УДК 65.012.8 DOI: 10.33111/mise.98.18

Урденко О. Г., аспірант,
кафедри Інформаційного менеджменту
Київський національний економічний університет імені Вадима Гетьмана

Urdenko O. G., Postgraduate
Student of the Information Management Departament,
Kyiv National Economic University named after Vadim Hetman

СИСТЕМНИЙ АНАЛІЗ РИЗИКІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ВИДОВИЩНИХ ЗАХОДІВ

SYSTEMATIC ANALYSIS OF RISKS IN MANAGEMENT INFORMATION SECURITY ENTERTAINMENT EVENTS

Анотація. *Аналіз сучасного стану та тенденцій розвитку світового інформаційного простору свідчить, що рівень інформаційної безпеки за окремими показниками, наближається до критично низької межі. Володіння персональною інформацією покладає на суб'єкти видовищних заходів, які мають на неї права, високий ступінь відповідальності за її збереження і захист від можливого зовнішнього впливу різного роду факторів і подій, що носять як навмисний, так і випадковий характер.*
Актуальність публікації та її практична значимість обумовлена критичною необхідністю створення та впровадження на українських підприємствах видовищних заходів власної системи управління інформаційною безпекою (ІБ), заснованої на міжнародному досвіді та стандартах.
У статті проведено системний аналіз ризиків управління ІБ підприємства видовищних заходів «KARABAS», дослідження та отримання необхідних аналітичних даних для менеджерів, які надають можливість прийняття управлінського рішення щодо мінімізації ризиків ІБ, дозволить складати оптимальний бюджет та мінімізувати матеріальні втрати підприємства видовищних заходів від реалізації загроз.
Автором запропоновано модель нечіткого висновку розроблюваної системи, яка базується на чотирьох вхідних параметрах (векторах даних): Resource cost, Probability of realization, Incidence, Destructiveness coefficient. Для побудови функції приналежності використовується симетрична гаусівська функція.
Згідно заданим лінгвістичним змінним побудовано базу знань аналізу та оцінювання ризиків інформаційної безпеки. Дієздатність цієї бази знань перевірено за допомогою використання контрольного прикладу, який успішно реалізовано за допомогою програмного додатку MatLab Fuzzy Logic Toolbox.
Представлено ілюстративні матеріали візуалізації процедури нечіткого логічного висновку системного аналізу ризиків.
Ключові слова: *функція приналежності, база знань, суб'єкти видовищних заходів, критичні події, джерело загрози, системний аналіз, ризик.*

Abstract. *An analysis of the current state and tendencies of the development of the world information space shows that the level of information security by some indicators is approaching a critically low limit. The possession of personal information imposes on the subjects of the entertaining activities, which have the right to it, a high degree of responsibility for its preservation and protection from the possible external influence of various factors and events of both deliberate and accidental nature.*

The urgency of the publication and its practical relevance is due to the critical need to create and implement in Ukraine enterprises spectacular measures of their own information security (IS) management system, based on international experience and standards.
The article provides a systematic analysis of the risk management of the enterprise KARABAS spectacular events, research and obtaining the necessary analytical data for managers that make the decision to minimize the risks of IB, will allow to make an optimal budget and minimize the material losses of the enterprise spectacular measures from the realization of threats.
The author proposes a model of fuzzy conclusion of the developed system, which is based on four input parameters (data vectors): Resource cost, Probability of realization, Incidence, Destructiveness coefficient. A symmetric Gaussian function is used to construct the membership function.
According to the given linguistic variables, the knowledge base for analysis and assessment of information security risks was built. The validity of this knowledge base was tested using a test case that was successfully implemented with the MatLab Fuzzy Logic Toolbox software application.
Illustrations of visualization of the procedure of fuzzy logical conclusion of systematic risk analysis are presented.
Keywords: *affiliation function, knowledge base, subjects of entertaining events, critical events, threat source, system analysis, risk.*

Вступ. Питанням аналізу ризиків інформаційної безпеки (ІБ) присвячена велика кількість наукових праць, більшість з яких або рясніють наявністю математичних формул і моделей, або не містять взагалі ніяких математичних обчислень, або в них існує перевага у бік будь-якої з двох вище наведених груп підходів. Проаналізуємо змістовні аспекти кожної групи підходів [3].

Підходи першої групи, як правило, використовують різні розділи вищої математики: теорію множин, теорію ймовірностей, дискретну математику і т.д. В якості ядра підходів вибирають принципи, засновані на теорії шансів або корисності (надійності), або нечітких множин, а також безперервний або дискретний розподіл тощо. Роботи, що відносяться до першої групи підходів, часто не враховують реальні вимоги організацій, які займаються аналізом ризиків; вимагають від експертів в області ІБ достатньо високої математичної підготовки, що часто негативно позначається на практиці застосування даних підходів.

Друга група підходів більшою мірою розвинена зарубіжними авторами. Статті авторів з США, Англії носять насамперед рекомендаційний характер для модернізації, перегляду деяких речей уже працюючих на основі стандартів ІБ: ISO, BS, що не вимагають глибокого знання вищої математики.

Третя група підходів у багатьох випадках поєднує в собі експертні оцінки та оцінки ризиків, що базуються на визначенні їх ймовірності за наявними статистичними даними. Подібні підходи можна успішно застосовувати в практичній діяльності (не дивля-

чись на ряд мінусів), так як використання бази статистики дозволяє звести до мінімуму суб'єктивну точку зору експерта на вирішувану задачу і проводити роботу з оцінки ризиків ІБ фахівцям без великого досвіду, кваліфікації [1, 2].

У деяких роботах здійснено підходи, що використовують теорії графів, нечіткої логіки. Це дозволяє наочніше уявити причинно-наслідкові зв'язки між об'єктами, потоками інформаційної системи, що, в свою чергу, сприяє найточнішому аналізу системи на етапі її проектування, полегшує роботу експертів з визначення оцінок ризиків ІБ. Крім того, аналіз ризиків здійснюють більше формалізовано, з простішою програмною реалізацією [6-9].

Для підходів другої групи природно використовувати прописи стандартів ІБ, нормативних документів, рекомендацій. Хоча їм не варто сліпо довіряти, але таке рішення задач ІБ економить час роботи фахівців із захисту інформації.

Відзначимо, що очевидні плюси застосування стандартів безпеки не відображені в більшості проаналізованих підходів. Як буде показано нижче, лише невелика кількість з них ґрунтується, або хоча б використовує, деякі рекомендації стандартів ІБ.

Багато організацій досі дотримуються старих способів точкового управління вразливостями, замість управління ризиками. Такий вибір ускладнює можливу сертифікацію організації, вимагає від фахівців з безпеки освоєння, підвищення досвіду в нових для них системах аналізу ризиків.

Звідси використовувати зазначені вище способи краще не повністю, а обирати деякі рекомендації, які не порушують роботу з аналізу ризиків, але можуть підвищити точність підсумкових результатів, скоротити час роботи експертів.

Процес аналізу ризиків є складовою частиною загальної системи управління організацією, тому для якіснішої роботи з ризиками інформаційних систем вибирають загальну процесну модель. Модель відображає роботу стандартного циклу управління Демінга, визначає: Планування — Виконання — Перевірку — Коригування. У стандартах ISO і BS присутня проекція даного процесу на роботу з аналізу та управління ризиками інформаційної безпеки.

У більшості розглянутих підходів здійснюють роботу найчастіше тільки по пункту оцінки ризиків, тобто безпосередньо по розділу «Виконання». Таким чином, підрахунок ризиків і виконана на його основі закупівля нових засобів і розробка підходів щодо підвищення безпеки, не набагато відрізняється за якістю від застосовуваного в аварійних ситуаціях так званого «заплаточного» методу. Тільки повністю здійснений цикл управління, подальше йо-

го циклічне повторення з коригуванням, переглядом ризиків, дозволяє забезпечити ІБ за допомогою системного аналізу ризиків.

Не можна не помітити відсутність у ряду обговорюваних підходів економічної складової аналізу. У результаті одержують, що управління ризиками — це лише закупівля засобів захисту, без урахування можливостей підприємств видовищних заходів.

Викладення основного матеріалу. Для запропонованої предметної області на підприємствах видовищних заходів можуть виникнути такі задачі і ситуації, які потребують прийняття управлінських рішень (табл. 1).

Таблиця 1

СИТУАЦІЇ, ЩО ПОТРЕБУЮТЬ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

Назва ситуації (задачі ПР)	Тип ситуації	Вид ситуації	Тип проблеми організаційного управління	Характерні особливості	Категорія творців рішень
Вживання заходів щодо зменшення ризику ІБ	відкрита	умова неповної інформації	слабко структурована	невизначеність наслідків прийняття рішення, нечіткі цілі, жорсткі часові обмеження	Керівник підприємства або керівник підрозділу ІБ
Вживання заходів щодо усунення ризику ІБ	відкрита	умова неповної інформації	слабко структурована	невизначеність наслідків прийняття рішення, нечіткі цілі, жорсткі часові обмеження	Керівник підприємства або керівник підрозділу ІБ
Ігнорування ризику	відкрита	умова неповної інформації	слабко структурована	невизначеність наслідків прийняття рішення, нечіткі цілі, жорсткі часові обмеження	Керівник підприємства або керівник підрозділу ІБ

Джерело: авторська розробка

Для задачі управління безпекою існує особа, що приймає рішення (ОПР) — керівник підприємства або керівник підрозділу інформаційної безпеки.

Невизначеність у прийнятті рішень є обумовленою за рахунок використання елементів нечіткої логіки під час оцінювання критеріїв та їх ваги [7]. Значення критеріїв можуть бути якісними (вжити заходи щодо зменшення ризику, прийняти ризик), так і кількісними — значення лінгвістичних змінних (вірогідність успішної реалізації загрози, вартість інформаційного ресурсу, частота виникнення небажаної загрози, коефіцієнт руйнівності). Кожна лінгвістична змінна має певну вагу, що задається ОПР і використовується під час процедури прийняття рішень. Значення ваги лінгвістичних змінних

обмежено інтервалом [0, 1]. Обмеження функцій приналежності визначено у інтервалі значень [0, 100].

Оцінювання ступеня досягнення поставлених цілей для задачі аналізу та оцінювання ризиків інформаційної безпеки інтелектуальної інформаційної системи полягає у дефазифікації, за допомогою використання алгоритму Mamdani, вхідного вектору даних. В якості такого показника використовується три критерії: купувати, продавати квитки або зачекати кращого часу. Обмеження для значень критеріїв рішень (усунути, зменшити чи прийняти ризик), визначені у інтервалі [0, 100].

Цілями процедури прийняття рішень для кожного з суб'єктів ОПР є знаходження відповідного значення з дефазифікації, де кожне значення інтервалу [0, 100] відповідає конкретному рішенню (усунути, зменшити чи прийняти ризик).

Для вирішення задачі системного аналізу і оцінювання ризиків інформаційної безпеки пропонується використовувати нечітку логіку.

Об'єктами, під час управління якими здійснюється розв'язання поставленої задачі є вартість ресурсу ІІС для якого оцінюється ризик, вірогідність успішної реалізації загроз для цього ресурсу, частота виникнення небажаних подій та коефіцієнт руйнівності.

До вихідної інформації відносяться рішення покупки квитків, продажу квитків або зачекати біль кращого часу. Вихідні рішення отримуються з моделі нечіткого висновку з алгоритмом Mamdani і відповідною базою правил.

Перелік вихідних повідомлень представлено у табл. 2.

Таблиця 2

ПЕРЕЛІК ВИХІДНИХ ПОВІДОМЛЕНЬ

Назва вихідного повідомлення	Ідентифікатор	Форма подання	Періодичність видання	Термін видання і допустимий час затримки	Користувач інформації
Рішення по ризику	decision	Повідомлення	За потреби	До кінця робочого дня	Фахівець з ІБ

Джерело: авторська розробка

Вихідна інформація призначена для спеціаліста департамента інформаційної безпеки, який аналізує її, приводить до зрозумілого для керівництва підприємства виду та подає на розгляд з власними рекомендаціями та вказівками. Рішення ризикам розраховується у моделі нечіткого висновку за алгоритмом Mamdani і відповідною базою правил.

Вхідна інформація складається з даних, які використовуються для розрахунків у моделі нечіткого висновку. Ці вхідні дані, там де це можливо отримуються із статистичних даних, що наявні у даній сфері, а там де ні — за рахунок експертних висновків. Перелік вхідних повідомлень представлено у табл. 3.

Вхідний вектор «Вартість ресурсу ІС» (Resource cost) — має діапазон значень [0,100], вартість визначається експертним підходом, при розрахунку враховується вартість розробки, утримання та обслуговування.

Таблиця 3

ПЕРЕЛІК ВХІДНИХ ПОВІДОМЛЕНЬ

Назва вхідного повідомлення	Ідентифікатор	Форма подання	Термін і частота надходження
Resource cost	Cost	Набір даних	У разі необхідності оцінювання ризиків
Probability of realization	Probability	Набір даних	
Incidence	Incidence	Набір даних	
Destructiveness coefficient	Coefficient	Набір даних	

Джерело: авторська розробка

Вхідний вектор «Вірогідність успішної реалізації загрози» (Probability of realization) — має діапазон значень [0,100], визначається залежно від ситуації експертним чи статистичним методами.

Вхідний вектор «Частота виникнення небажаних подій» (Incidence) — має діапазон значень [0,100], визначається експертним методом.

Вхідний вектор «Коефіцієнт руйнівності» (Destructiveness coefficient) — має діапазон значень [0,100], визначається залежно від критичності ресурсу ІС відносно роботи ІС у цілому.

Для оцінювання ризиків інформаційної безпеки підприємства за допомогою засобів нечіткої логіки необхідно залучати експертів різноманітних сфер:

- розробників відповідних ІІС;
- обслуговуючий персонал;
- спеціалістів з ІБ.

Модель нечіткого висновку розроблюваної системи базується на чотирьох вхідних параметрах (векторах даних):

- Resource cost;
- Probability of realization;
- Incidence;

– Destructiveness coefficient.

Для побудови функції приналежності використовується симетрична гаусівська функція

$$\mu(x) = e^{\frac{(x-b)^2}{2a^2}},$$

де a^2 — дисперсія розподілу;

b — математичне сподівання.

В інструментарії Fuzzy Logic Toolbox середовища MatLab дана функція має ім'я gaussmf і задається двома параметрами у вигляді: [a, b].

Лінгвістична змінна Resource cost (Вартість ресурсу ІС) — чим вища вартість ресурсу ІС, тим критичніший він для підприємства і тим більший збиток отримає підприємство в разі реалізації загроз, що стосуються нього. Діапазон значень даного параметра — [0 100]. Вигляд даної лінгвістичної змінної показано на рис. 1.

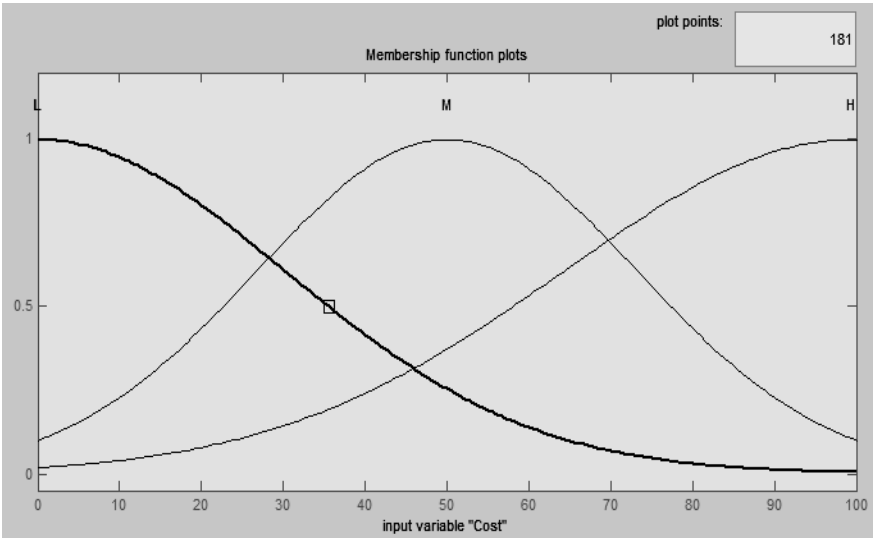

Рис.1. Функції лінгвістичної змінної Resource cost

Джерело: власний розрахунок

Для даної змінної введено 3 лінгвістичних терма:

Low — функція даного терма побудована за параметрами [30 0]. Даний терм означає низьку ціну ресурсу ІС;

Medium — функція даного терма побудована за параметрами [23 50]. Даний терм означає середню ціну ресурсу ІС;

High — функція даного терма побудована за параметрами [35 100]. Даний терм означає високу ціну ресурсу ІС;

Лінгвістична змінна Probability of realization (Вірогідність успішної реалізації загрози) — описує частоту виникнення певної небажаної події (за якийсь фіксований період). Діапазон значень даного параметра — [0 100]. Вигляд даної лінгвістичної змінної показано на рис. 2.

Для даної змінної введено 3 лінгвістичних терма:

Low — функція даного терма побудована за параметрами [25.5 0]. Даний терм означає низьку вірогідність успішної реалізації загрози;

Medium — функція даного терма побудована за параметрами [25 50]. Даний терм означає середню вірогідність успішної реалізації загрози;

High — функція даного терма побудована за параметрами [32 100]. Даний терм означає високу вірогідність успішної реалізації загрози;

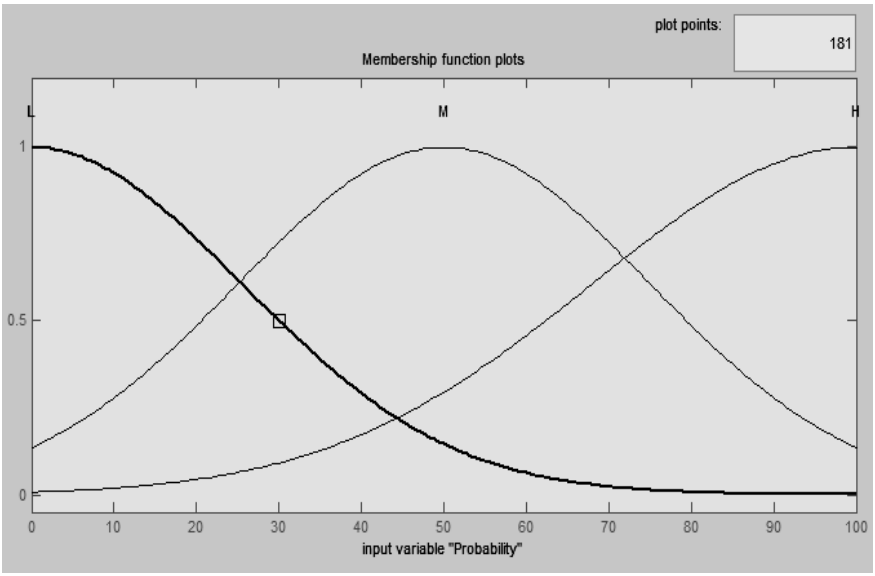

Рис. 2. Функції лінгвістичної змінної Probability of realization

Джерело: власний розрахунок

Лінгвістична змінна Incidence (Частота виникнення небажаних подій) — описує вірогідність успішної реалізації загрози. До таких подій відносяться, наприклад дії користувачів, що призводять до виникнення чи реалізації загроз. Діапазон значень даного параметра — [0 100]. Вигляд даної лінгвістичної змінної показано на рис. 3.

Для даної змінної введено 3 лінгвістичних терма:

Low — функція даного терма побудована за параметрами [35 0]. Даний терм означає низьку частоту виникнення небажаної події;

Medium — функція даного терма побудована за параметрами [18 50]. Даний терм означає середню частоту виникнення небажаної події;

High — функція даного терма побудована за параметрами [36 100]. Даний терм означає високу частоту виникнення небажаної події;

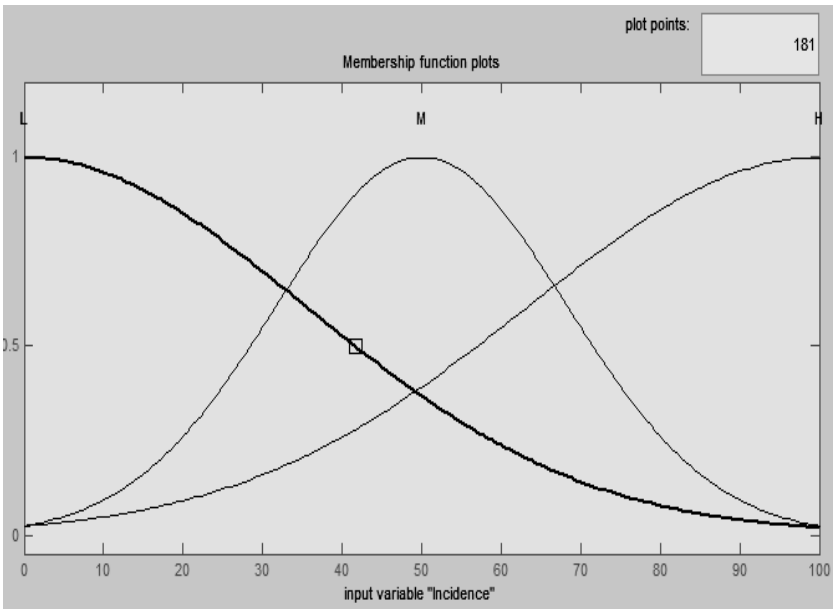

Рис. 3. Функції лінгвістичної змінної Incidence

Джерело: власний розрахунок

Лінгвістична змінна Destructiveness coefficient (Коефіцієнт руйнівності) — описує ступінь руйнівності впливу на ресурс. Визначається експертом на основі аналізу конкретної загрози пев-

ному ресурсу. Діапазон значень даного параметра — [0 100]. Вигляд даної лінгвістичної змінної показано на рис. 4.

Для даної змінної введено 3 лінгвістичних терма:

Low — функція даного терма побудована за параметрами [35 0]. Даний терм означає низьке значення руйнівності впливу на ресурс;

Medium — функція даного терма побудована за параметрами [18 50]. Даний терм означає середнє значення руйнівності впливу на ресурс;

High — функція даного терма побудована за параметрами [36 100]. Даний терм означає високе значення руйнівності впливу на ресурс.

База знань моделі нечіткого висновку розробляється за алгоритмом Мамдані. Даний алгоритм описує кілька послідовних етапів:

- формування бази правил;
- фазифікація;
- агрегування підумов;
- активізація підзаключень;
- акумулювання заключень;
- дефазифікація.

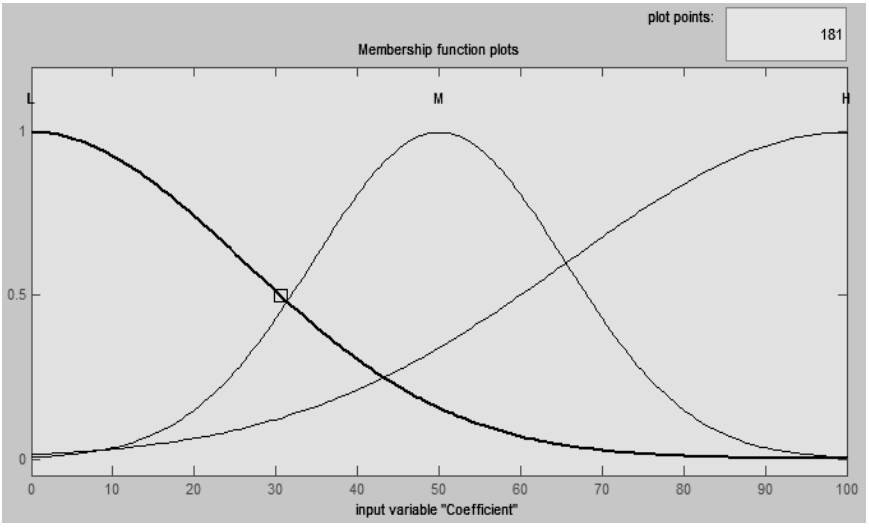

Рис. 4. Функції лінгвістичної змінної Destructiveness coefficient

Джерело: власний розрахунок

При цьому кожний наступний етап отримує на вхід значення отримані на попередньому кроці.

Алгоритм примітний тим, що він працює за принципом «чорної скриньки». На вхід надходять кількісні значення, на виході вони ж. На проміжних етапах використовується апарат нечіткої логіки і теорія нечітких множин.

Згідно заданим лінгвістичним змінним побудуємо базу знань аналізу та оцінювання ризиків інформаційної безпеки:

- Правило 1: ЯКЩО «*Ціна* — низька» І «*Імовірність* — низька» І «*Частота подій* — низька» І «*Значення коефіцієнта* — низьке» ТО «Рішення — прийняти ризик».
- Правило 2: ЯКЩО «*Ціна* — низька» І «*Імовірність* — низька» І «*Частота подій* — низька» І «*Значення коефіцієнта* — середнє» ТО «Рішення — прийняти ризик».
- Правило 3: ЯКЩО «*Ціна* — низька» І «*Імовірність* — низька» І «*Частота подій* — низька» І «*Значення коефіцієнта* — низьке» ТО «Рішення — прийняти ризик».
- Правило 4: ЯКЩО «*Ціна* — середня» І «*Імовірність* — середня» І «*Частота подій* — середня» І «*Значення коефіцієнта* — середнє» ТО «Рішення — знизити ризик».
- Правило 5: ЯКЩО «*Ціна* — висока» І «*Імовірність* — висока» І «*Частота подій* — висока» І «*Значення коефіцієнта* — високе» ТО «Рішення — усунути ризик».
- Правило 6: ЯКЩО «*Ціна* — середня» І «*Імовірність* — низька» І «*Частота подій* — низька» І «*Значення коефіцієнта* — низьке» ТО «Рішення — прийняти ризик».
- Правило 7: ЯКЩО «*Ціна* — низька» І «*Імовірність* — низька» І «*Частота подій* — середня» І «*Значення коефіцієнта* — середнє» ТО «Рішення — знизити ризик».
- Правило 8: ЯКЩО «*Ціна* — низька» І «*Імовірність* — низька» І «*Частота подій* — середня» І «*Значення коефіцієнта* — середнє» ТО «Рішення — знизити ризик».
- Правило 9: ЯКЩО «*Ціна* — низька» І «*Імовірність* — низька» І «*Частота подій* — низька» І «*Значення коефіцієнта* — високе» ТО «Рішення — знизити ризик».
- Правило 10: ЯКЩО «*Ціна* — середня» І «*Імовірність* — низька» І «*Частота подій* — низька» І «*Значення коефіцієнта* — середнє» ТО «Рішення — знизити ризик».
- Правило 11: ЯКЩО «*Ціна* — середня» І «*Імовірність* — низька» І «*Частота подій* — низька» І «*Значення коефіцієнта* — високе» ТО «Рішення — знизити ризик».

- Правило 12: ЯКЩО «*Ціна* — висока» І «*Імовірність* — середня» І «*Частота подій* — середня» І «*Значення коефіцієнта* — середнє» ТО «Рішення — усунути ризик».
- Правило 13: ЯКЩО «*Ціна* — висока» І «*Імовірність* — висока» І «*Частота подій* — середня» І «*Значення коефіцієнта* — середнє» ТО «Рішення — усунути ризик».
- Правило 14: ЯКЩО «*Ціна* — висока» І «*Імовірність* — висока» І «*Частота подій* — висока» І «*Значення коефіцієнта* — середнє» ТО «Рішення — усунути ризик».
- Правило 15: ЯКЩО «*Ціна* — висока» І «*Імовірність* — висока» І «*Частота подій* — середня» І «*Значення коефіцієнта* — високе» ТО «Рішення — усунути ризик».
- Правило 16: ЯКЩО «*Ціна* — середня» І «*Імовірність* — висока» І «*Частота подій* — висока» І «*Значення коефіцієнта* — високе» ТО «Рішення — усунути ризик».
- Правило 17: ЯКЩО «*Ціна* — середня» І «*Імовірність* — низька» І «*Частота подій* — середня» І «*Значення коефіцієнта* — високе» ТО «Рішення — знизити ризик».
- Правило 18: ЯКЩО «*Ціна* — висока» І «*Імовірність* — висока» І «*Частота подій* — висока» І «*Значення коефіцієнта* — низьке» ТО «Рішення — усунути ризик».
- Правило 19: ЯКЩО «*Ціна* — висока» І «*Імовірність* — висока» І «*Частота подій* — низька» І «*Значення коефіцієнта* — високе» ТО «Рішення — усунути ризик».
- Правило 20: ЯКЩО «*Ціна* — висока» І «*Імовірність* — висока» І «*Частота подій* — середня» І «*Значення коефіцієнта* — високе» ТО «Рішення — усунути ризик».
- Правило 21: ЯКЩО «*Ціна* — висока» І «*Імовірність* — висока» І «*Частота подій* — низька» І «*Значення коефіцієнта* — середнє» ТО «Рішення — усунути ризик».
- Правило 22: ЯКЩО «*Ціна* — низька» І «*Імовірність* — низька» І «*Частота подій* — висока» І «*Значення коефіцієнта* — високе» ТО «Рішення — знизити ризик».
- Правило 23: ЯКЩО «*Ціна* — середня» І «*Імовірність* — середня» І «*Частота подій* — висока» І «*Значення коефіцієнта* — високе» ТО «Рішення — усунути ризик».
- Правило 24: ЯКЩО «*Ціна* — висока» І «*Імовірність* — низька» І «*Частота подій* — низька» І «*Значення коефіцієнта* — низьке» ТО «Рішення — знизити ризик».

Ілюстративні матеріали візуалізації процедури нечіткого логічного висновку системного аналізу ризиків представлено на рис. 5–8.

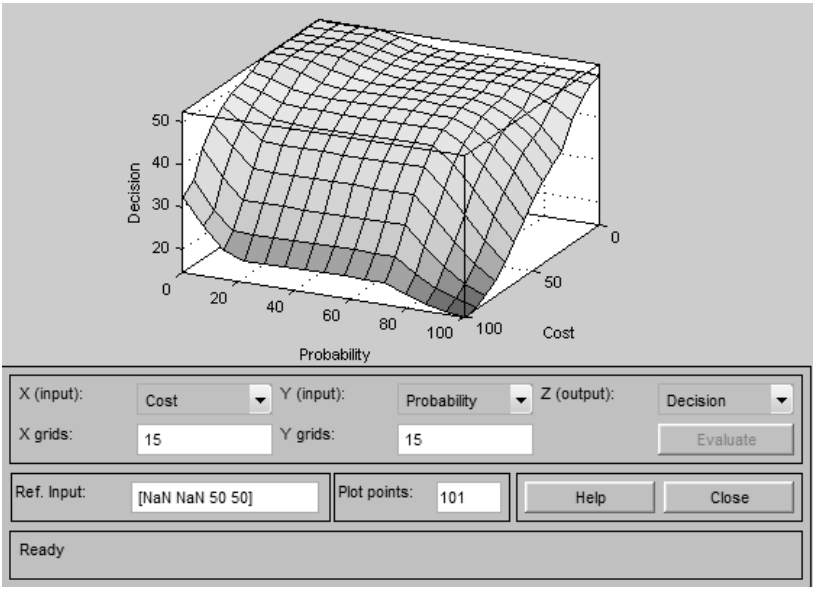

Рис. 5.

Джерело: власний розрахунок

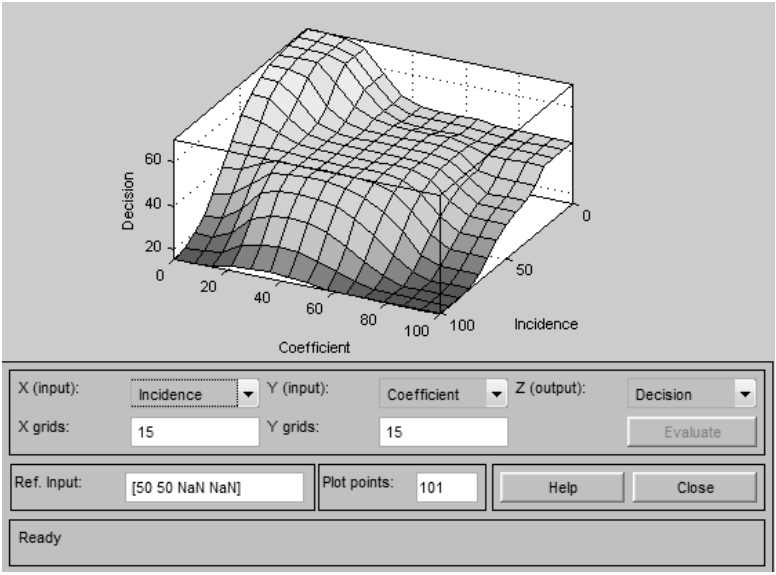

Рис. 6.

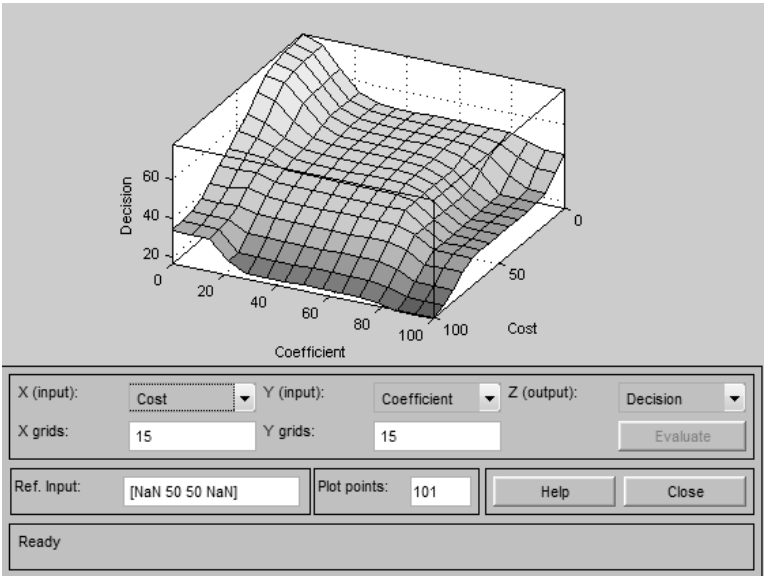

Рис. 7.

Джерело: власний розрахунок

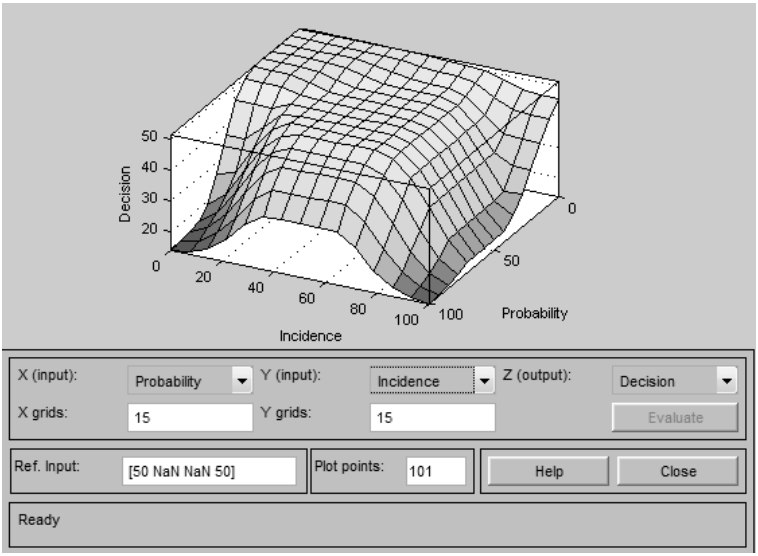

Рис. 8.

Джерело: власний розрахунок

Перевірка функціонування розробленої методики з аналізу та оцінювання ризиків управління інформаційною безпекою інтелектуальної інформаційної системи була здійснена в реальних умовах функціонуючого підприємства видовищних заходів «KARABAS».

Висновки

Одержані результати можуть бути використані для мінімізації ризиків, складання оптимального бюджету інформаційної безпеки та мінімізації матеріальних втрат підприємства від реалізації загроз інформаційної безпеки. Розроблена методика є ефективною системою завдяки алгоритму нечіткої логіки. Було спроектовано та розроблено базу знань, що може використовуватись для оцінювання ризиків інформаційної безпеки. Дієздатність цієї бази знань перевірено за допомогою використання контрольного прикладу, який успішно реалізовано за допомогою програмного додатку MatLab Fuzzy Logic Toolbox.

Отримана в результаті розробки система аналізу та оцінювання ризиків може бути використана як складова інтелектуальної системи прийняття рішень з управління інформаційною безпекою видовищних заходів.

Література

1. Бєгун А. В., Ігнатова Ю. В., Урденко О. Г. Оцінка економічної ефективності захисту неоднорідних даних підприємств малого та середнього бізнесу. Фінансово-кредитне забезпечення інноваційної діяльності малого та середнього бізнесу / за заг. ред. М.І. Диби. — К.: ВД «Освіта України» , 2019. — п.4.3. — С. 333–358.
2. Бєгун А. В., Осипова О. І., Урденко О. Г. Ситуаційний логменеджмент інформаційної безпеки підприємства // Моделювання та інформаційні системи в економіці. Міжвідомчий наук. збірник. Вип. № 95. — К:. КНЕУ, 2018. — С. 18–29.
3. П. В. Плетнёв, В. М. Белов. Сравнительный анализ существующих методов определения рисков ИБ // Ползуновский вестник, № 3/1’2011. — Барнаул, 2011. — с. 221–223.
4. Козенков Д.Е., Никитин П.А. Основные методы оценки рисков в современном риск-менеджменте // БізнесІнформ, № 10’2012. — Харків, 2012 — с. 248–253.
5. Нечітка логіка [Електронний ресурс]. — Режим доступу: URL: http://www.victoria.lviv.ua/html/oio/html/theme11.htm. — Назва з екрану.
6. Zadeh L. Fuzzy Sets // Information and Control. — 1965. — № 8. — P. 338–353.

7. А. В. Матвійчук. Штучний інтелект в економіці: нейронні мережі, нечітка логіка / КНЕУ, 2010. — 361 с.
8. Структура Fuzzy Logic Toolbox [Електронний ресурс]. — Режим доступу: URL: http://matlab.exponenta.ru/fuzzylogic/book2/index.php
9. Address Allocation for Private Internets [Electronic Resource]. — Mode of access: URL: http://www.rfc-editor.org/rfc/rfc1918.txt. Title from the screen.

References

1. Begun A.V., Ignatova Yu.V., Urdenko O. G. Assessment of economic efficiency of protection of heterogeneous data of small and medium-sized enterprises. Financial-credit support of innovative activity of small and medium-sized business / by head. ed. E. Deeby. — K .: VD “Education of Ukraine”, 2019. — p.4.3. — P. 333–358.
2. Begun A. V., Osipova O. I., Urdenko O. G. Situational log-management of information security of enterprise // Modeling and information systems in economy. Interdepartmental Sciences. collection. No. № 95. — To :. KNEU, 2018 — P. 18–29.
3. P. V. Pletnev, V. M. Belov. Comparative analysis of existing methods of risk assessment of IB // Polzunovskii vestnik, № 3 / 1’2011. — Barnaul, 2011. — p. 221–223
4. Kozenkov D. E., Nikitin P. A. Basic methods of risk assessment in modern risk management // BusinessInform, # 10’2012. — Kharkiv, 2012 — p.248–253
5. Fuzzy logic [Electronic resource]. — Access mode: URL: http://www.victoria.lviv.ua/html/oio/html/theme11.htm. — The name from the screen.
6. Zadeh L. Fuzzy Sets // Information and Control. 1965. № 8. P. 338–353.
7. A. V. Matviychuk. Artificial Intelligence in Economics: Neural Networks, Fuzzy Logic / KNEU, 2010. — 361 p.
8. Structure of the Fuzzy Logic Toolbox. — Access mode: URL: http://matlab.exponenta.ru/fuzzylogic/book2/index.php
9. Address Allocation for Private Internets [Electronic Resource]. — Mode of access: URL: http://www.rfc-editor.org/rfc/rfc1918.txt. Title from the screen.

Статтю подано до редакції 01.10.2019 р.