЕУ, 2002. — 446 с.
2. Завгородний В.И. Информационные риски и экономическая безопасность предприятия / В.И. Завгородний. — М.: Финакадемия, 2008. — 160 с.
3. Кульба В.В. Модифицированные сети Петри / В.В. Кульба, А.Г. Мамиконов, А.Р. Швецов. — М.: ИПУ, 1991. — 45 с.
4. Липаев В.В. Функциональная безопасность программных средств / В.В. Липаев. — М.: СИНТЕГ, 2004. — 348 с.
5. Матвійчук А.В. Моделювання економічних процесів із застосуванням методів нечіткої логіки / А.В. Матвійчук. — К.: КНЕУ, 2007. — 264 с.
6. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А.П. Ротштейн. — Винница: УНІВЕРСУМ-Вінниця, 1999. — 320 с.
7. Zadeh L.A. Fuzzy sets / L.A. Zadeh. — Information and Control, 1965. — № 8. — P. 338—353.

References:

1. Vitlins'kyj, V.V. Verchenko, P.I. Sihal, A.V. and Nakonechnyj, Ya.S. (2002), Ekonomichnyjryzyk: ihrovimodeli [Economicrisk: playingmodels], KNEU, Kyiv, Ukraine.
2. Zavgorodnij, V.I. (2008), Informacionnyeriski i jekonomicheskajabezo pasnost' predprijatija [Information risks and economic security], Finakademija, Moscow, Russia.
3. Kul'ba, V.V. Mamikonov, A.G. Shvecov, A.R. (1991), Modificirovannyeseti Petri [Modified Petri net], IPU, Moscow, Russia.
4. Lipaev, V.V. (2004), Funkcional'najabezopasnost' programmnyhsredstv [Functional safety of software], SINTEG, Moscow, Russia.
5. Matviichuk, A.V. (2007), Modeliuvannia ekonomichnykh protsesiv i zzastosuvanniam metodiv nechitkoilohiky [Modeling of Economic Processes Using Fuzzy Logic Methods], KNEU, Kyiv, Ukraine.
6. Rothstein, A.P. (1999), Yntellektual'nyetekhnolohyyydentyfykatsyy: nechetkyemnozhestva, henetycheskyealhorytmy, nejronnyesety [Intellectual Technology of Identification: fuzzy set, genetic algorithms, neural network], UNIVERSUM-Vinnitsa, Vinnitsa, Ukraine.
7. Zadeh, L.A. (1965), "Fuzzy sets", Information and Control, vol. 8, pp. 338—353.

Стаття надійшла до редакції 20.11.2015 р.