УДК 004.056

СИСТЕМА ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Кочетков О.В.[1], Гаур Т.О.[2], Машін В.М.[2]

[1] Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна, 1.
[2]Одеський національний морський університет,
65000, Україна, м. Одеса, вул. Мечникова, 34.
[1]kmkakbn@gmail.com, [2]mebarka@mail.ru, [2]mashin@ua.fm,

СИСТЕМА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ

Кочетков А.В.[1], Гаур Т.А.[2], Машин В.Н.[2]

[1] Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
[2]Одесский национальный морской университет,
65000, Украина, г. Одесса, ул. Мечникова, 34.
[1]kmkakbn@gmail.com, [2]mebarka@mail.ru, [2]mashin@ua.fm,

THE ENTERPRISE INFORMATION SECURITY RISK ASSESSMENT SYSTEM BASED ON FUZZY LOGIC

Kochetkov A.V.[1], Gaur T.A.[2], Mashin V.N. [2]

[1]O.S. Popov Odessa national academy of telecommunications,
1 Kuznechna St., Odesa, 65029, Ukraine.
[2]Odessa national maritime university,
34 Mechnikova str, Odessa 65029, Ukraine.
[1]kmkakbn@gmail.com, [2]mebarka@mail.ru, [2]mashin@ua.fm,

Анотація. В роботі розглядається процес створення нечіткої продукційної моделі оцінки ризику інформаційної безпеки підприємства. Показано, що традиційні методи недостатньо придатні для вирішення подібних завдань саме тому, що вони не завжди взмозі чітко описати умови і надати необхідні дані для прийняття відповідних рішень, як правило, виникає невизначеність. Показано, що існуючі методи урахування та оцінки ризиків не позбавлені суб'єктивізму й суттєвих умов, що призводять до неправильних оцінок ризиків проектів. Суттєво, що якісно виконаний аналіз інформаційних ризиків дозволяє провести порівняльний аналіз «ефективність – вартість» різних варіантів захисту, обрати адекватні контрзаходи і засоби контролю, оцінити рівень залишкових ризиків. Крім того, інструментальні засоби аналізу ризиків, що ґрунтуються на сучасних базах знань і процедурах логічного висновку, дозволяють побудувати структурні та об'єктно-орієнтовані моделі інформаційних активів компанії, моделі загроз і моделі ризиків, пов'язаних з окремими інформаційними та бізнес-транзакціями і, отже, виявляти такі інформаційні активи компанії, ризик порушення захищеності яких є критичним, тобто неприйнятним. Запропоновано використання теорії нечіткої логіки для оцінки ризиків.

Для моделювання ризику інформаційної безпеки підприємства, запропоновано нечіткі моделі надавати у вигляді нечітких мереж. Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збиток організації. Взаємозв'язок між факторами (антецедентом) і показниками ризику (консеквентом) являє собою бінарне нечітке відношення на декартовому множенні відповідних нечітких множин. Нечітке причинно-наслідкове відношення між антецеденом і консеквентом задається у вигляді нечіткої продукції. Використовуваний в методиці

механізм отримання оцінок ризику на основі нечіткої логіки дозволяє отримати чисельне значення ризику, лінгвістичний опис ступеня ризику, а також рівень впевненості експерта у виникненні ризикової події.

Ключові слова: продукційна модель, інформаційна безпека, показники ризику, нечітка логіка, оцінки ризику.

Аннотация. В работе рассматривается процесс создания нечеткой продукционной модели оценки риска информационной безопасности предприятия. Показано, что традиционные методы недостаточно пригодны для решения подобных задач именно потому, что они не всегда в состоянии четко описать условия и предоставить необходимые данные для принятия соответствующих решений, как правило, возникает неопределенность. Показано, что существующие методы учета и оценки рисков не лишены субъективизма и важных условий, приводящих к неправильным оценкам рисков проектов. Существенно, что качественно выполненный анализ информационных рисков позволяет провести сравнительный анализ «эффективность – стоимость» различных вариантов защиты, выбрать адекватные контрмеры и средства контроля, оценить уровень остаточных рисков. Кроме того, инструментальные средства анализа рисков, основанные на современных базах знаний и процедурах логического вывода, позволяют построить структурные и объектно-ориентированные модели информационных активов компании, модели угроз и модели рисков, связанных с отдельными информационными и бизнес-транзакциями и, следовательно, выявлять такие информационные активы компании, риск нарушения защищенности которых является критическим, то есть неприемлемым. Предложено использование теории нечеткой логики для оценки рисков.

Для моделирования риска информационной безопасности предприятия, предложено нечеткие модели представлять в виде нечетких сетей. Модель содержит базы правил и позволяет проводить лингвистический анализ рисков, которые несут потенциальные угрозы и ущерб организации. Взаимосвязь между факторами (антецедентом) и показателями риска (консеквентом) представляет собой бинарное нечеткое отношение на декартовом умножении соответствующих нечетких множеств. Нечеткое причинно-следственное отношение между антецедентом и консеквентом задается в виде нечеткой продукции. Используемый в методике механизм получения оценок риска на основе нечеткой логики позволяет получить численное значение риска, лингвистическое описание степени риска, а также уровень уверенности эксперта в возникновении рискового события.

Ключевые слова: продукционная модель, информационная безопасность, показатели риска, нечеткая логика, оценки риска.

Abstract. The paper discusses the process of creating a fuzzy production model for assessing the risk of information security of an enterprise. It is shown that traditional methods are not sufficiently suitable for solving such problems precisely because they are not always able to clearly describe the conditions and provide the necessary data for making appropriate decisions, as a rule, uncertainty arises. It is shown that the existing methods of accounting and risk assessment are not deprived of subjectivity and important conditions leading to incorrect estimates of project risks. It is significant that a qualitatively performed analysis of information risks allows us to conduct a comparative analysis of "effectiveness - cost" of various protection options, select adequate countermeasures and controls, and assess the level of residual risks. In addition, risk analysis tools based on modern knowledge bases and inference procedures allow building structural and object-oriented models of information assets of a company, threat models and risk models associated with individual information and business transactions and, therefore, identifying such information assets of the company, the risk of violation of security which is critical, that is unacceptable. The proposed use of the theory of fuzzy logic to assess risks.

To model the information security risk of an organization, it is proposed to present fuzzy models as fuzzy networks. The model contains a rule base and allows for linguistic analysis of risks that pose potential threats and damage to the organization. The relationship between factors (antecedent) and risk indicators (sequential) is a binary fuzzy relation on the Cartesian multiplication of the corresponding fuzzy sets. The fuzzy causal relationship between the antecedent and the sequential is given in the form of fuzzy products. The mechanism used in the methodology for obtaining risk assessments based on fuzzy logic allows obtaining a numerical value of risk, a linguistic description of the degree of risk, as well as the level of expert confidence in the occurrence of a risk event.

Key words: product model, information security, risk indicators, fuzzy logic, risk assessment.

Проблеми прийняття рішень у складних умовах займають у даний час особливе місце в інформаційних технологіях. Математичні методи широко застосовуються для опису й аналізу складних економічних, соціальних та інших систем. Традиційні методи недостатньо придатні для вирішення подібних завдань саме тому, що вони не взмозі описати виникану

невизначеність. Ретельне опрацювання та урахування ризиків стали невід'ємною частиною і важливою складовою успіху діяльності кожної компанії. Проте все частіше компаніям доводиться приймати рішення в умовах невизначеності, які можуть призвести до непередбачуваних наслідків і, відповідно, небажаним результатам і збиткам. Своєчасне виявлення, а також адекватна і найбільш точна оцінка ризиків є однією з нагальних проблем сучасного аналізу. На жаль, існуючі на сьогодні методи урахування та оцінки ризиків не позбавлені суб'єктивізму й суттєвих передумов, що призводять до неправильних оцінок ризику проектів. Теорія нечіткої логіки для оцінки ризику – це новий підхід що динамічно розвивається. Останнім часом нечітке моделювання є одним із найбільш активних і перспективних напрямів прикладних досліджень у галузі управління та прийняття рішень.

Сучасні методики та технології управління інформаційними ризиками дозволяють оцінити існуючий рівень залишкових інформаційних ризиків у вітчизняних компаніях [2]. Це особливо важливо в тих випадках, коли до інформаційної системи компанії застосовуються підвищені вимоги в галузі захисту інформації та безперервності бізнесу. Сьогодні існує низка методик аналізу ризиків, у тому числі з використанням CASE коштів, адаптованих до використання у вітчизняних умовах [1]. Суттєво, що якісно виконаний аналіз інформаційних ризиків дозволяє провести порівняльний аналіз «ефективність – вартість» різних варіантів захисту, вибрати адекватні контрзаходи і засоби контролю, оцінити рівень залишкових ризиків [6, 7]. Крім того, інструментальні засоби аналізу ризиків, що грунтуються на сучасних базах знань і процедурах логічного висновку, дозволяють побудувати структурні та об'єктно-орієнтовані моделі інформаційних активів компанії, моделі загроз і моделі ризиків, пов'язаних з окремими інформаційними та бізнес-транзакціями і, отже, виявляти такі інформаційні активи компанії, ризик порушення захищеності яких є критичним, тобто неприйнятним. Такі інструментальні засоби надають можливість побудувати різні моделі захисту інформаційних активів компанії, порівнювати між собою за критерієм «ефективність-вартість» різні варіанти комплексів заходів захисту та контролю, а також проводити моніторинг виконання вимог з організації режиму інформаційної безпеки вітчизняної компанії [8, 10].

Відомо, що ризик є подією, яка може створити суттєвий збиток. Оцінка ризику – процес, протягом якого виконується визначення збитків або збитку в кількісному або якісному вираженні. В даний час є кілька методологій, за допомогою яких здійснюється оцінка ризиків [3 – 5]. Для моделювання ризику інформаційної безпеки організації, нечіткі моделі [9] доцільно надавати у вигляді нечітких мереж, елементи і сукупності елементів яких реалізують різні компоненти нечітких моделей і етапи нечіткого виводу.

Метою статті є створення системи, що допомагає спростити процес роботи підприємства, відкинувши завідомо неправдиві варіанти, запобігти ризику або звернути увагу підприємця на помилки, неточності і недоліки в його проекті, оптимізувати витрати на засоби контролю та захисту, комплексне планування й управління ризиками на всіх стадіях життєвого циклу інформаційних систем, скоротити час на розробку і супровід корпоративної системи захисту інформації, підтримка безперервності бізнесу, оперативне прийняття рішень з питань управління безпекою.

На основі проведеного аналізу виявлені фактори ризиків, що виникають на кожному з етапів розвитку підприємства.

Наприклад, помилки, здійснені підприємством на етапі прийняття рішень про впровадження інформаційної системи та її вибору, не тільки підвищують імовірність реалізації факторів ризику на наступних етапах, а й посилюють негативні наслідки всіх цих факторів.

У процесі аналізу факторів ризику виявлені показники, які можуть бути джерелами ризику інформаційної безпеки організації:

- програмно-апаратний рівень захисту;
- рівень організаційного захисту;
- рівень правового захисту.

При завданні лінгвістичних змінних, що характеризують фактори ризику, можуть використовуватися такі терм-множини, що визначають рівні факторів:

Т1 = {Низький (Н), Високий (В)};

Т2 = {Низький (Н), Середній (С), Високий (В)};

Т3 = {Дуже Низький (Дн), Низький (Н), Середній (С), Високий (В)};

Т4 = {Дуже Низький (Дн), Низький (Н), Середній (С), Високий (В), Дуже Високий (ДВ)}.

Для програмно-апаратного рівня захисту:

- Дн - незадовільна, для забезпечення початкового рівня захисту;
- Н - задовільна, для забезпечення початкового рівня захисту;
- С - достатня, для базового інформаційного захисту;
- В - повністю відповідає рівню конфіденційності інформації;
- Дв - вищий рівень конфіденційності інформації, що не можливо розсекретити.

Рівень організаційного захисту:

- Дн - дуже слабке планування та відсутність моніторингу уразливостей;
- Н - слабке планування та відсутність моніторингу уразливостей;
- С - планування і моніторинг уразливостей проводяться нерегулярно;
- В - своєчасне планування і моніторинг уразливостей;
- Дв - планове, своєчасне планування і моніторинг уразливостей.

Рівень правового захисту:

- Дн - застаріла та неповна документація;
- Н - уривкова і неповна документація;
- С - документація є, але недостатньо детальна;
- В - документація повна і синхронізована;
- Дв - документація повна і найостанніша (оновлюється).

У процесі аналізу ризику виявлені показники, які можуть характеризувати ризики інформаційної безпеки організації (табл.1).

Таблиця 1 – Показники ризику інформаційної безпеки організації

Позначення	Найменування ЛП	Примітка
Y1	Ризик зниження ефективності захисту	Характеризує потенційну можливість зниження / збільшення ефективності захисту по відношенню до необхідної ефективності для конкретного підприємства
Y2	Ризик виникнення потенційних загроз	Характеризує можливості виникнення потенційних загроз для підприємства
У3	Ризик матеріального збитку	Характеризує можливість виникнення матеріального збитку для підприємства при порушеннях параметрів інформаційної безпеки підприємства

При завданні лінгвістичних змінних, що характеризують показники ризику, використовується наступні терм-множини, що визначають показники ризику:

Т1 = {Низька очевидність ризику (НОР); Середня очевидність ризику (СОР); Висока очевидність ризику (ВОР)};

Т2 = {Дуже низька очевидність ризику (Днор); Низька очевидність ризику (НОР); Середня очевидність ризику (СОР); Висока очевидність ризику (ВОР); Дуже висока очевидність ризику (Двор)}.

Взаємозв'язок між факторами (антецедентом) і показниками ризику (консеквентом) являє собою бінарне нечітке відношення на декартовім множенні відповідних нечітких множин. Нечітке причинно-наслідкове відношення між антецедентом і консеквентом задається у вигляді нечіткої продукції [1]. Продукційні правила надані в табл. 2.

Оператори використовуються для запису комбінацій логічних понять нечіткою логікою, щоб обчислювати ступені істинності. Застосовуються стандартні логічні оператори AND, OR і NOT.

Таблиця 2 – Нечіткі продукційні правила для показника ризику Y_1

Позначення	Антецедент	Консеквент
База правил П1		
П1.1	$(x_1=Н \wedge x_2=Н \wedge x_3=Н) \vee (x_1=С \wedge x_2=Н \wedge x_3=Н) \vee (x_1=Н \wedge x_2=С \wedge x_3=Н)$	Y_1 = Дуже ВОР (дуже висока очевидність ризику)
П1.2	$(x_1=В \wedge x_2=Н \wedge x_3=Н) \vee (x_1=С \wedge x_2=С \wedge x_3=Н) \vee (x_1=Н \wedge x_2=В \wedge x_3=Н) \wedge (x_1=С \wedge x_2=В \wedge x_3=Н) \vee (x_1=Н \wedge x_2=Н \wedge x_3=С) \vee (x_1=Н \wedge x_2=С \wedge x_3=С) \vee (x_1=Н \wedge x_2=В \wedge x_3=С) \vee (x_1=Н \wedge x_2=Н \wedge x_3=В)$	Y_1 = ВОР (висока очевидність ризику)
П1.3	$(x_1=В \wedge x_2=С \wedge x_3=Н) \vee (x_1=В \wedge x_2=В \wedge x_3=Н) \vee (x_1=С \wedge x_2=Н \wedge x_3=С) \vee (x_1=В \wedge x_2=Н \wedge x_3=С) \vee (x_1=С \wedge x_2=С \wedge x_3=С) \vee (x_1=С \wedge x_2=В \wedge x_3=С) \vee (x_1=С \wedge x_2=Н \wedge x_3=В) \vee (x_1=Н \wedge x_2=С \wedge x_3=В) \vee (x_1=С \wedge x_2=С \wedge x_3=В) \vee (x_1=Н \wedge x_2=В \wedge x_3=В)$	Y_1 = СОР (середня очевидність ризику)
П1.4	$(x_1=В \wedge x_2=С \wedge x_3=С) \vee (x_1=В \wedge x_2=В \wedge x_3=С) \vee (x_1=В \wedge x_2=Н \wedge x_3=В) \vee (x_1=В \wedge x_2=С \wedge x_3=В) \vee (x_1=С \wedge x_2=В \wedge x3=В)$	Y_1 = НОР (низька очевидність ризику)
П1.5	$x_1=В \wedge x_2=В \wedge x_3=В$	Y_1 = Дуже НОР (дуже низька очевидність ризику)

Далі, як приклад, розглянемо базу правил для показника ризику Y1.

Бази правил нечіткої логіки, подібно традиційним експертним системам, грунтуються на базі знань, побудованої на основі людського досвіду. У той самий час існують суттєві відмінності в обробці і характеристиках цих знань.

Реалізація процесу нечіткого моделювання бази правил відбувається за допомогою застосування спеціалізованого пакета Fuzzy Logic Toolbox програмного засобу MATLAB [3]. Виконання нечіткого висновку реалізується на основі алгоритму Мамдані (Mamdani).

Підготовка завдання для вирішення методами нечіткої логіки (фазифікації) дозволяє конвертувати реальні значення змінних у нечіткі. На цьому кроці необхідно задати функції приналежності для терм-множин вхідних і вихідних лінгвістичних змінних:

ПАЗ у моделі відповідає лінгвістичній змінній «Програмно-апаратний рівень захисту» - x_1;

ОргЗ у моделі відповідає лінгвістичній змінній «Рівень організаційного захисту» - x_2;

ПравЗ у моделі відповідає лінгвістичній змінній «Рівень правового захисту» - x_3;

РизикЗ відповідає лінгвістичній змінній «Ризик зниження ефективності захисту» - Y_1.

«Програмно-апаратний рівень захисту» буде мати наступний вигляд:
μ_{Δ}^{H} [0 0 0.15 0.35]; μ_{Δ}^{C} [0.15 0.4 0.6 0.85]; μ_{Δ}^{B} [0.65 0.85 1 1].
«Рівень організаційного захисту» буде мати наступний вигляд:
μ_{Δ}^{H} [0 0 0.15 0.35]; μ_{Δ}^{C} [0.15 0.4 0.6 0.85]; μ_{Δ}^{B} [0.65 0.85 1 1].
«Рівень правового захисту» матиме такий вигляд:
μ_{Δ}^{H} [0 0 0.15 0.35]; μ_{Δ}^{C} [0.15 0.4 0.6 0.85]; μ_{Δ}^{B} [0.65 0.85 1 1].
На рис. 1 показані графіки функцій приналежності терм-множин лінгвістичної змінної РизикЗ - «Ризик зниження ефективності захисту».

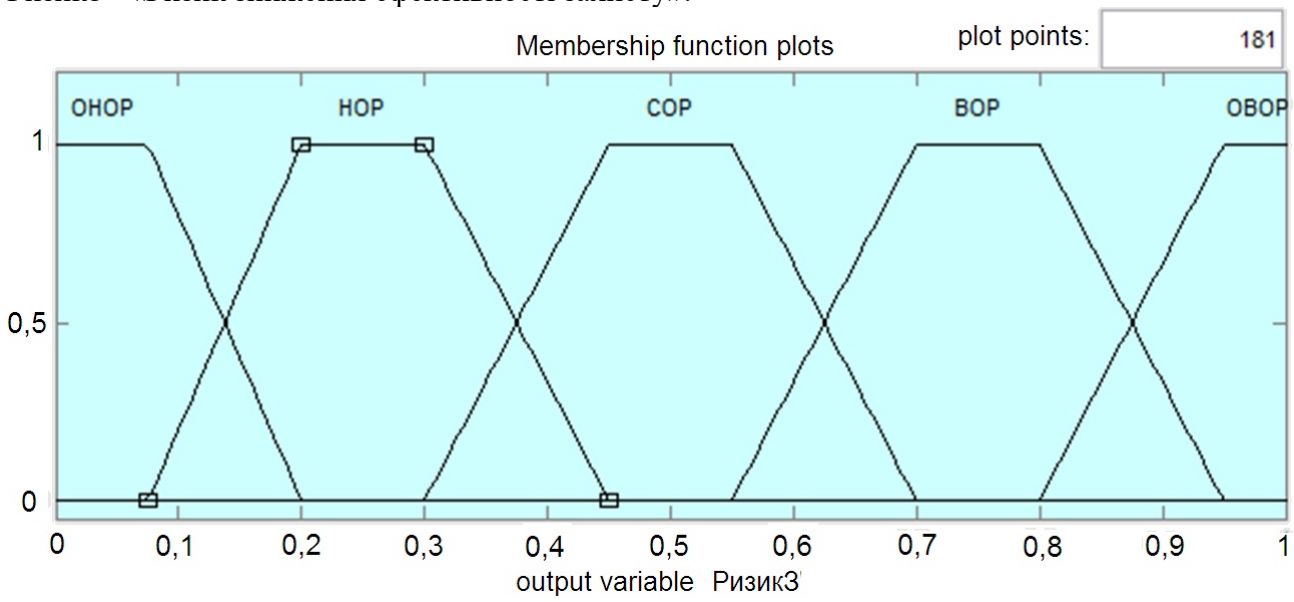

Рисунок 1 – Функції приналежності для вихідної змінної РизикЗ

Для вихідної змінної РизикЗ (лінгвістична змінна «Ризик зниження ефективності захисту») терм-множина складається з п'яти термів:

Т = {Дуже низька очевидність ризику (Днор); Низька очевидність ризику (НОР); Середня очевидність ризику (СОР); Висока очевидність ризику (ВОР); Дуже висока очевидність ризику (Двор)}. Функції належності лінгвістичних змінних є трапецієвидними.

«Ризик зниження ефективності захисту» буде мати наступний вигляд:
$\mu_{\Delta}^{\text{ДНОР}}$ [0 0 0.75 0.2]; $\mu_{\Delta}^{\text{НОР}}$ [0.075 0.2 0.3 0.45]; $\mu_{\Delta}^{\text{СОР}}$ [0.3 0.45 0.55 0.7];
$\mu_{\Delta}^{\text{ВОР}}$ [0.55 0.7 0.8 0.95]; $\mu_{\Delta}^{\text{ДВОР}}$ [0.8 0.95 1 1].

Правила моделі формуються на основі загальних закономірностей поведінки досліджуваної системи і дозволяють «вкласти» у механізм виведення логічну модель прикладного рівня. Правила обчислюються на основі оцінки тверджень кожного правила, що складаються з логічних комбінацій декількох тверджень.

В алгоритмі Мамдані база правил повинна задаватися у вигляді структури з трьома входами і одним виходом (рис. 2).

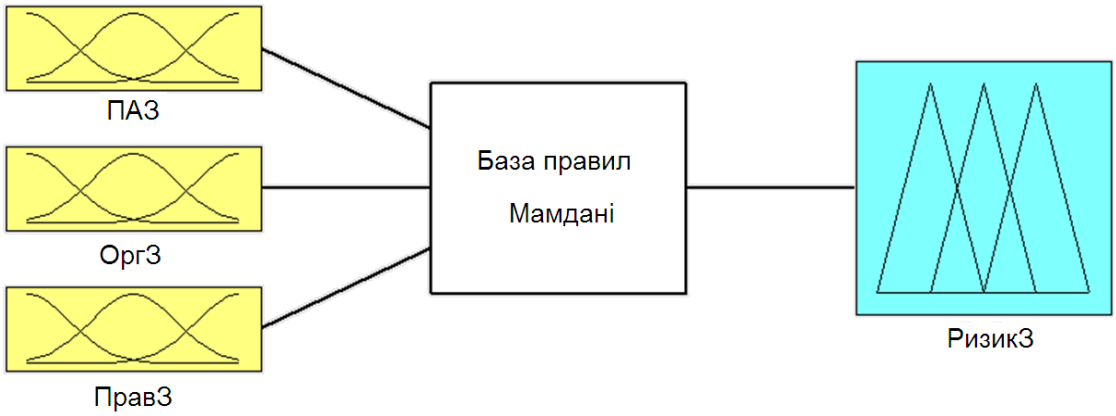

Рисунок 2 – Структура нечіткої моделі для бази правил П1

Функції належності дають можливість визначати поняття нечіткі за своєю природою: "дуже низька очевидність ризику", "низька очевидність ризику", "середня очевидність ризику", "висока очевидність ризику", "дуже висока очевидність ризику". На рис. 3 показана поверхня залежності вихідної лінгвістичної змінної від двох вхідних з фіксованим значенням третьої змінної для бази правил П1 нечіткої моделі.

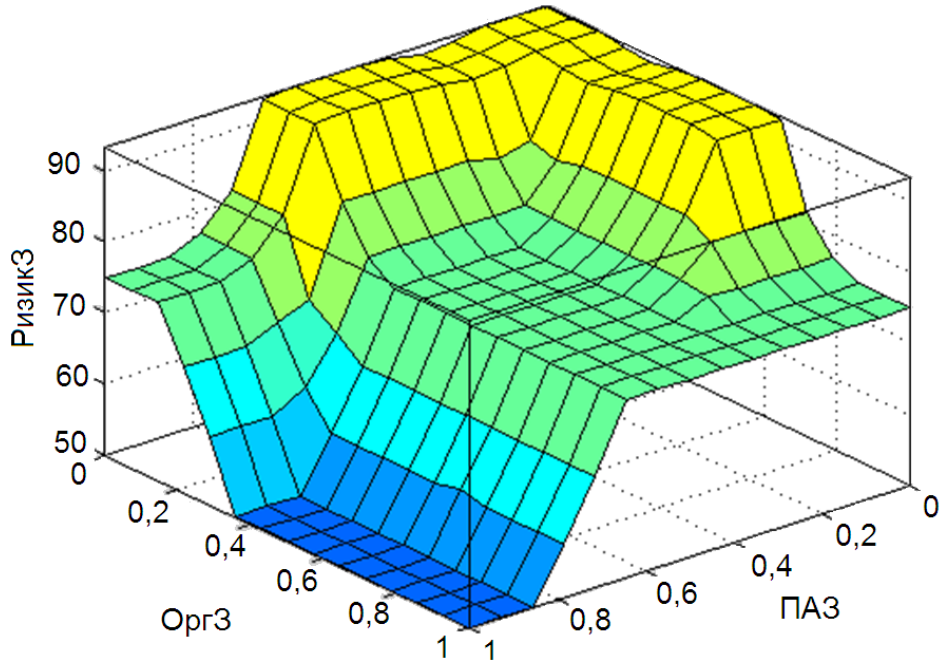

Рисунок 3 – Графічний вид залежностей вихідної лінгвістичної змінної РизикЗ від ПАЗ і ОргЗ

Графічний вид залежностей вихідної лінгвістичної змінної РизикЗ - «Ризик зниження ефективності захисту» від вхідних значень змінних ПАЗ - «Програмно - апаратний рівень захисту» та ОргЗ - «Рівень організаційного захисту» показує закономірне зростання величини ризику зниження ефективності захисту організації при зменшенні рівня програмно-апаратного захисту та рівня організаційного захисту. Рівень Правового захисту (ПравЗ)_const = 0,1.

Робимо висновок. Розроблена нечітка продукційна модель дозволяє суттєво розширити можливості існуючих методик, зняти обмеження на число врахованих вхідних змінних та інтегрувати, як якісні, так і кількісні підходи до оцінки ризиків. Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збиток організації. Використовуваний в методиці механізм отримання оцінок ризику на основі нечіткої логіки дозволяє отримати чисельне значення ризику, лінгвістичний опис

ступеня ризику, а також рівень впевненості експерта у виникненні ризикової події, які дозволять ІТ-менеджерам виявити пріоритети ризиків (дуже високий, високий, середній, низький, дуже низький) і виробити план заходів щодо зниження впливу найбільш небезпечних загроз на інформаційну безпеку організації.

ЛІТЕРАТУРА:

1. Хохлов Н.В. Управление риском / Хохлов Н.В. – М.:Юнити-Дана, 2006. – 245 с.
2. Цветкова Е.В. Риски в экономической деятельности: учеб. пособ. / Е.В.Цветкова, И.О.Арлюкова. – СПб.: Питер, 2005. – 175 с.
3. Чернова Г.В. Практика управления рисками на уровне предприятия / Чернова Г.В. – СПб.: Питер, 2006. – 280 с.
4. Сидоров М.А. Управление риском и устойчивое развитие / Сидоров М.А. – М.: Изд-во РЭА им. Плеханова, 2005. – 237 с.
5. Шапкин А.С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций: монография / Шапкин А.С. – М.: Дашков и Ко, 2003. – 544 с.
6. Захарченко Н.В. Повышение информационной скрытности передачи неравновероятного алфавита / [Захарченко Н.В., Гаджиев М.М., Кочетков А.В., Шамшидин Е.Б.] // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2016. – №1(54). – С.188 – 192.
7. Захарченко М.В. Підвищення інформаційної скритності передачі нерівноймовірного алфавіту при таймерному кодуванні / [М.В.Захарченко, О.В.Кочетков, Є.О.Севастєєв, А.С.Кріль] // Сучасні інформаційні технології у сфері безпеки та оборони. – 2017. – № 2 (29). – С. 26 – 31.
8. Федосеев А.В. “Бизнес в шоколаде. Как делать долги, тратить деньги, ни за что не отвечать, отлично жить и иметь успешный бізнес / [А.В. Федосеев, Б.М. Карабанов, Е.Ю. Добровольский, П.С. Боровков]. – СПб.: Питер, 2010. – 480 с.
9. Алтунин А. Е. Модели и алгоритмы принятия решений в нечетких условиях: монография / А.Е. Алтунин, М.В. Семухин. – Тюмень: Издательство Тюменского государственного университета, 2000. – 352 с.
10. Богатин Ю. В. Инвестиционный анализ: учеб. пособ. [для вузов]. / Ю.В. Богатин, В.А. Швандер. – М.: ЮНИТИ-ДАНА, 2000. – 184 с.

REFERENCES:

1. Hohlov N.V. “Upravlenie riskom” M.:Juniti-Dana, (2006): 245.
2. Cvetkova E.V. “Riski v jekonomicheskoj dejatel'nosti: Uchebnoe posobie” SPb: Piter, (2005): 175.
3. Chernova G.V. “Praktika upravlenija riskami na urovne predprijatija” SPb.: Piter, (2006): 280.
4. Sidorov M.A. “Upravlenie riskom i ustojchivoe razvitie M.: Izd-vo RJeA im. Plehanova, (2005): 237.
5. Shapkin A.S. Jekonomicheskie i finansovye riski. Ocenka, upravlenie, portfel' investicij: Monografija / A.S. Shapkin. M.: Dashkov i Ko, (2003): 544.
6. Zaharchenko N.V. “Povyshenie informacionnoj skrytnosti peredachi ne ravnoverojatnogo alfavita.” Zaharchenko N.V., Gadzhiev M.M., Kochetkov A.V., Shamshidin E.B. Vimirjuval'na ta obchisljuval'na tehnika v tehnologichnih procesah. Hmel'nic'kij: Hmel'-nic'kij nac. un-t, №1(54) (2016): 188 - 192.
7. Zaxarchenko M.V. “Pidvy`shhennya informacijnoyi skry`tnosti peredachi nerivnojmovirnonogo alfavitu pry` tajmernomu koduvanni” M.V.Zaxarchenko, O.V.Kochetkov, Ye.O.Sevastyeyev, A.S.Kril` “Suchasni informacijni texnologiyi u sferi bezpeky` ta oborony”`. K.: NUOU № 2 (29) (2017): 26 – 31.
8. Fedoseev A.V. “Biznes v shokolade. Kak delat' dolgi, tratit' den'gi, ni za chto ne otvechat', otlichno zhit' i imet' uspeshnyj biznes” A.V.Fedoseev, B.M.Karabanov, E.Ju. Dobrovol'skij, P.S. Borovkov. SPb.: Piter, (2010): 480.
9. Altunin A. E. “Modeli i algoritmy prinjatija reshenij v nechetkih uslovijah”: Monografija. A.E. Altunin, M. V. Semuhin, Tjumen': Izdatel'stvo Tjumenskogo gosudarstvennogo universiteta, (2000): 352.
10. Bogatin Ju. V. Investicionnyj analiz: Uchebnoe posobie dlja vuzov. / Ju.V. Bogatin, V. A. Shvander – M.: JuNITI-DANA, (2000): 184.

DOI 10.33243/2518-7139-2019-1-1-97-104