А. Лозовая, канд. экон. наук, доц.
Киевский национальный университет имени Тараса Шевченко, Киев, Украина

ИСПОЛЬЗОВАНИЕ ЭВРИСТИЧЕСКИХ МЕТОДОВ И ПРИЕМОВ ДЛЯ СТИМУЛИРОВАНИЯ КОЛЛЕКТИВНОГО ТВОРЧЕСТВА ПЕРСОНАЛА ПРЕДПРИЯТИЯ

В статье раскрывается проблема становления и развития эвристических методов стимулирования творческой активности персонала предприятия на основе анализа научных достижений и практического опыта. Предложен алгоритм формирования творческой команды работников и реализации творческого проекта. Проведен сравнительный анализ основных эвристических методов и приемов для фазы научных исследований и разработки.

Ключевые слова: эвристика, эвристические методы стимулирования творческой активности, инновационный процесс на предприятии, творческий проект, стимулирования творческой активности.

Bulletin of Taras Shevchenko National University of Kyiv. Economics, 2015, 6(171): 48-54
DOI: dx.doi.org/ 10.17721/1728-2667.2015/171-6/9
УДК [005.52:005.334:519.86]:334.784(043.3)
JEL C38

Г. Мельник, канд. екон. наук
Чернівецький національний університет імені Юрія Федьковича, Чернівці

МОДЕЛЬ ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНИХ РИЗИКІВ В КОРПОРАТИВНИХ СИСТЕМАХ

Проаналізовано особливості та світовий досвід інформаційного ризик-менеджменту. Обґрунтовано необхідність комплексного підходу до аналізу та управління інформаційними ризиками в корпоративних системах, в якому б із системних позицій розглядались усі складові якості і безпеки інформації, що впливають на ефективність використання засобів та механізмів захисту безпеки інформації в корпоративних інформаційних системах (КІС). Розроблено економіко-математичну модель із застосуванням теорії та інструментарію нечітких множин і нечіткої логіки, що дозволяє більш точно оцінювати ступінь інформаційних ризиків на підприємстві.

Ключові слова: інформаційний ризик, корпоративна інформаційна система, аналіз чинників інформаційних ризиків, вразливість, рівень загроз, дієвість засобів захисту інформації.

Вступ. Сучасні підприємства мають складну структуру, що зумовлена багатопрофільною діяльністю, територіальним розміщенням підрозділів, чисельними корпоративними зв'язками з партнерами. Корпоративними, зазвичай, називають системи управління підприємством, що враховують особливості структуризації та наявність окремих органів управління. Серед корпоративних систем виокремлюють організаційні, інформаційні, тощо. Більшість бізнес-функцій та управлінських процесів підприємств і організацій охоплюють корпоративні інформаційні системи (надалі КІС).

Впровадження нових інформаційних технологій завжди пов'язане з новими ризиками. Чим складнішою є структура корпоративної системи, тим вищим є ступінь ризику здійснення стосовно неї загроз: проникнення ззовні чи несанкціонований доступ зсередини підприємства, зокрема з метою фінансового шахрайства або розкриття комерційної таємниці, викривлення чи знищення інформації тощо. Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави.

Існуюча методологія інформаційного ризик-менеджменту не передбачає комплексного підходу до управління інформаційними ризиками в корпоративних системах і не дозволяє встановити взаємозв'язок інформаційних та інших видів економічних ризиків. Використання економіко-математичних моделей управління інформаційними ризиками не завжди узгоджене та зорієнтоване на досягнення кінцевого результату бізнес-процесів, що призводить до зниження ефективності управління ризиками всього підприємства.

Потребує належної уваги використання сучасних математичних методів в моделюванні процесу управління інформаційними ризиками. Можна дійти висновку, що, відповідно до цих об'єктивних вимог, зросла актуальність економіко-математичного моделювання процесів оцінювання та управління інформаційними ризиками в корпоративних системах.

Метою статті є розробка системи економіко-математичних моделей оцінювання загального рівня інформаційних ризиків в корпоративних системах. Предметом дослідження є методологія та інструментарій економіко-математичного моделювання у процесах управління інформаційними ризиками в корпоративних системах.

Аналіз останніх досліджень та публікацій. У науковій літературі, національних і міжнародних стандартах [1] приділяється велика увага проблемам управління ризиками, що пов'язані з використанням інформації в діяльності підприємств. Вчені Бернстайн П., Бланк І.А., Вітлінський В.В., Луман Н., Марковіц Г., Найт Ф.Х., Самуельсон П. та інші розробили загальні принципи та інструментарій управління економічними ризиками. Математичні методи та інструментарій економіко-математичного моделювання представлені в роботах Клейнера Г.Б., Кульби В.В., Матвійчука А.В. [2], Сігала А.В. та інших. Статистичні методи моделювання можуть використовуватися для вивчення інформаційних ризиків в комбінації з неформальними методами досліджень [2, 3]. Управління інформаційними ризиками в умовах невизначеності може здійснюватися з використанням методів м'яких обчислень, таких як інтервальний метод, нейронні мережі, генетичні алгоритми, а також нечіткі множини та нечітка логіка.

Інформаційні ризики як різновид економічних ризиків розглядаються, зокрема, в працях Вертузаєва М.С., Завгороднього В.І. [3], Ліпаєва В.В. [4]. Найбільш близьким до поняття "інформаційний ризик" є поняття "загроза безпеці інформації". Ліпаєв В.В. вкладає в поняття "інформаційний ризик" наступний зміст: це можлива подія, в результаті якої несанкціоновано знищується, спотворюється інформація, порушується її конфіденційність або доступність [4]. Причому частина авторів такого трактування інформаційного ризику під захистом інформації розуміють захист в основному від зловмисних дій.

Проблеми оцінювання якості інформації і надійності апаратних і програмних засобів розглядаються в працях Байхельта Ф., Зегжда П.Д., Муна С., Стенга Д.І., Франкена П. та інших. Стенг Д.І. ще більшою мірою звужує поняття інформаційного ризику [5] і розглядає в його межах тільки загрозу безпеці інформації в комп'ютерних системах. Прихильниками таких підходів до розуміння категорії "інформаційні ризики" є, як правило,

фахівці в галузі захисту інформації. Інша група фахівців під інформаційним ризиком розуміє можливість виникнення збитків, неотримання прибутку та інші негативні наслідки для підприємства. Прикладом одного з таких підходів може служити наступне визначення Мішеля Мура: "Інформаційні ризики – це небезпека виникнення збитків або шкоди в результаті застосування компанією інформаційних технологій. Іншими словами, інформаційні ризики пов'язані із створенням, передачею, зберіганням та використанням інформації за допомогою електронних носіїв та інших засобів зв'язку" [6]. Недоліком подібних визначень є нечітке окреслення об'єктів, ушкодження чи зміна властивостей яких внаслідок події, що обтяжена ризиком, призведуть до збитків. У наведеному визначенні з розгляду виключені інформаційні ризики, що можуть бути пов'язані з паперовим документообігом, з впливом зловмисників на інформаційні ресурси заходами шпигунства чи диверсій тощо.

Автори багатьох робіт, зокрема Мішель Мур [6] та Дж. Джонс [7], для детального аналізу джерела ризику пропонують спершу створити його модель. В залежності від мети дослідження та джерел ризиків обирається спосіб моделювання і рівень деталізації об'єктів та процесів.

Методологія дослідження. Корпоративна інформаційна система є складною людино-машинною чи соціотехнічною системою, що включає в свій склад інформаційну систему підприємства. Для дослідження таких систем використовуються різні типи моделей. Процес функціонування КІС підприємства 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.

Одним з розділів математики, що знайшли широке застосування в моделюванні складних систем, є теорія множин. Розширити можливості класичної теорії множин дозволяє теорія нечітких множин [2, 8, 9, 10]. При моделюванні складних систем доцільно використовувати апарат нечітких множин для розподілу об'єктів за підмножинами в умовах недостатньої інформації та випадковості процесів. При дослідженні інформаційних ризиків таке завдання стоїть, наприклад, при вирішенні задачі віднесення довільного ризику до множини значущих ризиків у конкретній корпоративній системі. 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.

Пропонується 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 ґрунтується на наступних 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 обґрунтування 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.

Результати. В іноземних методиках аналізу інформаційних ризиків використовується модель оцінювання ризику за трьома факторами: загроза, вразливість, величина можливих збитків. Виділяють чотири основні кроки аналізу інформаційних ризиків [7]:

I. Ідентифікація компонент:

1. інформаційних ресурсів (активів) компанії, що можуть бути об'єктом ризику. Згідно стандарту безпеки ISO/IEC 27001:2013 [1] інформаційний актив – це матеріальний чи нематеріальний об'єкт, який є інформацією або містить інформацію, використовується для зберігання чи обробки інформації, складає цінність для підприємства (організації);

2. можливих загроз (комбінації загроз) активу. Для управління ризиками необхідно ідентифікувати можливі небезпеки, які загрожують КІС. Такими можуть бути, наприклад, стихійне лихо, відключення електроживлення або атаки зловмисників з наслідками різного ступеню складності.

II. Оцінювання частоти подій можливих втрат внаслідок дії ризику:

- можливий рівень сили (Threat capability), з якою агенти загрози діятимуть на актив. Припускається, що деяка частина популяції агентів загрози є більш здатною до впливу на актив, інша – менш здатною [7]. Проводиться експертне оцінювання рівня загроз за набором показників, які характеризують можливість доступу порушника відповідного класу до інформаційних ресурсів за шкалою: *TC_VH* – "дуже високий" рівень загрози, *TC_H* – "високий", *TC_M* – "середній", *TC_L* – "низький", *TC_VL* – "дуже низький";
- очікувана дієвість засобів контролю (Control strength) впродовж відведеного часового інтервалу. Взявши за основу зорієнтованість на середню здатності агентів загрози, приймається базовий рівень ефективності контролю [7]. Для оцінювання використовується шкала: *CS_VH* – "дуже високий" рівень захисту, *CS_H* – "високий", *CS_M* – "середній", *CS_L* – "низький", *CS_VL* – "дуже низький";
- вразливість розглядається як результат впливу факторів можливого рівня сили загрози та дієвості засобів контролю [7] і оцінюється за шкалою: *V_VH* – "дуже високий" рівень вразливості, *V_H* – "високий", *V_M* – "середній", *V_L* – "низький", *V_VL* – "дуже низький". Приклад бази знань для оцінювання рівня вразливості приводиться в табл. 1.

Таблиця 1. **Оцінювання рівня вразливості корпоративної системи**

		Вразливість				
можливий рівень сили загрози	*TC_VH*	*V_VH*	*V_VH*	*V_VH*	*V_H*	*V_M*
	TC_H	*V_VH*	*V_VH*	*V_H*	*V_M*	*V_L*
	TC_M	*V_VH*	*V_H*	*V_M*	*V_L*	*V_VL*
	TC_L	*V_H*	*V_M*	*V_L*	*V_VL*	*V_VL*
	TC_VL	*V_M*	*V_L*	*V_VL*	*V_VL*	*V_VL*
		CS_VL	*CS_L*	*CS_M*	*CS_H*	*CS_VH*8
		дієвість засобів контролю				

Джерело: [7]

- частота виникнення загрози – можлива частота реалізації чинників ризику (агентів загрози) в межах певного часового інтервалу. Під чинниками слід розуміти опис типів зловмисників, які навмисно або випадково, діями або бездіяльністю здатні нанести збитки корпоративній системі [7]. Оцінювання може проводитись за шкалою: *TEF _VH* – "дуже висока" частота реалізації чинників ризику, *TEF _H* – "висока", *TEF _M* – "середня", *TEF _L* – "низька", *TEF _VL* – "дуже низька";
- частота виникнення подій втрат – можлива частота протягом визначеного часового інтервалу, з якою агент загрози завдає шкоди активу, розглядається як результат впливу факторів частоти виникнення загрози та вразливості [7]. Використовуються наступні оцінки: *LEF _VH* – "дуже високий" рівень частоти подій втрат інформаційних активів, *LEF _H* – "високий", *LEF _M* – "середній", *LEF _L* – "низький", *LEF _VL* – "дуже низький". Приклад бази знань для оцінювання рівня частоти виникнення подій втрат приводиться в табл. 2.

Таблиця 2. **Оцінювання рівня частоти подій втрат внаслідок інформаційних ризиків**

		Частота подій втрат				
Частота виникнення подій загрози	*TEF _VH*	*LEF _M*	*LEF _H*	*LEF _VH*	*LEF _VH*	*LEF _VH*8
	TEF _H	*LEF _L*	*LEF _M*	*LEF _H*	*LEF _H*	*LEF _H*
	TEF _M	*LEF _VL*	*LEF _L*	*LEF _M*	*LEF _M*	*LEF _M*
	TEF _L	*LEF _VL*	*LEF _VL*	*LEF _L*	*LEF _L*	*LEF _L*
	TEF _VL	*LEF _VL*	*LEF _VL*	*LEF _VL*	*LEF _VL*	*LEF _VL*
		V _VL	*V _L*	*V _M*	*V _H*	*V _VH*
		Вразливість				

Джерело: [7]

III. Оцінювання величини можливих збитків:

- визначення можливої дії кожного з агентів загрози інформаційному активу;
- оцінювання величини кожної з можливих форм збитків, що пов'язані з дією певного агенту загрози;
- оцінювання величини всіх можливих форм збитків за шкалою: *PL _VH* – "дуже великі", *PL _H* – "великі", *PL _Sg* – "суттєві", *PL _M* – "середні", *PL _L* – "малі", *PL _VL* – "дуже малі" збитки у відповідних грошових одиницях. Визначення величини можливих збитків може проводитися відносно бюджету корпоративної системи з врахуванням вартості інформаційних активів, вартості репутації підприємства, тощо.

IV. Результат аналізу інформаційних ризиків корпоративної системи зводиться до оцінювання загального рівня інформаційних ризиків в корпоративній системі за шкалою: *C* – "критичний", *H* – "високий", *M* – "середній", *L* – "низький" рівень інформаційних ризиків. Приклад бази знань для оцінювання приводиться в табл. 7.

Таблиця 3. **Оцінювання загального рівня інформаційних ризиків у корпоративній системі**

		Рівень інформаційних ризиків				
Величина можливих збитків	*PL _VH*	*H*	*H*	*C*	*C*	*C*
	PL _H	*M*	*H*	*H*	*C*	*C*
	PL _Sg	*M*	*M*	*H*	*H*	*C*
	PL _M	*L*	*M*	*M*	*H*	*H*
	PL _L	*L*	*L*	*M*	*M*	*H*
	PL _VL	*L*	*L*	*L*	*M*	*M*
		LEF _VL	*LEF _L*	*LEF _M*	*LEF _H*	*LEF _VH*
		Частота події втрат				

Джерело: [7]

Пропонується застосувати лінгвістичний підхід до моделювання аналізу факторів інформаційного ризику [9, 10]. Такий підхід забезпечує кількісний опис окремих елементів моделі за умов нечіткої інформації про значення критеріїв оцінювання факторів ризику, їх наслідки в умовах дії агенту загрози, альтернативні шляхи для уникнення негативного впливу інформаційних ризиків. У відповідності до лінгвістичного підходу, в якості значень критеріїв та характеристики відношень між ними допускається не тільки кількісне оцінювання, але й речення на природній мові.

На підставі розрахованих значень груп показників рівня частоти подій втрат інформаційних активів та величини можливих збитків внаслідок інформаційних ризиків проводиться оцінювання загального рівня інформаційних ризиків в корпоративній системі:

$$\Lambda = f_{\Lambda}(\Upsilon, P), \qquad (1)$$

де Υ – оцінка рівня частоти подій втрат інформаційних активів; P – попередньо оцінена величина можливих збитків.

Терм-множина вхідної змінної Υ, що є множиною ступенів частоти виникнення можливих втрат, матиме вигляд:

$$LEF = \{LEF\_VH, LEF\_H, LEF\_M, LEF\_L, LEF\_VL\}, \qquad (2)$$

де *LEF _VH* – "дуже висока" частота, *LEF _H* – "висока", *LEF _M* – "середня", *LEF _L* – "низька", *LEF _VL* – "дуже низька". Терм-множина вхідної змінної P записується у вигляді:

$$LD = \{PL\_VH, PL\_H, PL\_Sg, PL\_M, PL\_L, PL\_VL\}, \qquad (3)$$

де *PL _VH* – "дуже велика", *PL _H* – "велика", *PL _Sg* – "суттєва", *PL _M* – "середня", *PL _L* – "мала", *PL _VL* – "дуже мала" величина втрати відносно бюджету корпоративної системи.

Для оцінювання та опрацювання лінгвістичної змінної Λ рекомендовано скористатися шкалою з чотирьох якісних термів: *C* – "критичний", *H* – "високий",

M – "середній", *L* – "низький" рівень ризику. Терм-множина вихідної змінної Λ представляється у вигляді:

$$IR = \{C, H, M, L\}. \quad (4)$$

Наступним етапом аналізу є формування системи нечітких знань для визначення кожного з рівнів інформаційних ризиків. Використовуючи [2, 8], сформовано набір вирішальних правил, які реалізують співвідношення (1). У табл. 4 наведено такий набір.

Таблиця 4. **База знань для визначення рівня інформаційних ризиків**

Номер вхідної комбінації	Узагальнені значення груп показників		Вага m_{ij}	Вихідна змінна Λ
	Рівень частоти виникнення можливих втрат Υ	Величина можливих збитків *P*		
11	*PL_VH*	*LEF_M*	m_{11}	*C*
12	*PL_VH*	*LEF_H*	m_{12}	
13	*PL_VH*	*LEF_VH*	m_{13}	
14	*PL_H*	*LEF_H*	m_{14}	
15	*PL_H*	*LEF_VH*	m_{15}	
16	*PL_Sg*	*LEF_VH*	m_{16}	
21	*PL_VH*	*LEF_VL*	m_{21}	*H*
22	*PL_VH*	*LEF_L*	m_{22}	
23	*PL_H*	*LEF_L*	m_{23}	
24	*PL_H*	*LEF_M*	m_{24}	
25	*PL_Sg*	*LEF_M*	m_{25}	
26	*PL_Sg*	*LEF_H*	m_{26}	
27	*PL_M*	*LEF_H*	m_{27}	
28	*PL_M*	*LEF_VH*	m_{28}	
29	*PL_L*	*LEF_VH*	m_{29}	
31	*PL_H*	*LEF_VL*	m_{31}	*M*
32	*PL_Sg*	*LEF_VL*	m_{32}	
33	*PL_Sg*	*LEF_L*	m_{33}	
34	*PL_M*	*LEF_L*	m_{34}	
35	*PL_M*	*LEF_M*	m_{35}	
36	*PL_L*	*LEF_M*	m_{36}	
37	*PL_L*	*LEF_H*	m_{37}	
38	*PL_VL*	*LEF_H*	m_{38}	
39	*PL_VL*	*LEF_VH*	m_{39}	
41	*PL_M*	*LEF_VL*	m_{41}	*L*
42	*PL_L*	*LEF_VL*	m_{42}	
43	*PL_L*	*LEF_L*	m_{43}	
44	*PL_VL*	*LEF_VL*	m_{44}	
45	*PL_VL*	*LEF_L*	m_{45}	
46	*PL_VL*	*LEF_M*	m_{46}	

Джерело: розробка автора

Наступним кроком є визначення математичної форми запису вирішальних правил за допомогою функцій належності для визначення рівнів інформаційних ризиків. Наприклад, вирішальне правило для визначення інформаційних ризиків рівня *M* може бути записане таким чином:

$$\begin{aligned}\mu^{M}(\Upsilon, P) = {} & m_{31}\left[\mu^{LEF\_VL}(\Upsilon) \bullet \mu^{PL\_H}(P)\right] \vee m_{32}\left[\mu^{LEF\_VL}(\Upsilon) \bullet \mu^{PL\_Sg}(P)\right] \vee m_{33}\left[\mu^{LEF\_L}(\Upsilon) \bullet \mu^{PL\_Sg}(P)\right] \vee \\ & \vee m_{34}\left[\mu^{LEF\_L}(\Upsilon) \bullet \mu^{PL\_M}(P)\right] \vee m_{35}\left[\mu^{LEF\_M}(\Upsilon) \bullet \mu^{PL\_M}(P)\right] \vee m_{36}\left[\mu^{LEF\_M}(\Upsilon) \bullet \mu^{PL\_L}(P)\right] \vee \\ & \vee m_{37}\left[\mu^{LEF\_H}(\Upsilon) \bullet \mu^{PL\_L}(P)\right] \vee m_{38}\left[\mu^{LEF\_H}(\Upsilon) \bullet \mu^{PL\_VL}(P)\right] \vee m_{39}\left[\mu^{LEF\_VH}(\Upsilon) \bullet \mu^{PL\_VL}(P)\right],\end{aligned} \quad (5)$$

де $\mu^{M}(\Upsilon, P)$ – функція належності вихідної змінної Λ значенню *M* з нечіткого терму (4); $m_{3k}(k = \overline{1,9})$ – ваговий коефіцієнт для відповідної *k*-ї комбінації; $\mu^{lef_j}(\Upsilon)$ – функція належності параметра Υ до нечіткого терму lef_j з терм-множини *LEF* (2); $\mu^{ld_i}(P)$ – функція належності параметра *P* до нечіткого терму ld_i з терм-множини *LD* (3).

Подібним чином формується вся база знань з використанням експертних даних та виводиться система нечітких логічних рівнянь. Результатом представленої концепції та інструментарію оцінювання рівня частоти подій втрат та величини можливих втрат інформаційних

активів є лінгвістичний опис загального рівня інформаційних ризиків в корпоративній системі.

Були побудовані дзвоноподібні функції належності термів вихідної змінної Λ до терм-множини (4), параметри яких представлено в табл. 5:

$$\mu^T(x) = \frac{1}{1+\left|\frac{x-c}{a}\right|^{2b}}, \quad (6)$$

де T – довільний нечіткий терм; a – коефіцієнт концентрації; b – коефіцієнт крутизни; c – координата максимуму функції, $\mu^T(c) = 1$.

Таблиця 5. **Параметри функцій належності термів до терм-множини** *IR*

Назва терму	Функція належності	Параметри		
		координата максимуму *c*	коефіцієнт концентрації *a*	коефіцієнт "крутизни" *b*
L	$\mu^1(x)$	0	0,1	2
M	$\mu^2(x)$	0,33	0,1	2
H	$\mu^3(x)$	0,67	0,1	2
C	$\mu^4(x)$	1	0,1	2

Джерело: розробка автора

Графічне представлення функції належності вихідної змінної, бази логічного висновку представлені на рис. 1 і 2 відповідно.

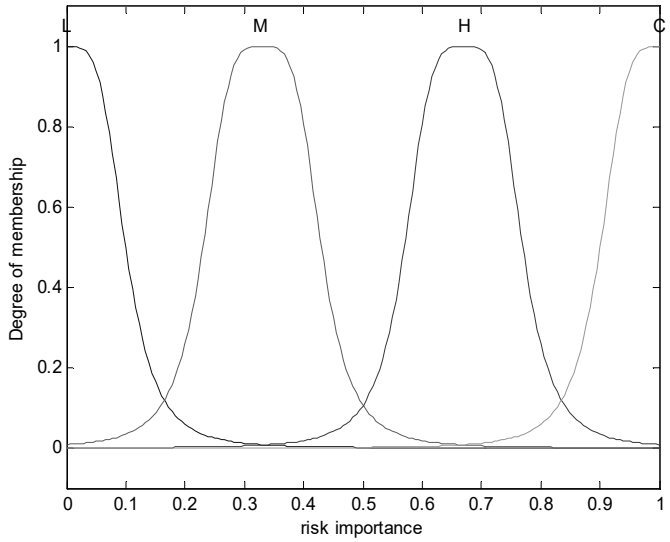

Рис. 1. Графіки функцій належності показника рівня інформаційних ризиків в корпоративній системі.

Джерело: розробка автора

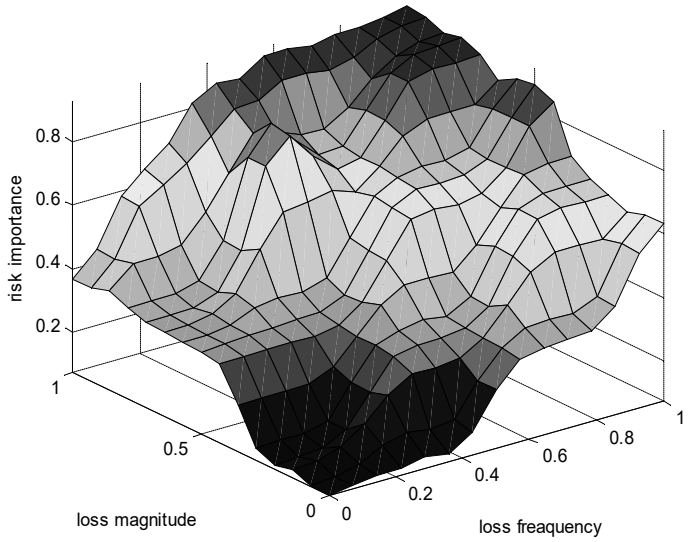

Рис. 2. Графічне представлення системи нечіткого висновку показника рівня інформаційних ризиків

Джерело: розробка автора

Результати проведених досліджень щодо оцінювання рівня інформаційних ризиків в корпоративній системі представлено в табл. 6.

Таблиця 6. **Оцінювання рівня інформаційних ризиків**

Назва підприємства	Величина можливих збитків	Рівень частоти можливих втрат	Рівень інформаційних ризиків
Підприємство 1	*PL_M*	*LEF_L*	*M*
	0,4012	0,3545	0,3751
Підприємство 2	*PL_Sg*	*LEF_M*	*H*
	0,5971	0,5799	0,6348
Підприємство 3	*PL_Sg*	*LEF_M*	*H*
	0,5991	0,4376	0,6252
Підприємство 4	*PL_H*	*LEF_L*	*H*
	0,7749	0,1740	0,6109

Джерело: розробка автора

Як видно з табл. 6, на Підприємстві 2, Підприємстві 3, та Підприємстві 4 визначено рівень інформаційних ризиків, що відповідає оцінці "високий", на Підприємстві 1 – "середній".

За результатами оцінювання чинників інформаційних ризиків було прийняте рішення щодо методів зниження рівня інформаційних ризиків на підприємствах. Наприклад, на Підприємстві 3 були вжиті додаткові заходи з підвищення рівня дієвості засобів захисту, оскільки високий рівень вразливості був викликаний саме недоліками роботи цих ресурсів та їх невідповідності високому рівню загроз інформаційної безпеки підприємства. Можна прийти висновку, що подібна модель оцінювання загального рівня ризику гнучка та адаптивна і може бути налаштована у відповідності до одержаної бази знань.

Висновки. Категорія "інформаційний ризик" повинна розглядатися з позицій керівника підприємства, який зацікавлений в управлінні всіма ризиками, що пов'язані з використанням управлінської інформації на підприємстві. Пропонується пов'язувати інформаційні ризики не тільки з порушенням безпеки інформації, але і з втратою якості інформації, що використовується в бізнес-процесах.

Аналіз інформаційних ризиків є основою для побудови підсистеми управління інформаційною безпекою підприємства. В ході аналізу та оцінювання рівня інформаційних ризиків слід дотримуватися наступних кроків: ідентифікація інформаційних ресурсів (активів) компанії, що можуть бути об'єктом ризику, можливих загроз активу та визначення рівня загроз безпеки КІС підприємства; оцінювання рівня дієвості засобів контролю безпеки корпоративної системи; оцінювання вразливості корпоративної системи, що розглядається як результат впливу факторів вірогідного рівня сили загрози та рівня дієвості засобів контролю; оцінювання частоти подій втрат від інформаційних ризиків як результату впливу факторів частоти виникнення загрози та вразливості корпоративної системи; оцінювання величини можливих збитків від інформаційних ризиків в корпоративної системи; оцінювання рівня інформаційних ризиків в корпоративної системи як результуючої двох факторів: частоти подій втрат та величини можливих втрат від інформаційних ризиків.

Побудовано модель оцінювання загального рівня інформаційних ризиків у корпоративній системі з застосуванням лінгвістичного підходу, що забезпечує кількісний опис окремих елементів моделі за умов нечіткої інформації про значення критеріїв оцінювання чинників (факторів) ризику. Це дає можливість виділити значущі чинники ризику, їх наслідки в умовах дії агента загрози, і, тим самим, визначити альтернативні шляхи для уникнення негативного впливу ризику: заміна чи модифікація засобів контролю безпеки; впровадження механізмів захисту відповідно до можливого рівня загроз певних класів порушників інформаційної безпеки; реалізація режиму функціональної замкнутості, який виключав би використання апаратного та програмного забезпечення, що не має відповідного паспорту безпеки тощо.

Результатом представленої технології та інструментарію оцінювання рівня інформаційних ризиків в корпоративній системі є лінгвістичний опис і можливість аналізу та оцінювання факторів інформаційних ризиків, а саме, рівня частоти виникнення подій загроз та вразливості корпоративної системи. Розроблений концептуальний підхід 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.

Запропонована модель оцінювання рівня інформаційних ризиків може лягти в основу розбудови підсистеми управління інформаційними ризиками як на стадії проектування корпоративної інформаційної системи підприємства, так і в ході її експлуатації. Модель легко адаптується для виконання задач управління інформаційними ризиками на рівні з іншими задачами. При цьому не вимагається кардинально змінювати організаційну структуру підприємства. Необхідно лише реорганізувати її, максимально пристосувати до розв'язання задач управління інформаційними ризиками.

Дискусія. Незважаючи на вагомість здійснених напрацювань, залишається низка невирішених проблем, а саме: розбудова математичних моделей та відповідного інструментарію для зниження (факторів вразливості) чи підвищення (факторів дієвості засобів захисту) впливу чинників на загальний рівень інформаційних ризиків; розробка положень щодо застосування механізмів управління окремими факторами інформаційних ризиків.

Список використаних джерел

1. Information Technology. Information Security. Information Assurancy. Режим доступу: http://www.isaca.org. – Назва з екрану. – Дата звернення: 12.03.2015.

2. Матвійчук А. В. Моделювання економічних процесів із застосуванням методів нечіткої логіки / А. В. Матвійчук. – К.: КНЕУ, 2007. – 264 с.

3. Завгородний В. И. Информационные риски и экономическая безопасность предприятия / В. И. Завгородний. – М.: Финакадемия, 2008. – 160 с.

4. Липаев В. В. Функциональная безопасность программных средств / В. В. Липаев. – М.: СИНТЕГ, 2004. – 348 с.

5. Стенг Д. И. Секреты безопасности сетей / Д. И. Стенг, С. Мун. – К.: Диалектика, 1996. – 544 с.

6. Мур М. Управление информационными рисками / М. Мур // Финансовый директор. – 2003. – № 9. – С.64–69.

7. Jones J. A. An Introduction to FAIR / J. A. Jones – Trustees of Norwich University, 2005 – 67 p.

8. Zadeh L. A. Fuzzy sets / L. A. Zadeh. – Information and Control, 1965. – №8.– P. 338–353.

9. Zadeh L. A. On optimal control and linear programming / L. A. Zadeh, B. H. Whalen. – IRE Trans. Automatic control, Ac-7, 1962. – P. 45 – 46.

10. Zimmermann H.-J. Fuzzy Sets, Decision Making and Expert Systems / H.-J. Zimmermann. – Kluwer:Dordrecht, 1987. – 335 p.

Надійшла до редколегії 26.04.15

Г. Мельник, канд. экон. наук
Черновицкий национальный университет имени Юрия Федьковича, Черновцы, Украина

МОДЕЛЬ ОЦЕНИВАНИЯ УРОВНЯ ИНФОРМАЦИОННЫХ РИСКОВ В КОРПОРАТИВНЫХ СИСТЕМАХ

Проведен анализ особенностей и мирового опыта информационного риск-менеджмента. Обоснована необходимость комплексного подхода к управлению информационными рисками в корпоративных системах, при котором системно рассматривались бы все составляющие качества и безопасности информации, влияющие на эффективность использования средств и механизмов защиты информации в корпоративных информационных системах. Построена экономико-математическая модель с использованием теории и инструментов нечетких множеств и нечеткой логики, позволяющая точнее оценить степень информационных рисков на предприятии.

Ключевые слова: информационный риск, корпоративная информационная система, анализ факторов информационных рисков, уязвимость, уровень угрозы, действенность средств защиты информации.

Melnyk H., PhD in Economics
Chernivtsi National University named after Yuriy Fedkovych, Chernivtsi, Ukraine

MODEL OF INFORMATION RISK MEASUREMENT IN CORPORATE SYSTEMS

The features and world experience of information risk management are analyzed. The necessity of a comprehensive approach to the analysis and management of information risks in corporate systems is proved. The economic-mathematical model was built with the application of the theory and tools of fuzzy sets and fuzzy logic, which can more accurately measure the risk of information and make effective decisions in reducing the risk of possible lost in the corporate systems.

Keywords: information risk, corporate information systems, analysis of information risk factors, vulnerability, threat level, the effectiveness of defense information.

Bulletin of Taras Shevchenko National University of Kyiv. Economics, 2015, 6(171): 54-60
DOI: dx.doi.org/ 10.17721/1728-2667.2015/171-6/10
УДК 336.717.8
JEL G20

В. Осецький, д-р екон. наук, проф.
Київський національний університет імені Тараса Шевченка, Київ,
І. Браткова, асп. відділу фінансових ринків,
ДННУ "Академія фінансового управління", Київ

ФУНКЦІЇ ДЕРЖАВНИХ БОРГОВИХ ЗОБОВ'ЯЗАНЬ: МИНУЛЕ ТА СУЧАСНІСТЬ

В статті розглянуто основні передумови виникнення ринку державних цінних паперів та його функції на різних етапах розвитку економічних відносин. Також, виділено основні види боргових зобов'язань уряду, що емітувались в різних країнах в процесі становлення фінансової системи. Встановлено, що, хоча початкові функції державних цінних паперів були дещо обмеженими в сфері регулювання грошово-кредитного ринку, вони відігравали важливу роль в акумуляції фінансових ресурсів до державного бюджету та спрямовувались на вирішення важливих, зокрема воєнних, питань. Крім того, акцентується увага на тому, що в процесі становлення ринку урядової позики розширювались не лише його функції, а й змінювались характеристики боргових зобов'язань держави як цінного паперу. Як результат, на основі проведеного дослідження з урахуванням сучасних тенденцій сформовано більш повний перелік цілей, для досягнення яких здійснюється випуск боргових інструментів державних запозичень.

Ключові слова: державний кредит, державні цінні папери, дефіцит бюджету, операції на відкритому ринку, мобілізація фінансових ресурсів.

ВСТУП. Державні запозичення з'являються на певному етапі розвитку економічної системи. Уряди країн використовували позики ще багато століть тому, так як часто виникали ситуації, коли запозичення залишались чи не єдиним способом залучення додаткових фінансових ресурсів. Важливими є також і передумовами випуску державних позик з позиції кредиторів. До них, зокрема, належать: наявність суб'єктів, що мають у своєму розпорядженні тимчасово вільні кошти; довіра інвесторів до держави, що стимулює їх зацікавленість у купівлі боргових цінних паперів уряду; спроможність держави погасити свої зобов'язання тощо.

Об'єктивна необхідність використання державою інструментів позики пов'язана з наявністю суперечності між існуючими потребами суспільства і можливістю держави їх задовольнити за рахунок наявних фінансових ресурсів. Виконання державою покладених на неї функцій у різних сферах економіки передбачає також і фінансову складову, необхідну для їх реалізації. Саме тому виникає необхідність пошуку нових джерел поповнення державного бюджету, одним з яких є випуск державних цінних паперів.

Державні цінні папери є свідоцтвом про надання їхніми власниками позики державі в особі національного уряду та місцевих органів управління. Випуск інструментів позики здійснюється з метою мобілізації грошового капіталу для фінансування державних витрат, якщо недостатньо бюджетних коштів. Держава гарантує викуп своїх боргових зобов'язань, тому вони вважаються першокласними цінними паперами з високим ринковим рейтингом.

Аналіз останніх досліджень та публікацій. Проблемі здійснення державних запозичень присвячені роботи багатьох вітчизняних та зарубіжних вчених. Загалом, серед усієї сукупності теорій державного кредиту можна виокремити дві основні групи, що різняться самим ставленням до існування урядових позик. Їх можна представити наступним чином:

- Державний кредит є негативним явищем і політика уряду має бути спрямована на поступове зменшення, а в подальшому – на повну ліквідацію державного боргу. Це пов'язано з тим, що як і виплата відсотків по зобов'язаннях, так і сплата основної суми боргу лягають важким тягарем на населення країни, а також така ситуація може викликати підвищення податкових ставок.
- Державний кредит розглядається як нормальне явище. Не варто категорично ставитись до зростання державного боргу, адже за рахунок отриманих коштів можна досягнути позитивного ефекту в діяльності держави і, відповідно, значно ефективніше використовувати наявний капітал.

Натомість вітчизняні науковці зазвичай аналізують як позитивні, так і негативні наслідки державних позик. При цьому, вони не заперечують саме існування дер-