УДК [005.52:005.334:519.86]:334.784(043.3)

НЕЧІТКИЙ ПІДХІД ДО ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНИХ РИЗИКІВ У CRM-СИСТЕМАХ

О. І. Черняк

Доктор економічних наук, професор,
завідуючий кафедри економічної кібернетики

Київський національний університет імені Тараса Шевченка
вулиця Васильківська, 90а, м. Київ, 03022, Україна
chernyak@univ.kiev.ua

Д. О. Сікорський

Магістр з економічної кібернетики,
аспірант кафедри економічної кібернетики

Київський національний університет імені Тараса Шевченка
вулиця Васильківська, 90а, м. Київ, 03022, Україна
sikorskiy.dima@outlook.com

У статті проведено аналіз світового досвіду з управління інформаційними ризиками та обґрунтовано необхідність створення комплексного підходу до оцінювання рівня інформаційних ризиків як у корпоративних системах загалом, так і CRM-системах зокрема. Такий підхід передбачає систематизований аналіз усіх складових якості та безпеки інформації, що впливають на ефективність використання засобів і механізмів захисту інформації в CRM-системах. Розроблено економіко-математичну модель на підґрунті інструментарію теорії нечітких множин і нечіткої логіки, що дозволяє враховувати в аналізі інформаційних ризиків на підприємстві як кількісні характеристики інформаційних систем, так і якісні та нормативні показники, враховувати експертні знання в предметній області та здійснювати налаштування моделей на реальних прикладах створення систем безпеки в інформаційному середовищі.

Ключові слова: *інформаційний ризик, CRM-система, чинники інформаційних ризиків, вразливість, рівень загроз, дієвість засобів захисту інформації.*

НЕЧЕТКИЙ ПОДХОД К ОЦЕНИВАНИЮ УРОВНЯ ИНФОРМАЦИОННЫХ РИСКОВ В CRM-СИСТЕМАХ

А. И. Черняк

Доктор экономических наук, профессор,
заведующий кафедры экономической кибернетики

Киевский национальный университет имени Тараса Шевченко
улица Васильковская, 90а, м. Киев, 03022, Украина
chernyak@univ.kiev.ua

Д. О. Сикорский

Магистр по экономической кибернетике,
аспирант кафедры экономической кибернетики

Киевский национальный университет имени Тараса Шевченко
улица Васильковская, 90а, м. Киев, 03022, Украина
sikorskiy.dima@outlook.com

В статье проведен анализ мирового опыта управления информационными рисками и обоснована необходимость создания комплексного подхода к оцениванию уровня информационных рисков как в корпоративных системах в целом, так и в CRM-системах в частности. Такой подход предусматривает систематизированный анализ всех составляющих качества и безопасности информации, влияющих на эффективность использования средств и механизмов защиты информации в CRM-системах. Построена экономико-математическая модель на основе инструментария теории нечетких множеств и нечеткой логики, позволяющая учитывать в анализе информационных рисков на предприятии как количественные характеристики информационных систем, так и качественные и нормативные показатели, принимать во внимание экспертные знания в предметной области и осуществлять настройку моделей на реальных примерах создания систем безопасности в информационной среде.

Ключевые слова: *информационный риск, CRM-система, факторы информационных рисков, уязвимость, уровень угрозы, действенность средств защиты информации.*

FUZZY APPROACH TO INFORMATION RISKS' MEASUREMENT IN CRM-SYSTEMS

Oleksandr Chernyak

DSc (Economic Sciences), Professor,
Head of Department of Economic Cybernetics

Taras Shevchenko National University of Kyiv
90a Vasylkivska Street, Kyiv, 03022, Ukraine
chernyak@univ.kiev.ua

Dmytro Sikorskyi

Master's Degree in Economic Cybernetics,
PhD student, Department of Economic Cybernetics

Taras Shevchenko National University of Kyiv
90a Vasylkivska Street, Kyiv, 03022, Ukraine
sikorskiy.dima@outlook.com

The features and world experience of information risks management are analyzed in the article. The necessity of development of a comprehensive approach to the analysis and management of information risks in corporate systems as a whole, and in the CRM-system in particular is proved. This approach provides a systematic analysis of all components of quality and security of information, affecting to efficiency of usage of data protection mechanisms in the CRM-system. The economic and mathematical model was built with the application of tools of fuzzy sets and fuzzy logic theory, which can more accurately measure the quantitative and qualitative aspects of information risk at enterprise, take into account expert knowledge in the subject area and carry out tuning of models on the real examples of security systems in the corporation information environment.

Keywords: *information risk, CRM-system, information risk's factors, vulnerability, threat level, effectiveness of data protection tools.*

JEL Classification: C45, C89, D81

Вступ

Сучасні підприємства зазвичай характеризуються складною структурою, що зумовлена територіальним розгалуженням підрозділів, багатопрофільною діяльністю, чисельними корпоратив-

ними зв'язками з партнерами. Більшість бізнес-функцій щодо збору, зберігання, обробки й аналізу інформації про споживачів, партнерів та інформації про взаєморозрахунки забезпечують інформаційні системи управління відносинами із замовниками (клієнтами), — CRM-системи [1]. Сучасна CRM-система направлена на вивчення ринку і конкретних потреб клієнтів. На основі цих знань розробляються нові товари або послуги і, таким чином, компанія досягає поставлених цілей і покращує свій фінансовий результат.

Впровадження нових інформаційних технологій завжди пов'язане з новими ризиками. Існуюча методологія інформаційного ризик-менеджменту не передбачає комплексного підходу до управління ризиком безпеки інформації в CRM-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.

У науковій літературі, національних і міжнародних стандартах [2] приділяється значна увага проблемам управління ризиками, що пов'язані з використанням інформації в діяльності підприємств. Учені Бернстайн П. [3], Марковіц Г. [4], Найт Ф. Х. [5], Самуельсон П. [6] та інші розробили загальні принципи управління економічними ризиками. Математичні методи та інструментарій моделювання ризиків представлені в роботах Вітлінського В. В. [7], Галіцина В. К. [8], Клейнера Г. Б. [9], Матвійчука А. В. [10], Суслова О. П. [11] та інших.

Інформаційні ризики як різновид економічних ризиків розглядається в працях Завгороднього В. І. [12], Ліпаєва В. В. [13] і Мельник Г. В. [14]. Так, Ліпаєв В. В. вкладає у поняття «інформаційний ризик» наступний зміст: це можлива подія, у результаті якої несанкціоновано знищується, спотворюється інформація, порушується її конфіденційність або доступність [13]. При цьому під захистом інформації розуміють захист в основному від зловмисних дій.

Проблеми оцінювання якості інформації та надійності апаратних і програмних засобів розглядаються в працях Байхельта Ф., Франкена П. [15], Зегжда П. Д. [16], Мура М. [17] та інших. Ще більшою мірою звужують поняття інформаційного ризику Стенг Д. І. та Мун С. [18] і трактують його тільки як загрозу без-

пеці інформації в комп'ютерних системах. Фахівці в галузі захисту інформації здебільшого схиляються саме до цього розуміння категорії «інформаційні ризики». Частина дослідників інформаційного ризик-менеджменту під інформаційним ризиком розуміють тільки можливість виникнення збитків, недоотримання прибутку та інші негативні наслідки для підприємства. Недоліком подібних визначень є нечітке окреслення об'єктів, ушкодження чи зміна властивостей яких призведуть до збитків і виключення з розгляду ризиків, що можуть бути пов'язані з впливом зловмисників на інформаційні ресурси заходами шпигунства чи диверсій, з навмисним ушкодженням інформації, з паперовим документообігом тощо.

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

Методологія дослідження

Метою статті є розробка системи економіко-математичних моделей оцінювання загального рівня інформаційних ризиків у CRM-системах. Предметом дослідження є методологія та інструментарій економіко-математичного моделювання у процесах управління інформаційними ризиками в CRM-системах. Об'єктом дослідження є інформаційні ризики в CRM-системах підприємства.

Процес функціонування CRM-систем підприємства здійснюється в умовах протиборства підприємства як соціотехнічної системи, з одного боку, і конкурентів, зловмисників, негативних впливів інших об'єктів чи явищ, з іншого боку. Для дослідження таких систем використовуються різні типи моделей.

Одним з розділів математики, що знайшли широке застосування в моделюванні складних систем, є теорія множин. Розширити можливості класичної теорії множин дозволяє теорія нечітких множин [10, 19—21]. При моделюванні складних систем в умовах недостатньої інформації та випадковості процесів для розподілу об'єктів за підмножинами доцільно використовувати апарат нечітких множин. При дослідженні інформаційних ризи-

ків таке завдання стоїть, наприклад, при вирішенні задачі віднесення довільного чинника ризику до множини значущих чинників ризиків у конкретній CRM-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 впливу факторів ризику.

Отже, у статті пропонується розробити концептуальний підхід до оцінювання рівня ризиків, який дозволяв би замінити наближені табличні методи грубої оцінки ризиків сучасним математичним інструментарієм. Формування системи математичних моделей і методів управління інформаційними ризиками відповідно до цього концептуального підходу складається з таких етапів: розроблення і застосування методів ідентифікації інформаційних ресурсів (активів) підприємства, які можуть стати об'єктами інформаційних ризиків і загроз цим ресурсам; розроблення і застосування моделей кількісного аналізу й оцінювання окремих факторів (вразливості, дієвості засобів захисту тощо) і загального рівня інформаційних ризиків із застосуванням інструментарію нечіткої логіки; розроблення математичних моделей для економічного обґрунтування ефективності використання механізмів (засобів) зниження ступеня інформаційних ризиків і зменшення пов'язаних з цим втрат (збитків, шкоди) підприємству.

Побудова системи моделей аналізу та оцінювання інформаційних ризиків

У загальноприйнятих методиках аналізу інформаційних ризиків здійснюється оцінювання ризику за трьома факторами: загроза, вразливість, величина можливих збитків. Виділяють чотири основні кроки аналізу інформаційних ризиків [22]:

І. Ідентифікація компонент:

- інформаційних ресурсів (активів) компанії, що можуть бути об'єктом ризику. Згідно стандарту безпеки ISO/IEC 27001:2013 [2] інформаційний актив — це матеріальний чи нематеріальний об'єкт, який є інформацією або містить інформацію, використовується для збереження чи обробки інформації, складає цінність для підприємства (організації);
- можливих загроз (комбінації загроз) активу. Для управління ризиками необхідно ідентифікувати можливі небезпеки, які загрожують CRM-системі. Такими можуть бути, наприклад, сти-

хійне лихо, відключення електроживлення або атаки зловмисників з наслідками різного ступеня 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. 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. 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 і оцінюється за шкалою: V_VH — «дуже високий» рівень вразливості, V_H — «високий», V_M — «середній», V_L — «низький», V_VL — «дуже низький»;
- 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 CRM-системі [22]. 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 [22]. Використовуються такі оцінки: LEF_VH — «дуже високий» рівень частоти подій втрат інформаційних активів, LEF_H — «високий», LEF_M — «середній», LEF_L — «низький», LEF_VL — «дуже низький».

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 агента 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 проводитись відносно бюджету CRM-системи з урахуванням вартості інформаційних активів, вартісної оцінки репутації підприємства тощо.

IV. Результат аналізу інформаційних ризиків CRM-системи зводиться до оцінювання загального рівня інформаційних ризиків за шкалою: *C* — «критичний», *H* — «високий», *M* — «середній», *L* — «низький» рівень інформаційних ризиків. Приклад бази знань для оцінювання рівня інформаційних ризиків у CRM-системі за величиною можливих збитків та частотою події втрат приводиться в табл. 1.

Таблиця 1

ОЦІНЮВАННЯ ЗАГАЛЬНОГО РІВНЯ ІНФОРМАЦІЙНИХ РИЗИКІВ У CRM-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: [22]

Схему декомпозиції інформаційних ризиків представлено на рис. 1.

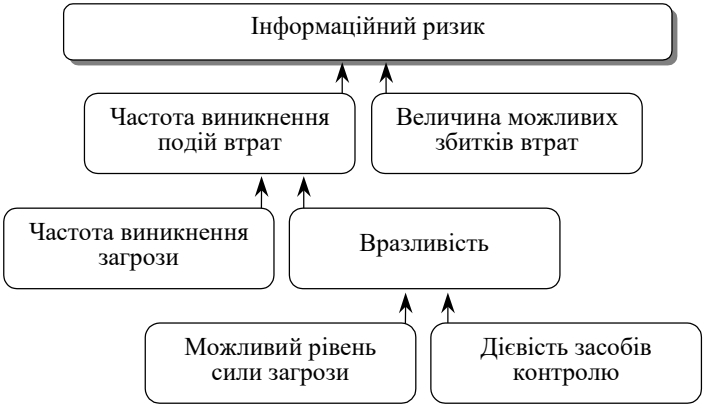

Рис. 1. Схема декомпозиції інформаційного ризику (джерело [24])

Моделювання рівня інформаційних ризиків у CRM-системі

Для аналізу чинників інформаційного ризику пропонується застосувати лінгвістичний підхід [20, 21]. За умов нечіткої інформації про значення критеріїв оцінювання факторів ризику, їх наслідки в умовах дії агента загрози, альтернативні шляхи для уникнення негативного впливу інформаційних ризиків такий підхід забезпечує кількісний опис окремих елементів моделі. Лінгвістичний підхід передбачає не тільки кількісне оцінювання якісних і нормативних критеріїв, але й урахування логічних висловлювань природною мовою для опису специфіки відношень між ними.

Для опису поведінки потенційного порушника найдоцільніше використовувати диференційований підхід, який буде враховувати 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 системи захисту CRM-системи:

1-й клас рекомендується для захисту суттєво важливої інформації, витік, порушення або модифікація якої можуть призвести до великих втрат для санкціонованого користувача. Стійкість за-

хисту має бути розрахована на висококваліфікованого порушника-професіонала;

2-й клас рекомендується використовувати для захисту важливої інформації при 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 кваліфікованого порушника-професіонала;

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

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

На підставі вищевказаної класифікації рівнів стійкості безпеки щодо загрози порушника пропонується застосувати лінгвістичний підхід до моделювання можливих загроз інформаційним активам CRM-системи. Для кожного класу безпеки (рівня стійкості захисту CRM-системи) поставимо у відповідність лінгвістичні показники T_1, T_2, T_3, T_4.

Для оцінювання та опрацювання лінгвістичних змінних T_1, T_2, T_3, T_4 і вихідної змінної U, що характеризує загальний рівень сили загрози інформаційній системі, сформовано шкалу з п'яти якісних термів: TC_VH — «дуже високий» рівень загроз, TC_H — «високий», TC_M — «середній», TC_L — «низький», TC_VL — «дуже низький». Терм-множина вхідних змінних T_1, T_2, T_3, T_4 та вихідної змінної U записується у вигляді:

$$D = \{TC\_VH, TC\_H, TC\_M, TC\_L, TC\_VL\}. \quad (1)$$

На основі розрахованих значень груп показників проводиться визначення рівня сили загрози:

$$U = \psi_U(T_1, T_2, T_3, T_4). \quad (2)$$

Для опису загального рівня сили загрози несанкціонованого доступу порушника сформовано базу нечітких знань (табл. 2).

Таблиця 2

БАЗА НЕЧІТКИХ ЗНАНЬ ДЛЯ ОПИСУ ЗАГАЛЬНОГО РІВНЯ СИЛИ ЗАГРОЗИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ПОРУШНИКА

Номер вхідної комбінації	Вхідні змінні				Вагові коефіцієнти ν	Вихідна змінна U
	T_1	T_2	T_3	T_4		
11	TC_VH	TC_VH	TC_VH	TC_VH	ν_{11}	TC_VH
12	TC_VH	TC_VH	TC_VH	TC_H	ν_{12}	
…						
$1k_1$	TC_H	TC_H	TC_VH	TC_VH	ν_{1k_1}	
21	TC_VH	TC_H	TC_H	TC_H	ν_{21}	TC_H
22	TC_H	TC_H	TC_H	TC_H	ν_{22}	
…						
$2k_2$	TC_M	TC_M	TC_H	TC_H	ν_{2k_2}	
31	TC_M	TC_M	TC_M	TC_H	ν_{31}	TC_M
32	TC_M	TC_M	TC_M	TC_M	ν_{32}	
…						
$3k_3$	TC_L	TC_L	TC_M	TC_M	ν_{3k_3}	
41	TC_L	TC_L	TC_L	TC_M	ν_{41}	TC_L
42	TC_L	TC_L	TC_L	TC_L	ν_{42}	
…						
$4k_4$	TC_VL	TC_L	TC_L	TC_L	ν_{4k_4}	
51	TC_VL	TC_VL	TC_L	TC_L	ν_{41}	TC_VL
52	TC_VL	TC_VL	TC_VL	TC_L	ν_{42}	
…						
$5k_5$	TC_VL	TC_VL	TC_VL	TC_VL	ν_{5k_5}	

Джерело: розробка авторів

Математична форма запису вирішального правила для визначення загального рівня сили загрози рівня d_j інформаційній системі матиме вигляд:

$$\mu^{d_j}(T_1,T_2,T_3,T_4)=\bigvee_{p=1}^{k_j}\left(v_{jp}\left[\bigwedge_{i=1}^{4}\mu^{d_i^{jp}}(T_i)\right]\right),\ j=\overline{1,5}, \qquad (3)$$

де $\mu^{d_j}(T_1,T_2,T_3,T_4)$ — функція належності вектора вхідних змінних (T_1,T_2,T_3,T_4) значенню вихідної змінної d_j з множини (1); k_j — кількість комбінацій значень змінних (T_1,T_2,T_3,T_4), для яких вихідна змінна приймає значення d_j; v_{jp} — ваговий коефіцієнт p-ї комбінації ($p=\overline{1,k_j}$) для вихідної змінної d_j; $\mu^{d_i^{jp}}(T_i)$ — функція належності вхідної змінної T_i до нечіткого терму d_i^{jp} ($i=\overline{1,4}$, $d_i^{jp}\in D$ за (1)).

Даний підхід дозволяє формувати модель оцінювання рівня сили загрози інформаційній системі внаслідок впливу чи дії порушників довільного класу.

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

У ході дослідження проблеми аналізу рівня дієвості засобів контролю захисту CRM-системи розроблено підхід із використанням нечітких описів. На першому етапі для випадку оцінки дієвості засобів контролю за критеріями конфіденційності, цілісності, доступності та спостережності необхідно сформувати набір окремих показників $A=\{A_i\}$, $i=\overline{1,4}$. Тобто отримуємо такий набір A критеріїв: A_1 — для оцінювання дієвості засобів контролю за критерієм конфіденційності; A_2 — для оцінювання дієвості за критерієм цілісності; A_3 — за критерієм доступності; A_4 — за критерієм спостережності.

На основі розрахованих значень груп показників проводиться визначення рівня дієвості засобів контролю інформаційної системи:

$$\Omega = \varphi_{\Omega}(A_1, A_2, A_3, A_4). \quad (4)$$

Для оцінювання та опрацювання лінгвістичних змінних A_1, A_2, A_3 та A_4 сформуємо шкалу з п'яти якісних термів: C_VH — «дуже високий», C_H — «високий», C_M — «середній», C_L — «низький», C_VL — «дуже низький» рівень дієвості. Взявши за основу зорієнтованість на середню здатність агентів загрози, приймається базовий рівень дієвості контролю за кожним з критеріїв, який і відповідатиме рівню «середній».

Для оцінювання значень вихідної лінгвістичної змінної Ω, що являє собою повну множину ступенів дієвості комплексу засобів контролю, будемо використовувати терми: CS_VH — «дуже високий» рівень дієвості, CS_H — «високий», CS_M — «середній», CS_L — «низький», CS_VL — «дуже низький».

Визначається можливий діапазон змінювання контрольованих параметрів A_1, A_2, A_3, A_4 та вихідної змінної Ω. Задається вигляд функцій належності нечітких термів для різних контрольованих параметрів. Функція належності відображає елементи з множини A на множину чисел в інтервалі $[0, 1]$, які вказують ступінь належності кожного елемента до відповідного лінгвістичного терму. Терм-множина вхідних змінних у загальному випадку представляється у вигляді:

$$E = \{C\_VH, C\_H, C\_M, C\_L, C\_VL\}. \quad (5)$$

А терм-множина вихідної змінної Ω записується у вигляді:

$$EM = \{CS\_VH, CS\_H, CS\_M, CS\_L, CS\_VL\}. \quad (6)$$

Для опису загального рівня дієвості контролю комплексу засобів захисту безпеки CRM-системи сформовано базу нечітких знань (табл. 3).

Таблиця 3

БАЗА НЕЧІТКИХ ЗНАНЬ ДЛЯ ОПИСУ ЗАГАЛЬНОГО РІВНЯ ДІЄВОСТІ КОНТРОЛЮ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ

Номер вхідної комбінації	Вхідні змінні				Вагові коефіцієнти η	Вихідна змінна Ω
	A_1	A_2	A_3			
11	C_VH	C_VH	C_VH	C_VH	η_{11}	CS_VH
12	C_VH	C_VH	C_VH	C_H	η_{12}	
…						
$1k_1$	C_H	C_H	C_VH	C_VH	η_{1k_1}	
21	C_H	C_H	C_H	C_VH	η_{21}	CS_H
22	C_H	C_H	C_H	C_H	η_{22}	
…						
$2k_2$	C_H	C_H	C_H	C_M	η_{2k_2}	
31	C_H	C_H	C_M	C_M	η_{31}	CS_M
32	C_H	C_H	C_M	C_M	η_{32}	
…						
$3k_3$	C_M	C_M	C_M	C_L	η_{3k_3}	
41	C_M	C_M	C_L	C_L	η_{41}	CS_L
42	C_M	C_L	C_L	C_L	η_{42}	
$4k_4$	C_L	C_L	C_L	C_VL	η_{4k_4}	
51	C_L	C_L	C_VL	C_VL	η_{51}	CS_VL
52	C_L	C_VL	C_VL	C_VL	η_{52}	
…						
$5k_5$	C_VL	C_VL	C_VL	C_VL	η_{5k_5}	

Джерело: розробка авторів

Математична форма запису вирішального правила для визначення рівня em_l дієвості засобів контролю матиме вигляд:

$$\mu^{em_l}(A_1, A_2, A_3, A_4) = \bigvee_{p=1}^{k_l} \left(\eta_{lp} \left[\bigwedge_{j=1}^{4} \mu^{e_j^{lp}}(A_j) \right] \right), l = \overline{1,5}, \quad (7)$$

де $\mu^{em_l}(A_1, A_2, A_3, A_4)$ — функція належності вектора вхідних змінних (A_1, A_2, A_3, A_4) значенню вихідної змінної em_l з множини (6); k_l — кількість комбінацій значень змінних (A_1, A_2, A_3, A_4), для яких вихідна змінна приймає значення em_l; η_{lp} — ваговий коефіцієнт для відповідної p-ї комбінації ($p = \overline{1, k_l}$) вихідної змінної em_l; $\mu^{e_j^{lp}}(A_j)$ — функція належності вхідної змінної A_j до нечіткого терму e_j^{lp} ($e_j^{lp} \in E$ за (5)).

Запропонована в [22] модель оцінювання рівня інформаційних ризиків передбачає наступним кроком аналіз рівня вразливості CRM-системи. Для оцінювання та опрацювання лінгвістичної змінної V, що відповідає рівню вразливості, сформовано шкалу з п'яти якісних термів: V_VH — «дуже високий» рівень вразливості, V_H — «високий», V_M — «середній», V_L — «низький», V_VL — «дуже низький». Терм-множина вихідної змінної V матиме вигляд:

$$VL = \{V\_VH, V\_H, V\_M, V\_L, V\_VL\}. \quad (8)$$

На попередніх етапах було визначено можливий діапазон змінювання контрольованих параметрів і шкала оцінювання загального рівня загроз (табл. 1) і рівня дієвості засобів контролю захисту CRM-системи (табл. 2). Функції належності термів вхідних змінних U (показник рівня сили загрози) та Ω (показник рівня дієвості засобів контролю захисту інформації) до власних терм-множин (1) та (6) були визначені та побудовані раніше — формули (3) та (7), відповідно.

У табл. 4 наведено набір вирішальних правил, що були сформовані з використанням бази знань [22].

Таблиця 4

БАЗА ЗНАНЬ ДЛЯ ВИЗНАЧЕННЯ РІВНЯ ВРАЗЛИВОСТІ CRM-СИСТЕМИ

Номер вхідної комбінації	Узагальнені значення груп показників		Вагові коефіцієнти q	Рівень вразливості CRM-системи V
	Рівень сили загрози U	Рівень дієвості засобів захисту Ω		
11	TC_VH	CS_VL	q_{11}	V_VH
12	TC_VH	CS_L	q_{12}	
13	TC_VH	CS_M	q_{13}	
14	TC_H	CS_VL	q_{14}	
15	TC_H	CS_L	q_{15}	
16	TC_M	CS_VL	q_{16}	
21	TC_VH	CS_H	q_{21}	V_H
22	TC_H	CS_M	q_{22}	
23	TC_M	CS_L	q_{23}	
24	TC_L	CS_VL	q_{24}	
31	TC_VH	CS_VH	q_{31}	V_M
32	TC_H	CS_H	q_{32}	
33	TC_L	CS_L	q_{33}	
34	TC_VL	CS_VL	q_{34}	
41	TC_H	CS_VH	q_{41}	V_L
42	TC_M	CS_H	q_{42}	
43	TC_L	CS_M	q_{43}	
44	TC_VL	CS_L	q_{44}	
51	TC_M	CS_VH	q_{51}	V_VL
52	TC_L	CS_H	q_{52}	
53	TC_L	CS_VH	q_{53}	
54	TC_VL	CS_M	q_{54}	
55	TC_VL	CS_H	q_{55}	
56	TC_VL	CS_VH	q_{56}	

Джерело: розробка авторів

Наступним кроком є представлення вирішальних правил з бази знань (табл. 4) щодо визначення рівня вразливості CRM-системи у математичній формі запису за допомогою функцій належності. Наприклад, вирішальне правило для визначення вразливості рівня V_M може бути записане таким чином:

$$\mu^{V-M}(U,\Omega)=q_{31}\left[\mu^{TC\_VH}(U)\bullet\mu^{CS\_VH}(\Omega)\right]\vee q_{32}\left[\mu^{TC\_H}(U)\bullet\mu^{CS\_H}(\Omega)\right]\vee \\ \vee q_{33}\left[\mu^{TC\_L}(U)\bullet\mu^{CS\_L}(\Omega)\right]\vee q_{34}\left[\mu^{TC\_VL}(U)\bullet\mu^{CS\_VL}(\Omega)\right], \quad (9)$$

де $\mu^{V-M}(U,\Omega)$ — функція належності вектора вхідних змінних (U,Ω) значенню V_M результуючої змінної V; q_{3p} — ваговий коефіцієнт p-ї комбінації $(p=\overline{1,4})$ для третього терму (V_M) вихідної змінної V; $\mu^{d_j^{3p}}(U)$ — функція належності параметра U до нечіткого терму $d_j^{3p}\in D$ (D — терм-множина (1)); $\mu^{em_l^{3p}}(\Omega)$ — функція належності параметра Ω до нечіткого терму $em_l^{3p}\in EM$ (EM — терм-множина (6)).

Представлений концептуальний підхід з використанням апарату нечіткої логіки дозволяє отримувати результати оцінювання рівня вразливості CRM-системи на основі попередньо зроблених оцінок низки факторів інформаційного ризику. Подібна модель є гнучкою, адаптивною та може бути налаштована до умов діяльності кожного окремого підприємства.

Методологія аналізу інформаційних ризиків [22] передбачає створення моделі оцінювання ризику за чинником частоти виникнення втрат, яка, в свою чергу, розглядається як складова частоти виникнення подій загрози та рівня вразливості CRM-системи. 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 [22].

Зазвичай, для оцінювання рівня частоти виникнення подій загрози використовуються різні методи, підґрунтям яких можуть бути:

- експертні оцінки;
- статистичні дані.

Використання подібних методик передбачає накопичення статистичних даних про події, які реально відбулися, аналіз і класифікацію їх причин, виявлення факторів, від яких вони залежать. Саме за такою інформацією можна оцінити рівень загрози в інформаційних системах. Це дозволяє абстрагуватися від несуттєвих технічних деталей, враховувати не тільки програмно-технічні, але й інші аспекти. Проте даний підхід містить значну частку суб'єктивізму конкретних експертів-аналітиків в оцінюванні того чи іншого чинника.

З огляду на недоліки існуючих підходів виникає необхідність у розробці методики аналізу рівня частоти виникнення подій загрози CRM-системі, що міститиме меншу частку суб'єктивізму та матиме властивості гнучкості й адаптивності за умов подальшого переоцінювання ризиків у процесі функціонування системи. З цією метою можна з успіхом застосувати апарат нечіткої логіки [10, 19—21], який дозволяє не лише налаштовувати модель на програмні та апаратні характеристики системи, але й ураховувати специфіку конкретної організації, підприємства, для яких проводиться аналіз.

На першому етапі необхідно сформувати набір окремих показників, які є найважливішими для оцінювання рівня частоти виникнення подій загрози CRM-системі. Наприклад, можна враховувати такий набір критеріїв:

— статистика зареєстрованих несприятливих подій у системах подібної структури;

— тенденції в статистиці за подібними порушеннями;

— наявність у системі інформації, в якій можуть бути зацікавлені потенційні внутрішні чи зовнішні порушники;

— оцінка моральних якостей персоналу;

— можливість отримати вигоду зі зміни інформації, що опрацьовується системою;

— наявність альтернативних способів доступу до інформації;

— статистика порушень в інших інформаційних системах організації.

Слід зазначити, що описаний набір критеріїв запропонований лише як приклад. Він є одним із можливих варіантів оцінювання рівня частоти виникнення подій загрози і може або формуватись експертом для кожної окремої CRM-системи індивідуально з урахуванням специфіки, або для оцінювання може використовуватися табл. 5.

Таблиця 5

ШКАЛА ОЦІНЮВАННЯ ЧАСТОТИ ВИНИКНЕННЯ ПОДІЙ ЗАГРОЗИ

дуже висока (TEF_VH)	> 100 разів на рік
висока (TEF_H)	від 10 до 100 разів на рік
середня (TEF_M)	від 1 до 10 разів на рік
низька (TEF_L)	від 0,1 до 1 разів на рік
дуже низька (TEF_V)	< 0,1 разів на рік (менше ніж раз на 10 років)

Джерело: [22]

Для оцінювання та опрацювання лінгвістичної змінної H, що відповідає частоті виникнення подій загрози, сформовано шкалу з п'яти якісних термів: TEF_VH — «дуже високий», TEF_H — «високий», TEF_M — «середній», TEF_L — «низький», TEF_VL — «дуже низький» рівень частоти виникнення подій загрози. Терм-множина пояснюючої змінної H матиме вигляд:

$$TEF = \{TEF\_VH, TEF\_H, TEF\_M, TEF\_L, TEF\_VL\}. \quad (10)$$

Для оцінювання значень кінцевої лінгвістичної змінної X_1, що є множиною ступенів частоти виникнення можливих втрат, використовуються терми: LEF_VH — «дуже висока» частота, LEF_H — «висока», LEF_M — «середня», LEF_L — «низька», LEF_VL — «дуже низька». Терм-множина вихідної змінної X_1 матиме вигляд:

$$LEF = \{LEF\_VH, LEF\_H, LEF\_M, LEF\_L, LEF\_VL\}. \quad (11)$$

На підставі розрахованих значень груп показників проводиться оцінювання рівня частоти виникнення можливих втрат активів інформаційної системи внаслідок впливу загроз:

$$X_1 = f_{X_1}(V, H). \quad (12)$$

Наступним етапом аналізу є формування системи нечітких знань для визначення кожного з рівнів частоти можливих втрат.

Відповідно до [22] сформовано набір вирішальних правил, які реалізують співвідношення (12). У табл. 6 наведено базу знань для визначення рівня частоти можливих втрат інформаційних активів.

Таблиця 6

БАЗА ЗНАНЬ ДЛЯ ВИЗНАЧЕННЯ РІВНЯ ЧАСТОТИ МОЖЛИВИХ ВТРАТ АКТИВІВ ВІД ІНФОРМАЦІЙНИХ РИЗИКІВ

Номер вхідної комбінації	Узагальнені значення груп показників		Вагові коефіцієнти δ	Кінцева змінна X_1
	Рівень частоти виникнення подій загрози H	Рівень вразливості V		
11	TEF_VH	V_M	δ_{11}	LEF_VH
12	TEF_VH	V_H	δ_{12}	
13	TEF_VH	V_VH	δ_{13}	
21	TEF_H	V_M	δ_{21}	LEF_H
22	TEF_H	V_H	δ_{22}	
23	TEF_H	V_VH	δ_{23}	
31	TEF_VH	V_VL	δ_{31}	LEF_M
32	TEF_H	V_L	δ_{32}	
33	TEF_M	V_M	δ_{33}	
34	TEF_M	V_H	δ_{34}	
35	TEF_M	V_VH	δ_{35}	
41	TEF_H	V_VL	δ_{41}	LEF_L
42	TEF_M	V_L	δ_{42}	
43	TEF_L	V_M	δ_{43}	
44	TEF_L	V_H	δ_{44}	
45	TEF_L	V_VH	δ_{45}	

Закінчення табл. 6

Номер вхідної комбінації	Узагальнені значення груп показників		Вагові коефіцієнти δ	Кінцева змінна X_1
	Рівень частоти виникнення подій загрози H	Рівень вразливості V		
51	TEF_M	V_VL	δ_{51}	LEF_VL
52	TEF_L	V_VL	δ_{52}	
53	TEF_L	V_L	δ_{53}	
54	TEF_VL	V_VL	δ_{54}	
55	TEF_VL	V_L	δ_{55}	
56	TEF_VL	V_M	δ_{56}	
57	TEF_VL	V_H	δ_{57}	
58	TEF_VL	V_VH	δ_{58}	

Джерело: розробка авторів

Наступним кроком є представлення у математичній формі запису вирішальних правил визначення рівнів частоти виникнення можливих втрат. Наприклад, вирішальне правило для визначення частоти можливих втрат рівня LEF_L з табл. 5 може бути записане таким чином:

$$\begin{aligned}\mu^{LEF\_L}(H,V) = {} & \delta_{41}\left[\mu^{TEF\_H}(H) \bullet \mu^{V\_VL}(V)\right] \vee \\ \vee\, & \delta_{42}\left[\mu^{TEF\_M}(H) \bullet \mu^{V\_L}(V)\right] \vee \delta_{43}\left[\mu^{TEF\_L}(H) \bullet \mu^{V\_M}(V)\right] \vee \\ \vee\, & \delta_{44}\left[\mu^{TEF\_L}(H) \bullet \mu^{V\_H}(V)\right] \vee \delta_{45}\left[\mu^{TEF\_L}(H) \bullet \mu^{V\_VH}(V)\right],\end{aligned} \qquad (13)$$

де $\mu^{LEF\_L}(H,V)$ — функція належності вектора вхідних змінних значенню LEF_L вихідної змінної X_1; δ_{4p} — ваговий коефіцієнт для p-ї комбінації $\left(p = \overline{1,5}\right)$ четвертого терму (LEF_L) вихідної змінної; $\mu^{tf_j}(H)$ — функція належності параметра H до нечіт-

кого терму $tf_j \in TEF$ (TEF — терм-множина (10)); $\mu^{vl_i}(V)$ — функція належності параметра V до нечіткого терму $vl_i \in VL$ (VL — терм-множина (8)).

Подібним чином формується вся база знань з використанням експертних даних і виводиться система нечітких логічних рівнянь.

Аналіз факторів інформаційних ризиків дає підстави визначити шість форм збитків внаслідок дії інформаційних ризиків [12, 13, 22]:

1) зниження продуктивності — зменшення спроможності підприємства генерувати первинну пропозицію (товари, послуги тощо) з відповідним падінням прибутку;

2) реакція — витрати, що пов'язані з управлінням подіями збитків (можлива відповідь на дії агента загрози);

3) заміна — витрати, пов'язані з заміною втрачених або пошкоджених активів (ремонт обладнання, придбання та заміна комп'ютера тощо);

4) штрафи та покарання — адміністративні та інші стягнення щодо підприємства;

5) перевага конкурентів — втрати активів (комерційні таємниці, плани тощо), що призводять до зниження конкурентоспроможності підприємства;

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

Вичерпний кількісний аналіз можливих збитків не завжди можливий через нестачу інформації про систему або діяльність підприємства, що аналізується, відсутність або нестачу даних про відмови, впливи людського фактора. За таких обставин може виявитись ефективним порівняльне кількісне або якісне ранжування ризику фахівцями, які є добре інформованими в даній галузі та функціонуванні подібних CRM-систем.

Сформулюємо формалізований підхід до оцінювання величини можливих втрат інформаційних активів з використанням нечітких описів. Для моделювання можливого обсягу збитків внаслідок дії агента загрози розглядаються тільки первинні фактори втрат, що лежать у площині вартості інформаційного активу. Так, величину втрати X_2 інформаційних активів пропонується характеризувати за факторами:

V_1 — зниження продуктивності;

V_2 — внутрішні витрати (реакція);

V_3 — вартість заміни активу;

V_4 — штрафи та санкції;

V_5 — втрати, що призводять до зниження конкурентоспроможності організації;

V_6 — репутація організації.

Оцінювання фактору V_j, $j=\overline{1,6}$, проводиться експертом за шкалою: L_VH — «збитки дуже великі», L_H — «збитки великі», L_M — «збитки середні», L_L — «збитки малі», L_VL — «збитки дуже малі». Тобто, терм-множина вхідних змінних може бути представлена у вигляді:

$$LA=\{L\_VH, L\_H, L\_M, L\_L, L\_VL\}. \qquad (14)$$

Для оцінювання та опрацювання лінгвістичного показника X_2 сформовано шкалу з шести якісних термів: PL_VH — «дуже високий» рівень збитків, PL_H — «високий», PL_Sg — «суттєвий», PL_M — «середній», PL_L — «низький», PL_VL — «дуже низький» рівень збитків у відповідних грошових одиницях відносно бюджету проекту інформаційної системи. Терм-множина вихідної змінної X_2 записується у вигляді:

$$LD=\{PL\_VH, PL\_H, PL\_Sg, PL\_M, PL\_L, PL\_VL\}. \qquad (15)$$

На підставі значень групи показників V_j, $j=\overline{1,6}$, проводиться оцінювання величини можливих збитків інформаційних активів CRM-системи від інформаційних ризиків:

$$X_2=\vartheta_{X_2}(V_1,V_2,V_3,V_4,V_5,V_6). \qquad (16)$$

Базу нечітких знань, що реалізує функцію (16) оцінювання величини можливих збитків інформаційних активів від інформаційних ризиків, можна подати у вигляді табл. 7.

Таблиця 7

БАЗА НЕЧІТКИХ ЗНАНЬ СТОСОВНО ВЕЛИЧИНИ МОЖЛИВИХ ЗБИТКІВ ІНФОРМАЦІЙНИХ АКТИВІВ

Номер вхідної комбінації	Вхідні змінні						Вагові коефіцієнти w	Вихідна змінна X_2
	V_1	V_2	V_3	V_4	V_5	V_6		
11	L_VH	L_VH	L_VH	L_VH	L_VH	L_VH	w_{11}	PL_VH
12	L_VH	L_VH	L_VH	L_VH	L_VH	L_H	w_{12}	
…								
$1k_1$	L_H	L_H	L_H	L_VH	L_VH	L_VH	w_{1k_1}	
21	L_H	L_H	L_H	L_H	L_VH	L_VH	w_{21}	PL_H
22	L_H	L_H	L_H	L_H	L_H	L_VH	w_{22}	
…								
$2k_2$	L_H	L_H	L_H	L_H	L_M	L_M	w_{2k_2}	
31	L_H	L_H	L_H	L_M	L_M	L_M	w_{31}	PL_Sg
32	L_H	L_H	L_M	L_M	L_M	L_M	w_{32}	
…								
$3k_3$	L_M	L_M	L_M	L_M	L_H	L_H	w_{3k_3}	
41	L_M	L_M	L_M	L_M	L_M	L_H	w_{41}	PL_M
42	L_M	L_M	L_M	L_M	L_M	L_M	w_{42}	
…								
$4k_4$	L_L	L_L	L_L	L_M	L_M	L_M	w_{4k_4}	
51	L_L	L_L	L_L	L_L	L_M	L_M	w_{51}	PL_L
52	L_L	L_L	L_L	L_L	L_L	L_M	w_{52}	
…								
$5k_5$	L_VL	L_VL	L_VL	L_L	L_L	L_L	w_{5k_5}	
61	L_VL	L_VL	L_VL	L_VL	L_L	L_L	w_{61}	PL_VL
62	L_VL	L_VL	L_VL	L_VL	L_VL	L_L	w_{62}	
…								
$6k_6$	L_VL	L_VL	L_VL	L_VL	L_VL	L_VL	w_{6k_6}	

Джерело: розробка авторів

Систему нечітких знань для опису моделі оцінювання величини можливих збитків інформаційних активів CRM-системи від інформаційних ризиків можна записати у вигляді:

$$\mu^{ld_i}(V_1,V_2,\ldots,V_6)=\bigvee_{p=1}^{k_i}\left(w_{ip}\left[\bigwedge_{j=1}^{6}\mu^{la_j^{ip}}(V_j)\right]\right), i=\overline{1,6}, \tag{17}$$

де $\mu^{ld_i}(V_1,V_2,\ldots,V_6)$ — функція належності вектора вхідних змінних $(V_1,V_2,\ldots,V_6)$ значенню вихідної змінної ld_i з множини (15); k_i — кількість комбінацій значень змінних $(V_1,V_2,\ldots,V_6)$, для яких вихідна змінна приймає значення ld_i з множини (15); w_{ip} — ваговий коефіцієнт для відповідної комбінації; $\mu^{la_j^{ip}}(V_j)$ — функція належності вхідної змінної V_j до нечіткого терму la_j^{ip} з множини (14).

На підставі розрахованих значень груп показників рівня частоти виникнення можливих втрат інформаційних активів і величини можливих збитків внаслідок інформаційних ризиків проводиться оцінювання загального рівня інформаційних ризиків у CRM-системі:

$$Y = f_Y(X_1, X_2), \tag{18}$$

де X_1 — оцінка рівня частоти виникнення втрат інформаційних активів; X_2 — попередньо оцінена величина можливих збитків.

Для оцінювання та опрацювання лінгвістичної змінної Y вирішено скористатись шкалою з чотирьох якісних термів: C — «критичний», H — «високий», M — «середній», L — «низький» рівень ризику. Терм-множина вихідної змінної Y представляється у вигляді:

$$IR = \{C, H, M, L\}. \tag{19}$$

Для опису функції (18) здійснюється формування системи нечітких знань для визначення кожного з рівнів інформаційних ризиків. Використовуючи [10, 19] сформовано набір вирішальних правил, які реалізують співвідношення (18), що зведено до табл. 8.

Таблиця 8

БАЗА ЗНАНЬ ДЛЯ ВИЗНАЧЕННЯ РІВНЯ ІНФОРМАЦІЙНИХ РИЗИКІВ

Номер вхідної комбінації	Узагальнені значення груп показників		Вагові коефіцієнти m	Вихідна змінна Y
	Рівень частоти виникнення можливих втрат X_1	Величина можливих збитків X_2		
11	LEF_M	PL_VH	m_{11}	C
12	LEF_H	PL_VH	m_{12}	
13	LEF_VH	PL_VH	m_{13}	
14	LEF_H	PL_H	m_{14}	
15	LEF_VH	PL_H	m_{15}	
16	LEF_VH	L_Sg	m_{16}	
21	LEF_VL	PL_VH	m_{21}	H
22	LEF_L	PL_VH	m_{22}	
23	LEF_L	PL_H	m_{23}	
24	LEF_M	PL_H	m_{24}	
25	LEF_M	L_Sg	m_{25}	
26	LEF_H	L_Sg	m_{26}	
27	LEF_H	PL_M	m_{27}	
28	LEF_VH	PL_M	m_{28}	
29	LEF_VH	PL_L	m_{29}	
31	LEF_VL	PL_H	m_{31}	M
32	LEF_VL	L_Sg	m_{32}	
33	LEF_L	L_Sg	m_{33}	
34	LEF_L	PL_M	m_{34}	
35	LEF_M	PL_M	m_{35}	
36	LEF_M	PL_L	m_{36}	
37	LEF_H	PL_L	m_{37}	
38	LEF_H	PL_VL	m_{38}	
39	LEF_VH	PL_VL	m_{39}	

Закінчення табл. 8

Номер вхідної комбінації	Узагальнені значення груп показників		Вагові коефіцієнти m	Вихідна змінна Y
	Рівень частоти виникнення можливих втрат X_1	Величина можливих збитків X_2		
41	LEF_VL	PL_M	m_{41}	L
42	LEF_VL	PL_L	m_{42}	
43	LEF_L	PL_L	m_{43}	
44	LEF_VL	PL_VL	m_{44}	
45	LEF_L	PL_VL	m_{45}	
46	LEF_M	PL_VL	m_{46}	

Джерело: розробка авторів

Вирішальні правила визначення рівнів інформаційних ризиків з табл. 8 за допомогою функцій належності набувають математичної форми запису, приклад якого для визначення інформаційних ризиків рівня *M* може бути представлений таким чином:

$$\begin{aligned}\mu^{M}(X_1,X_2) = {} & m_{31}\left[\mu^{LEF\_VL}(X_1)\bullet\mu^{PL\_H}(X_2)\right]\vee \\ \vee\, & m_{32}\left[\mu^{LEF\_VL}(X_1)\bullet\mu^{PL\_Sg}(X_2)\right]\vee m_{33}\left[\mu^{LEF\_L}(X_1)\bullet\mu^{PL\_Sg}(X_2)\right]\vee \\ \vee\, & m_{34}\left[\mu^{LEF\_L}(X_1)\bullet\mu^{PL\_M}(X_2)\right]\vee m_{35}\left[\mu^{LEF\_M}(X_1)\bullet\mu^{PL\_M}(X_2)\right]\vee \\ \vee\, & m_{36}\left[\mu^{LEF\_M}(X_1)\bullet\mu^{PL\_L}(X_2)\right]\vee m_{37}\left[\mu^{LEF\_H}(X_1)\bullet\mu^{PL\_L}(X_2)\right]\vee \\ \vee\, & m_{38}\left[\mu^{LEF\_H}(X_1)\bullet\mu^{PL\_VL}(X_2)\right]\vee m_{39}\left[\mu^{LEF\_VH}(X_1)\bullet\mu^{PL\_VL}(X_2)\right],\end{aligned} \qquad (20)$$

де $\mu^{M}(X_1, X_2)$ — функція належності вихідної змінної Y нечіткому значенню M з терм-множини (19); $m_{3p}(p=\overline{1,9})$ — ваговий коефіцієнт *p*-ї комбінації для визначення третього терму (*M*) вихідної змінної; $\mu^{lef_j}(X_1)$ — функція належності параметра X_1 до

нечіткого терму lef_j з терм-множини LEF (11); $\mu^{ld_i}(X_2)$ — функція належності параметра X_2 до нечіткого терму ld_i з терм-множини LD (15).

Аналогічним чином виводиться система нечітких логічних рівнянь для інших термів вихідної змінної на основі бази знань з табл. 8. Результатом застосування запропонованого концептуального підходу та інструментарію оцінювання частоти виникнення втрат і величини можливих втрат інформаційних активів є лінгвістичний опис загального рівня інформаційних ризиків у CRM-системі.

Графічне представлення функції належності вихідної змінної Y та результату моделювання інформаційних ризиків в CRM-системі на основі сконструйованої бази логічного висновку зображені на рис. 2 та 3, відповідно.

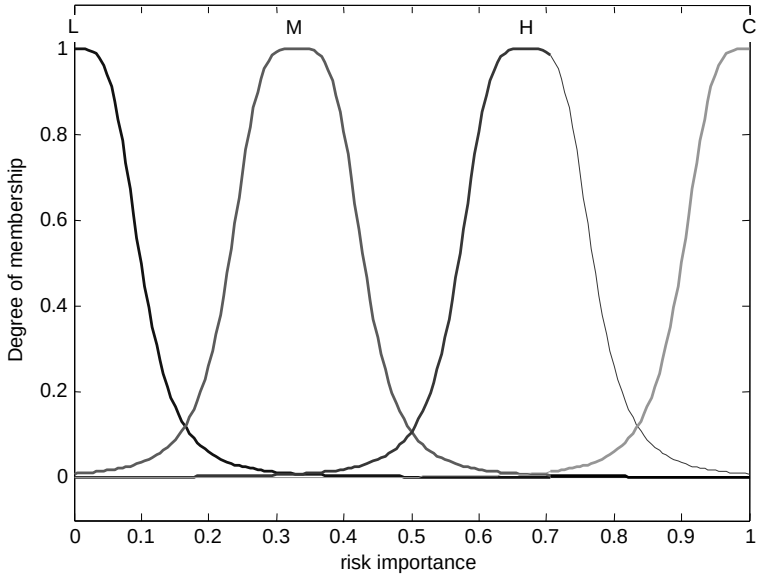

Рис. 2. Графіки функцій належності показника рівня інформаційних ризиків у CRM-системі

Джерело: розробка авторів

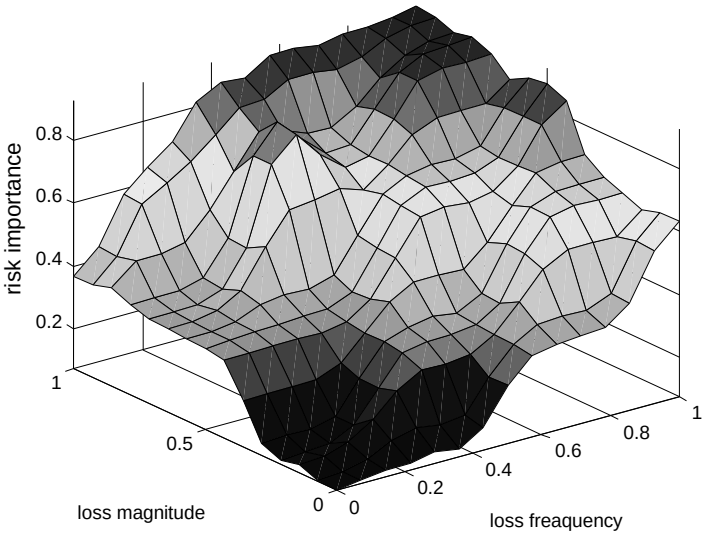

Рис. 3. Моделювання рівня інформаційних ризиків
Джерело: розробка авторів

Результати проведених модельних розрахунків щодо оцінювання рівня інформаційних ризиків у CRM-системах трьох підприємств представлено в табл. 9.

Таблиця 9

ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНИХ РИЗИКІВ В CRM-СИСТЕМАХ ПІДПРИЄМСТВ

Назва підприємства	Величина можливих збитків	Рівень частоти можливих втрат	Рівень інформаційних ризиків
Підприємство 1	PL_M	LEF_L	M
	0,41	0,34	0,38
Підприємство 2	PL_Sg	LEF_M	H
	0,49	0,57	0,63
Підприємство 3	PL_Sg	LEF_VH	C
	0,61	0,98	0,89

Джерело: розробка авторів

Дані розрахунків у табл. 9 свідчать, що на Підприємстві 1 рівень інформаційних ризиків відповідає оцінці «середній», на Підприємстві 2 — оцінці «високий», на Підприємстві 3 — оцінці «критичний».

Відповідно до результатів оцінювання чинників інформаційних ризиків було прийняте рішення щодо методів зниження рівня інформаційних ризиків на підприємствах. Наприклад, на Підприємстві 2 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 інформаційній безпеці підприємства. Підприємству 3 було надано рекомендації щодо перегляду політики інформаційної безпеки, що була прийнята раніше.

Висновки і перспективи подальших досліджень

Аналіз інформаційних ризиків є основою для побудови системи управління інформаційною безпекою підприємства. В результаті проведення дослідження сформульовано концептуальний підхід, що передбачає в процесі аналізу інформаційних ризиків дотримання таких кроків: ідентифікація інформаційних ресурсів (активів) компанії, що можуть бути об'єктом ризику, можливих загроз активу та визначення рівня загроз безпеки CRM-системі підприємства; оцінювання рівня дієвості засобів контролю безпеки CRM-системи; оцінювання вразливості CRM-системи, що розглядається як результат впливу факторів імовірного рівня сили загрози та рівня дієвості засобів контролю; оцінювання частоти виникнення можливих втрат від інформаційних ризиків як результат впливу факторів частоти виникнення загрози та вразливості CRM-системи; оцінювання величини можливих збитків від інформаційних ризиків у CRM-системі; оцінювання рівня інформаційних ризиків у CRM-системі як результуючої двох факторів: частоти виникнення втрат і величини можливих втрат від інформаційних ризиків.

Побудовано модель оцінювання загального рівня інформаційних ризиків у CRM-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: заміну чи модифікацію засобів контролю безпе-

ки; впровадження механізмів захисту відповідно до можливого рівня загроз певних класів порушників інформаційної безпеки; реалізацію режиму функціональної замкнутості, який виключав би використання апаратного та програмного забезпечення, що не має відповідного паспорту безпеки, тощо.

Результатом застосування запропонованого концептуального підходу та інструментарію оцінювання рівня інформаційних ризиків у CRM-системі є лінгвістичний опис і кількісна оцінка факторів інформаційних ризиків, а саме — рівня частоти виникнення можливих загроз і вразливості CRM-системи. Розроблений концептуальний підхід дозволяє формувати модель не тільки з можливістю її адаптації до конкретної інформаційної системи, але й із забезпеченням здатності до переоцінки ризику надалі. Подібна модель характеризується властивостями гнучкості та адаптивності, можливістю налаштування у відповідності до одержаної бази даних.

Запропонована модель оцінювання рівня інформаційних ризиків може бути покладена в основу розбудови системи управління інформаційними ризиками як на стадії проектування CRM-системи підприємства, так і в ході її експлуатації. При цьому не вимагається кардинально змінювати організаційну структуру підприємства. Необхідно лише реорганізувати її, максимально пристосувати до розв'язання задач управління інформаційними ризиками.

Незважаючи на обсяг виконаних досліджень, залишається низка невирішених проблем, а саме: розбудова математичних моделей і відповідного інструментарію для зниження (для факторів вразливості) чи підвищення (для факторів дієвості засобів захисту) впливу чинників на загальний рівень інформаційних ризиків; розробка положень щодо застосування механізмів управління окремими чинниками інформаційних ризиків.

Література

1. Функции CRM-систем [Електронний ресурс]. — Режим доступу: http://www.crmonline.ru/crm/functions.

2. Information Technology. Information Security. Information Assurancy [Електронний ресурс]. — Режим доступу : http://www.isaca.org.

3. *Bernstein P.* Against the Gods: The Remarkable Story of Risk / P. Bernstein. — New York : John Wiley & Sons, Inc, 1996. — 395 p.

4. *Markovitz H.* Portfolio Selection. Efficient diversification of investments / H. Markovitz. — New York : John Wiley & Sons, Inc, 1959. — 344 p.

5. *Найт Ф. Х.* Риск, неопределенность и прибыль / Ф. Х. Найт. — М.: Дело, 2003. — 360 с.

6. *Самуэльсон П.* Экономика / П. Самуэльсон, В. Нордхаус. — М. : Вильямс, 2006. — 1360 с.

7. *Вітлінський В. В.* Ризикологія в економіці та підприємництві / В. В. Вітлінський, Г. І. Великоіваненко. — К. : КНЕУ, 2004. — 480 с.

8. *Галіцин В. К.* Структурно-функціональний аналіз та моделювання розвитку економіки: монографія / В. К. Галіцин, О. П. Суслов, О. В. Галіцина, Н. К. Самченко. — К. : КНЕУ, 2013. — 377 с.

9. *Клейнер Г. Б.* Предприятия в нестабильной экономической среде: риски, стратегия, безопасность / Г. Б. Клейнер, В. П. Тамбовцев, Р. М. Качалов; под общей ред. Панова С. А. — М. : ОАО Экономика, 1997. — 288 с.

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

11. *Галіцин В. К.* Теорія керування : навч. посібник / В. К. Галіцин, О. П. Суслов. — К. : КНЕУ, 2016. — 416 с.

12. *Завгородний В. И.* Информационные риски и экономическая безопасность предприятия / В. И. Завгородний. — М. : Финакадемия, 2008. — 160 с.

13. *Липаев В. В.* Функциональная безопасность программных средств / В. В. Липаев. — М. : СИНТЕГ, 2004. — 348 с.

14. *Мельник Г. В.* Моделювання загроз ефективного функціонування інформаційної системи на підґрунті інструментарію нечіткої логіки / Г. В. Мельник, В. В. Вітлінський // Моделювання та інформаційні системи в економіці: Збірник наукових праць. — К. : КНЕУ, 2009. — Вип. 79. — С. 22—29.

15. *Байхельт Ф.* Надежность и техническое обслуживание. Математический подход / Ф. Байхельт, П. Франкен. — М. : Радио и связь, 1988. — 392 с.

16. *Зегжда П. Д.* Теория и практика обеспечения информационной безопасности / П. Д. Зегжда. — М. : Яхтсмен, 1996. — 192 с.

17. *Мур М.* Управление информационными рисками / М. Мур // Финансовый директор. — 2003. — № 9. — С. 64—69.

18. *Стенг Д. И.* Секреты безопасности сетей / Д. И. Стенг, С. Мун. — К.: Диалектика, 1996. — 544 с.

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

20. *Zadeh L. A.* On optimal control and linear programming / L. A. Zadeh, B. H. Whalen // IRE Trans. Automatic control. — 1962. — No. 7 (4). — P. 45—46.

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

22. *Jones J. A.* An Introduction to FAIR / J. A. Jones. — Norwich: Norwich University, 2005. — 67 p.

References

1. CRMonline. (2016). *Functions of the CRM-systems*. Retrieved from: http://www.crmonline.ru/crm/functions.
2. Information Technology. Information Security. Information Assurancy. (2016). Retrieved from: http://www.isaca.org.
3. Bernstein, P. (1996). *Against the Gods: The Remarkable Story of Risk*. New York: John Wiley & Sons, Inc.
4. Markovitz, H. (1959). *Portfolio Selection. Efficient diversification of investments*. New York : John Wiley & Sons, Inc.
5. Nayt, F. H. (2003). *Risk, neopredelennost' i pribyl'*. Moscow, Russia: Delo [in Russian].
6. Samuelson, P., & Nordhaus, V. (2006). *Ekonomika*. Moscow, Russia: Vilyams [in Russian].
7. Vitlins'kyy, V. V. (2004). *Ryzykolohiya v ekonomitsi ta pidpryyemnytstvi*. Kyiv, Ukraine : KNEU [in Ukrainian].
8. Halitsyn, V. K., Suslov, O. P., Halitsyna, O. V., & Samchenko, N. K. (2013). *Strukturno-funktsional'nyy analiz ta modelyuvannya rozvytku ekonomiky*. Kviv. Ukraine : KNEU [in Ukrainian].
9. Klevner, H. B., Tambovtsev, V. P., & Kachalov, R. M. (1997). *Predprivativa v nestabilnov ekonomicheskoy srede: riski, strategiya, bezopasnost*. — Moscow, Russia : Ekonomika [in Russian].
10. Matviychuk, A. V. (2007). *Modeljuvannja ekonomichnih procesiv iz zastosuvannjam metodiv nechitkoï logiky.* Kyiv, Ukraine : KNEU [in Ukrainian].
11. Halitsyn, V. K., & Suslov, O. P. (2016). *Teoriya keruvannya*. Kyiv, Ukraine : KNEU [in Ukrainian].
12. Zavgorodnij, V. I. (2008). *Informacionnye riski i jekonomicheskaja bezopasnost' predprijatija*. Moscow, Russia: Finakademija [in Russian].
13. Lipaev, V. V. (2004). *Funkcional'naja bezopasnost' programmnyh sredstv*. Moscow, Russia: SINTEG [in Russian].
14. Melnyk, H. V., & Vitlins'kyy, V. V. (2009). Modelyuvannya zahroz efektyvnoho funktsionuvannya informatsiynoyi systemy na pidgrunti instrumentariyu nechitkoyi lohiky. *Modelyuvannya ta informatsiyni systemy v ekonomitsi (Modeling and information systems in the economy)*, *79*, 22—29 [in Ukrainian].
15. Bavhelt, F., & Franken, P. (1988). *Nadezhnost i tehnicheskoe obslu zhivanie. Matematicheskiy podhod.* Moscow, Russia: Radio i svyaz [in Russian].
16. Zegzhda, P. D. (1996). *Teoriya i praktika obespecheniya informatsionnoy bezopasnosti*. Moscow, Russia : Yahtsmen [in Russian].
17. Mur, M. (2003). Upravlenie informacionnymi riskami. *Finansovyj direktor (Financial Director)*, *9*, 64—69 [in Russian].

18. Steng, D. I., & Mun, S. (1996). *Sekrety bezopasnosti setej*. Kyiv, Ukraine: Dialektika [in Russian].

19. Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*, 338—353.

20. Zadeh, L. A., & Whalen, B. H. (1962). On optimal control and linear programming. *IRE Trans. Automatic control*, *7*(4), 45—46.

21. Zimmermann. H.-J. (1987). *Fuzzy Sets, Decision Making and Expert Systems*. Kluwer: Dordrecht.

22. Jones, J. A. (2005). *An Introduction to FAIR*. Norwich: Norwich University.

Стаття надійшла до редакції 3.03.2016