УДК 004.934 DOI: 10.31673/2412-4338.2020.011451

Міщенко А.В. *Комунальне підприємство «Міжнародний аеропорт «Київ» (Жуляни)», Київ*
Курило О.В., Золотухіна О.А. *Державний університет телекомунікацій, Київ*

НЕЧІТКА МОДЕЛЬ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПІДТРИМКИ РІВНЯ ЗАХИЩЕНОСТІ ERP-СИСТЕМ

Робота присвячена питанню використання нечіткої моделі для оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем. Розглянуто вимоги до інформаційної безпеки ERP-систем та проаналізовано проблеми їх безпеки та вразливості. Визначено основні фактори, що впливають на оцінку ризиків.. Зважаючи на якісний, неточний та значною мірою не визначений, або неповний характер інформації про більшість факторів, запропоновано використання лінгвістичного підходу для їх опису. Такий підхід забезпечує можливість отримання кількісного опису елементів моделі за умов наявності лише нечіткої інформації про значення факторів ризику інформаційної безпеки і дозволяє спростити подальший процес ранжування факторів ризиків та чисельного розрахунку значень їх наслідків. Розроблена нечітка продукційна модель оцінки ризиків інформаційної безпеки ERP-систем, що дозволяє виконувати оцінку ризику за чотирма факторами: цінність ресурсу, вплив наслідку на ресурс, ймовірність виникнення загрози та вразливість ресурсу. База нечітких продукційних правил має структуру MISO. Зазначену модель реалізовано з використанням пакету прикладних програм MATLAB та пакету розширення Fuzzy Logic Toolbox. Для нечіткого виведення використано алгоритм Сугено. Результати моделювання процесу отримання оцінок ризиків інформаційної безпеки та аналізу отриманих результатів продемонстрували достатньо високу точність запропонованої моделі у порівнянні з експертними оцінками. Запропоновані підходи щодо оцінки ризиків можуть бути використані як для оцінки конкретних видів ризиків інформаційної безпеки ресурсів ERP-системи, так і загального ризику інформаційної безпеки ERP-системи.

Ключові слова: *ERP-система, загрози інформаційної безпеки, ризики інформаційної безпеки, нечітка модель, продукційна модель, нечітке логічне виведення.*

Mishchenko A.V., *Municipal Enterprise "International Airport "Kyiv" (Zhuliany)", Kyiv*
Kurilo O.V., Zolotukhina O.A. *State University of Telecommunications, Kyiv*

FUZZY MODEL FOR ASSESSING INFORMATION SECURITY RISKS AND MAINTAINING THE LEVEL OF SECURITY OF ERP-SYSTEMS

The work is devoted to the issue of using a fuzzy model to assess information security risks and support the level of security of ERP systems. The requirements for information security of ERP-systems are considered and the problems of their security and vulnerability are analyzed. The main factors influencing the risk assessment are identified. Given the qualitative, inaccurate and largely uncertain or incomplete nature of information on most factors, it is proposed to use a linguistic approach to describe them. This approach provides the opportunity to obtain a quantitative description of the model elements in the presence of only fuzzy information about the value of information security risk factors and allows to simplify the further process of ranking risk factors and numerically calculating the values of their consequences. A fuzzy production model for assessing the risk of information security of ERP systems is developed, which allows risk assessment to be performed on four factors: resource value, the impact of the consequences on the resource, the probabilityof a threat and resource vulnerability. The base of fuzzy production rules has a MISO structure. The specified model is implemented using the MATLAB application package and the Fuzzy Logic Toolbox extension package. For fuzzy inference, the Sugeno algorithm is used. The simulation results of the process of obtaining information security risk assessments demonstrated a rather high accuracy of the proposed model when comparing them with expert estimates. The proposed approaches to risk assessment can be used both for assessing specific types of risks with the information security of the ERP system and the general information security risk of the ERP system.

Keywords: *ERP-system, information security threats, information security risks, fuzzy model, production model, fuzzy inference.*

Мищенко А.В. *Коммунальное предприятие «Международный аэропорт «Киев» (Жуляны)», Киев*
Курило О.В., Золотухіна О.А. *Государственный университет телекоммуникаций, Киев*

НЕЧЕТКАЯ МОДЕЛЬ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПОДДЕРЖКИ УРОВНЯ ЗАЩИЩЕННОСТИ ERP-СИСТЕМ

Работа посвящена вопросу использования нечеткой модели для оценки рисков информационной безопасности и поддержки уровня защищенности ERP-систем. Рассмотрены требования к информационной безопасности ERP-систем и проанализированы проблемы их безопасности и уязвимости. Определены основные факторы, влияющие на оценку рисков. Учитывая качественный, неточный и во многом не определенный или неполный характер информации о большинстве факторов, предложено использование лингвистического подхода для их описания. Такой подход обеспечивает возможность получения количественного описания элементов модели при наличии только нечеткой информации о значении факторов риска информационной безопасности и позволяет упростить дальнейший процесс ранжирования факторов риска и численного расчета значений их последствий. Разработана нечеткая продукционная модель оценки рисков информационной безопасности ERP-систем, которая позволяет выполнять оценку риска по четырем факторам: ценность ресурса, влияние последствия на ресурс, вероятность возникновения угрозы и уязвимости ресурса. База нечетких продукционных правил имеет структуру MISO. Указанная модель реализована с использованием пакета прикладных программ MATLAB и пакета расширения Fuzzy Logic Toolbox. Для нечеткого вывода использован алгоритм Сугено. Результаты моделирования процесса получения оценок рисков информационной безопасности продемонстрировали достаточно высокую точность предложенной модели при их сравнении с экспертными оценками. Предложенные подходы к оценке рисков могут быть использованы как для оценки конкретных видов рисков информационной безопасностью ERP-системы, так и общего риска информационной безопасности ERP-системы.

Ключевые слова: *ERP-система, угрозы информационной безопасности, риски информационной безопасности, нечеткая модель, продукционная модель, нечеткий логический вывод.*

1. Вступ. Оцінка ризиків інформаційної безпеки є важливим елементом у загальному процесі управління ризиками безпеки, який є процесом забезпечення того, щоб позиція ризиків організації знаходилась у прийнятних межах, визначених вищим керівництвом, та складалася з чотирьох основних етапів: оцінка ризиків безпеки, тестування та нагляд, пом'якшення ризиків та операційна безпека [2]. Згідно Державного стандарту України (ДСТУ) ISO/IEC 27005:2015 [1], поняття «ризик» часто характеризують з посиланням на потенційні події і наслідки, або їх комбінацію, а «ризик інформаційної безпеки» пов'язують з можливістю використання загрозами вразливостей інформаційних ресурсів систем управління інформаційною безпекою (СУІБ) або групи інформаційних ресурсів СУІБ і, таким чином, призводити до збитків організації.

Кількісні оцінки ризику інформаційної безпеки використовують математичні формули для визначення коефіцієнта експозиції та очікувану втрату однієї або кожної загрози, а також ймовірності реалізації загрози, що називається річною швидкістю виникнення (Annualized Rate of Occurrence, ARO) [3]. Перевагами використання цього підходу є можливість кількісно визначити наслідки виникнення інцидентів, проаналізувати витрати і вигоди під час вибору засобів захисту та отримання більш точного визначення ризику. До недоліків можна віднести залежність кількісних показників від їх обсягу та точності шкали вимірювання, неточність результатів, необхідність збагачення якісним описом, велику вартість проведення аналізу, який вимагає більшого досвіду та сучасних інструментів.

Особливістю задач оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем є те, що більша частина даних про фактори ризиків має ознаки недосконалості та невизначеності: суперечливість, неточність, ненадійність або неповноту, є нелінійними та динамічно змінними. Останнім часом методи аналізу та оцінки ризиків, які засновані на елементах нечіткої логіки, розвиваються досить інтенсивно. Такі методи дозволяють змінити наближені табличні методи грубої оцінки ризиків на математичний метод, а також значно

розширити можливості математичних методів аналізу ризиків [4-6]. Механізм оцінювання ризиків за допомогою нечіткої логіки в загальному вигляді представляє експертну систему. Базу знань такої системі складають правила, які відображають логіку взаємозв'язку вхідних величин факторів ризику і рівнів ризику. Механізм нечіткої логіки передбачає формування рівнів оцінок факторів та подання їх у вигляді нечітких змінних. Процес формування такого виду оцінок у загальному випадку має досить складний характер, бо потребує великої кількості джерел інформації, врахування їх якості та використання досвіду експертів. Таким чином, на сьогоднішній день сучасним та актуальним є завдання розробки нечітких моделей і методів для оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем при недосконалості та невизначеності вхідних даних. Мета та задачі дослідження полягають у підвищенні якості оцінювання ризиків інформаційної безпеки та захищеності ERP-систем за рахунок використання нечіткої моделі оцінювання, що враховує особливості вхідних даних.

2. Аналіз проблем безпеки ERP-систем. Оскільки системи ERP обробляють та зберігають конфіденційну, особисту та комерційну інформацію, що стосується співробітників, замовників, постачальників, перспектив та проектів, подальший розвиток за межами оригінальної схеми додає додатку підвищений ризик порушень безпеки даних та недотримання правил. Спеціальні розробки, як правило, складають дуже малу частину всієї програми, але, оскільки вони отримують доступ та обробляють ті ж дані, що і основна програма, вони становлять значний ризик для безпеки, який може потенційно коштувати організації збитку від порушення безпеки. До основних загроз безпеки ERP-систем відносяться навмисні дії порушників, наприклад, злочинців, шпигунів, диверсантів, або скривджених осіб з числа персоналу організації [7]. Загрози безпеці можуть бути класифіковані за різними ознаками: за результатами дій порушників(загроза витоку інформації; загроза модифікації інформації; загроза втрати інформації), за мотивами порушників (ненавмисні; навмисні) тощо. Ненавмисні (випадкові) загрози найчастіше виникають в результаті стихійних лих, таких як повінь, ураган, землетрус, або пожежа; аварій або техногенних катастроф; збою або відмови апаратного забезпечення; наслідків помилок проектування і розробки компонентів ERP-системи, таких як: апаратне забезпечення, бізнес-процеси, технології обробки інформації, модулі та підпрограми, структур даних тощо; помилок експлуатації ERP-системи адміністраторами, користувачами, операторами системи та інших видів персоналу. Відповідно до Нормативного документу в галузі технічного захисту інформації (НД ТЗІ) 2.5-004-99 [8] в моделі оцінки ризиків будемо розглядати загрози наступних чотирьох типів відповідно до властивостей інформаційної безпеки:

1) загрози, що відносяться до несанкціонованого ознайомлення з інформацією та становлять загрози порушення конфіденційності інформації;

2) загрози, що відносяться до несанкціонованої модифікації інформації та становлять загрози порушення цілісності інформації;

3) загрози, що відносяться до порушення можливості використання системи або інформації, що оброблюється та становлять загрози порушення доступності інформації;

4) загрози, що відносяться до порушення можливості спостереження, керування та контролю за діями користувачів, можливості легальністю доступу, можливості та спроможності виконувати функції комплексом засобів захисту та становлять загрози порушення спостережуваності інформації.

При проведені аналізу негативних наслідків впливу на ERP-систему різних видів інформаційних загроз, як правило, розглядаються їх наступні категорії [9]:

– відмови та збої апаратного та/або мережевого забезпечення системи, аварійні ситуації та інші події, що відбуваються без участі персоналу;

– ненавмисні або помилкові дії адміністраторів, користувачів, операторів системи, або інших видів персоналу;

– несанкціонований доступ порушниками до інформації, яка формується, обробляється та зберігається в ERP-системі, наприклад, інформація що дозволяє виконувати

управління та прийняття рішень, реалізовувати бізнес-процеси та технології обробки інформації в ERP-системі; виконувати управління обладнанням ERP-системи, управління та роботу засобів захисту ERP-системи.

Серед найпоширеніших проблем безпеки ERP-системи можна вказати наступні загрози:

– затримка оновлень, які необхідні в основному для усунення слабких місць, виявлених у програмному забезпеченні, та установка яких якнайшвидше є життєво важливою для запобігання можливості використання цих слабких місць;

– недостатній контроль прав доступу, які при неправильному налаштуванні стають потенційними внутрішніми ризиками для системи та погрожують порушенням цілісності та конфіденційності інформації;

– недостатня підготовка персоналу, що працює з системою, особливо це стосується нових працівників, які не мають глибоких знань про внутрішні процеси та помилки яких можуть порушити принципи виконання бізнес-процесів;

– недостатня перевірка персоналу, що має безперешкодний доступ до системних процесів та можливість змінювати функціональність програмного забезпечення ERP-системи;

– використання неліцензійних програм, які можуть використовуватися разом з ERP-системою для досягнення єдиної мети (наприклад, підтримка даних про продажі у ERP-системі, але запуск звітів за допомогою Excel);

– помилки впровадження та конфігурації платформи (налаштування, неправильні облікові дані, відкриті порти і т. д.) ERP-системи, що має безліч файлів конфігурації, також можуть потенційно поставити під ризик процес функціонування та дані;

– недотримання нормативних норм та постанов, що призначені для захисту конфіденційної інформації, тягне за собою фінансові та репутаційні наслідки.

3. Розробка нечіткої моделі оцінки ризиків ERP-систем. У загальному випадку розрахунок ризиків інформаційної безпеки ERP-систем повинен проводитися по відношенню до кожного критичного бізнес-процесу та лише за тими уразливостями, які є актуальними для певного бізнес-процесу, при чому, слід мати на увазі, що ряд вразливостей можуть бути однакові для усіх бізнес процесів. Кожній вразливості з актуального переліку вразливостей співвідноситься загроза, умовами реалізації якої може бути ця вразливість, а за кожною визначеною парою проводиться оцінка ймовірності її виникнення та оцінка впливу реалізації цієї пари на цілісність, конфіденційність, доступність та спостережуваність. Під ризиком мається на увазі поєднання ймовірності нанесення шкоди шляхом подолання системи захисту з використанням вразливостей та тяжкості такої шкоди. Мінімізація ризиків здійснюється за допомогою розробки «політики безпеки» (схеми поведінки) та управління нею. Таким чином, поняття «ризик порушення інформаційної безпеки» повинен ґрунтуватися на аналізі «причин порушення інформаційної безпеки» і «наслідків порушення інформаційної безпеки». Оцінка ризику у найпростішому випадку виконується за допомогою двох чинників: ймовірність події і тяжкість можливих наслідків.

Як частина бізнес-ризиків підприємства, ризик інформаційної безпеки визначається як добуток втрат (фінансових) від порушення конфіденційності, цілісності, автентичності або доступності інформаційних ресурсів (тяжкість наслідків) на ймовірність такого порушення (ймовірність події):

$$R = A \cdot P_e \tag{1}$$

де: R – ризик реалізації загрози; A – фінансовий збиток від одноразової реалізації загрози; P_e – ймовірність події.

Ймовірність події (як ймовірність реалізації загрози) може бути об'єктивною або суб'єктивної величиною та повинна враховувати ймовірність загрози та рівень вразливості:

$$P_e = P_t \cdot V, \tag{2}$$

де: P_e– ймовірність події; P_t– ймовірність загрози; V – рівень вразливості.

Загальносистемний рівень ризику обчислюється як сума ризиків по всіх активах та кожній загрозі з урахуванням вразливостей, а ефект від вжитих контрзаходів – як різниця між сумою запланованих витрат на контрзаходи та сумарною оцінкою збитків при визначеному загальносистемному рівню ризику.

Для побудови моделі розрахунку оцінки ризику інформаційної безпеки пропонується використовувати нечітку продукційну модель, представлену множиною окремих нечітких продукційних правил виду «якщо A, то B» де A – передумова певного правила, а B – висновок правила у вигляді нечітких висловлювань. Модель призначена для визначення ступеня істинності висновків нечітких продукційних правил. Ступень істинності визначається на основі передумов з певним ступенем істинності відповідних правил.

Для побудови моделі розрахунку оцінки ризику будемо використовувати співвідношення (3) факторів ризику, відповідно до формул (1), (2)

$$R_{ij} = A_{ij} \cdot P_j^t \cdot P_{ij}^v, i \in IR, j \in Th, \quad (3)$$

де: R_{ij} – ризик i-го ресурсу при реалізації j-ї загрози; A_{ij} – очікуваний збиток від одноразової реалізації j-ї загрози для i-го ресурсу; P_j^t – ймовірність виникнення j-ї загрози; P_{ij}^v – вразливість i-го ресурсу до j-ї загрози; IR – множина ресурсів системи; Th – множина загроз для системи.

Під очікуваним збитком від одноразової реалізації загрози будемо розуміти вартість (або цінність) активу, що математично виражається як (4):

$$A_{ij} = A_i^V \cdot F_{ij}^e, i \in IR, j \in Th, \quad (4)$$

де: A_{ij} – очікуваний збиток від одноразової реалізації j-ї загрози для i-го ресурсу; A_j^V – цінність i-го ресурсу; F_{ij}^e – вплив наслідку при реалізації j-ї загрози на i-й ресурс, або схильність i-го ресурсу до j-ї загрози; IR – множина ресурсів системи; Th – множина загроз для системи.

Враховуючи (3) та (4), отримаємо загальне співвідношення факторів для оцінки ризику (5):

$$R_{ij} = A_i^V \cdot F_{ij}^e \cdot P_j^t \cdot P_{ij}^v, i \in IR, j \in Th, \quad (5)$$

де: R_{ij} – ризик i-го ресурсу при реалізації j-ї загрози; A_i^V – цінність i-го ресурсу; F_{ij}^e – вплив наслідку при реалізації j-ї загрози на i-й ресурс або схильність i-го ресурсу до j-ї загрози; P_j^t – ймовірність виникнення j-ої загрози; P_{ij}^v – вразливість i-го ресурсу до j-ої загрози; IR – множина ресурсів системи; Th – множина загроз для системи.

Оскільки для кожного інформаційного ресурсу може бути визначена безліч ризиків (від одного до усіх), оцінку загального ризику за інформаційним ресурсом будемо визначати як максимальну оцінку серед ризиків ресурсу (6):

$$R_i = max(R_{ik}), k \in Th_i, \quad (6)$$

де: R_i – ризик i-го ресурсу при реалізації загроз; R_{ik} – ризик i-го ресурсу при реалізації k-ї загрози; Th_i – множина ризиків для i-го ресурсу.

В свою чергу, оцінку загальносистемного ризику визначимо як максимальну оцінку серед оцінок ризиків ресурсів (7):

$$R = max(R_i), i \in IR, \quad (7)$$

де: R – загальносистемний ризик; R_i – ризик i-го ресурсу; IR – множина ресурсів системи.

Розмір фінансового збитку для інформаційного ресурсу визначимо як добуток ризику інформаційного ресурсу на вартість ресурсу (8):

$$FL_i = R_i \cdot Co_i, i \in IR, \quad (8)$$

де: FL_i – фінансовий збиток i-го ресурсу; R_i – ризик i-го ресурсу; Co_i– вартість i-го ресурсу;

IR – множина ресурсів системи.

В свою чергу, загальний фінансовий збиток визначимо як суму фінансових збитків за усіма ресурсами:

$$FL = \sum_i FL_i, i \in IR, \quad (9)$$

де: FL – загальний фінансовий збиток; FL_i – фінансовий збиток *i*-го ресурсу; IR – множина ресурсів системи.

До опису факторів ризику інформаційної безпеки застосуємо лінгвістичний підхід. Це забезпечить кількісний опис елементів моделі в умовах нечіткої інформації про значення рівня ризику, вартості ресурсу, впливу наслідку, ймовірності виникнення загрози, вразливості захисту ресурсу та способів уникнення негативного впливу від реалізації ризиків. Для оцінки кожного з ризиків пропонується нечітка модель з чотирма вхідними параметрами (X_1,X_2,X_3,X_4) та одним виходом Y (структура MISO [10]). Кількість вхідних параметрів обрано відповідною до кількості факторів, що впливають на ступінь ризику (5). Таким чином, оцінку ризику інформаційної безпеки можна виразити як:

$$Y = f_Y(X_1, X_2, X_3, X_4), \quad (10)$$

де X_1 – цінність ресурсу, X_2 – вплив наслідку, X_3 – ймовірність виникнення загрози, X_4 –вразливість ресурсу

Для підтримки рівня захищеності ERP-системи необхідно визначити, які ризики, відповідно до рівня їх оцінки – risk level (RL), вимагають обробки за певними рекомендаціями. Для цього введемо 3 типи рівнів ризиків: прийнятний ризик – acceptable risk level (ARL) – будемо вважати незначним, обробка такого ризику не потрібна; середній ризик – middle risk level (MRL) – рекомендований до обробки з метою його мінімізації; високий ризик – high risk level (HRL) – будемо вважати істотним і його обробка є обов'язковою.

Визначення типу ризику будемо виконувати наступним чином:

$$\text{RL} = \begin{cases} ARL, R_{ij} \in [min_R; Pr_1]; \\ MRL, R_{ij} \in (Pr_1; Pr_2]; \quad i \in IR, j \in Th, \\ HRL, R_{ij} \in (Pr_2; max_R]; \end{cases} \quad (11)$$

де: RL – тип рівня ризику; R_{ij} – ризик і-го ресурсу при реалізації j-ї загрози; min_R – мінімальне значення оцінки ризику; max_R – максимальне значення оцінки ризику; Pr_1 – параметр, максимальне значення оцінки ризику прийнятного типу; Pr_2 – параметр, максимальне значення оцінки ризику середнього типу; IR – множина ресурсів системи; Th - множина загроз для системи. Максимальне значення оцінки прийнятного та середнього ризику (Pr_2та Pr_2 відповідно) встановлюються експертами.

Для опису лінгвістичної змінної Y будемо використовувати терм-множину $T(Y)$ з п’ятьох якісних термів: $T(Y)$ = {«Дуже низький ризик» (VLR); Низький ризик» (LR); «Середній ризик» (MR); «Високий ризик» (HR); «Дуже високий ризик» (VHR)}. Область визначення E_Y лінгвістичної змінної Y встановимо на інтервалі $[0; 100]$. Діапазони інтервалів для спрощення розрахунку можна взяти з кроком 20. Враховуючи обрану область визначення оцінки ризику інформаційної безпеки при визначенні типу ризику для надання рекомендацій відносно його зменшення за формулою (8), будемо використовувати наступні значення: min_R=0, max_R=100.

Цінність інформації будемо визначати як зв’язок між типом конфіденційності та критичності – criticality (C) інформації. Оцінка цінності формується як сума балів, що відповідають типу та рівню критичності інформації (табл.1). Критичність інформації будемо визначати, враховуючи оцінки наслідків порушення властивостей інформації. Для оцінювання лінгвістичної змінної X_1 «Цінність ресурсу» будемо використовувати терм-множину $T(X_1)$ з трьох якісних термів: $T(X_1)$ = {Низька цінність (LW); Середня цінність (MW); Висока цінність (HW)}. Область визначення E_{X_1} лінгвістичної змінної X_1 встановимо

на інтервалі [4;19]. Шкала оцінювання рівня цінності для кожної лінгвістичної змінної визначається значеннями 4, 11 та 19 відповідно.

Таблиця 1

Визначення оцінки цінності інформації

Тип інформації	Критичність інформації (С)		
	Незначна (1-3 бал)	Суттєва (4-9 балів)	Критична (10-15 балів)
Відкрита (1 бал)	2-4	5-10	11-16
Для внутрішнього використання (2 бали)	3-5	6-11	12-17
Конфіденційна (3 бали)	4-6	7-12	13-18
Суворо конфіденційна (4 бали)	5-7	8-13	14-19

Для оцінювання лінгвістичної змінної X_3 «Рівень ймовірності загрози» будемо використовувати терм-множину $T(X_3)$ з п'ятьох якісних термів: $T(X_3)$ = {Дуже низька ймовірність загрози (VLT); Низька ймовірність загрози (LT); Середня ймовірність загрози (MT); Висока ймовірність загрози (HT); Дуже висока ймовірність (VHT)}. Область визначення E_{X_3} лінгвістичної змінної X_3 встановимо на інтервалі [0,05;365]. Терму VLT відповідає ситуація, коли загроза практично ніколи не реалізується або реалізується не більше ніж 2-3 рази на п'ять років (частота в діапазоні [0;0,6]). Терму LT відповідає ситуація, коли загроза виникає 1-2 рази на рік (частота в діапазоні [1;2]). Терму MT відповідає ситуація, коли загроза виникає 1 раз в 2-3 місяці (частота в діапазоні [4;6]). Терму HT відповідає ситуація, коли загроза виникає 1-2 рази на місяць (частота в діапазоні [12;24]). Терму VHT відповідає ситуація, коли загроза виникає від 1 раз на тиждень до 1 разу на день (частота в діапазоні [52;365]).

При оцінюванні лінгвістичної змінної X_4 «Вразливість ресурсу» будемо спиратися на загальну систему оцінки вразливостей Common Vulnerability Scoring System (CVSS), що складається з трьох метрик та надає спосіб зафіксувати основні характеристики вразливості й створити числовий бал, що відображає її критичність [11]. Для отримання якісної метрики вразливостей будемо використовувати систему оцінки Національної бази даних вразливостей National Vulnerability Database (NVD) [12]. У базі даних NVD значення рівня безпеки вразливості обчислюються значеннями від 0 до 10 та описуються лінгвістично термами None, Low, Medium,High та Critical [13]. Відповідно до лінгвістичних термів бази NVD для оцінювання лінгвістичної змінної X_4 «Вразливість ресурсу» будемо використовувати терм-множину $T(X_4)$ з чотирьох якісних термів: $T(X_4)$ = {Низька вразливість (LV); Середня вразливість (MV); Висока вразливість (HV); Критична вразливість (CV)}. Область визначення E_{X_4} лінгвістичної змінної X_4 встановимо на інтервалі [0;10]. У списку наведено оцінки рівня вразливості згідно NVD за балами та лінгвістично, опис наслідку експлуатації та відповідні рівні вразливості ресурсу за терм-множиною $T(X_4)$:

– рівень вразливості LV: рівень за NVD None (вразливість не має впливу на ресурс, бал за NVD 0.0) або Low (вразливість, що має незначний вплив на ресурс, не впливає на доступність, цілісність та конфіденційність інформації, бал за NVD 0.1-3.9);

– рівень вразливості MV: рівень за NVD Medium (вразливість, що може мати певний вплив на ресурс, але має складність реалізації або не спричиняють серйозних наслідків; можливий доступ до конфіденційної інформації, зміна деякої інформації, але немає контролю над інформацією, або масштаби втрат невеликі; відбуваються збої в доступності ресурсу, бал за NVD 4.0-6.9);

– рівень вразливості HV: рівень за NVD High (вразливість, що має істотний вплив на ресурс, можливий доступ до конфіденційної інформації, зміна інформації та контроль над інформацією; суттєві збої в доступності ресурсу та зменшення продуктивності, бал за NVD 7.0-8.9);

– рівень вразливості CV: рівень за NVD Critical (вразливість, наслідок експлуатації якої має серйозний вплив на ресурс: повна втрата доступності та цілісності інформації, повне

розкриття конфіденційної інформації, бал за NVD 9.0-10.0);

Відповідно до розробленої структури нечіткої моделі за допомогою інструменту Fuzzy Logic Designer пакету Fuzzy Logic Toolbox було розроблено нечітку продукційну модель, структуру якої наведено на рис.1.

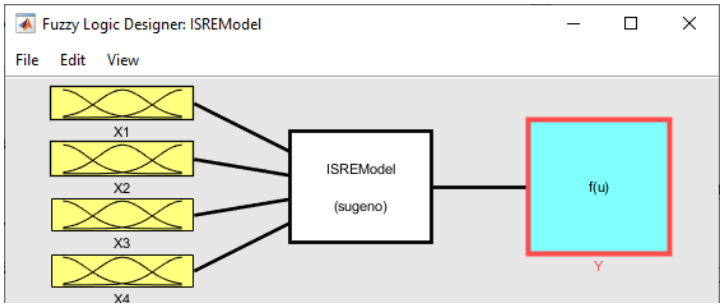

Рис. 1. Структура нечіткої продукційної моделі, реалізована у Fuzzy Logic Toolbox

Розроблена нечітка модель має структуру MISO (Multi Inputs – Single Output): чотири входи (фактори оцінки ризику) та один вихід (оцінка ризику). Серед доступних у Fuzzy Logic Toolbox моделей, що використовують алгоритми нечіткого висновку, було обрано модель Сугено. Типом функції приналежності обрано колоколоподібну криву – функцію розподілу Гауса.

Відповідно до структури правил було сформовано початкову базу правил, фрагмент якої наведено на рис. 2.

1. If (X1 is LW) and (X2 is VLC) and (X3 is VLT) and (X4 is LV) then (Y is VLR) (1)
2. If (X1 is LW) and (X2 is VLC) and (X3 is VLT) and (X4 is MV) then (Y is VLR) (1)
3. If (X1 is LW) and (X2 is VLC) and (X3 is VLT) and (X4 is HV) then (Y is LR) (1)
4. If (X1 is LW) and (X2 is VLC) and (X3 is VLT) and (X4 is CV) then (Y is LR) (1)
5. If (X1 is LW) and (X2 is VLC) and (X3 is LT) and (X4 is LV) then (Y is VLR) (1)
6. If (X1 is LW) and (X2 is VLC) and (X3 is LT) and (X4 is MV) then (Y is VLR) (1)
7. If (X1 is LW) and (X2 is VLC) and (X3 is LT) and (X4 is HV) then (Y is LR) (1)
8. If (X1 is LW) and (X2 is VLC) and (X3 is LT) and (X4 is CV) then (Y is LR) (1)
9. If (X1 is LW) and (X2 is VLC) and (X3 is MT) and (X4 is LV) then (Y is VLR) (1)
10. If (X1 is LW) and (X2 is VLC) and (X3 is MT) and (X4 is MV) then (Y is VLR) (1)

Рис. 2. Фрагмент бази продукційних правил моделі

\

Засобами інструментарію дозволяється при створюванні правила вказувати вагу, тобто значущість правила, яка має область визначення [0;1]. В побудованій базі усі правила, за замовчуванням, мають однакову вагу 1. Візуально результати роботи логічного висновку розробленої нечіткої продукційної моделі для певного набору даних можна отримати за допомогою вікна перегляду правил Rule Viewer інструменту Fuzzy Logic Toolbox, ліва частина якого відображає функції приналежності вхідних X_1, X_2, X_3, X_4, права частина значення вихідного Y з поясненням механізму прийняття рішення. На рис.3 наведено приклади формування результатів роботи логічного висновку для вхідних X_1=5, X_2=4, X_3=54 та X_4=6, які відповідають значенням термів LW (ресурс має низьку цінність), HC (для ресурсу характерні суттєві наслідки реалізації загрози), VHT (дуже висока ймовірність загрози) та MV (ресурс має середню вразливість). За результатами висновків отримано оцінку ризику Y=54,2, що відповідає середньому рівню ризику MR.

Тестування на 4 тестових наборах, кожен з яких складався з 300 правил, показало відхилення модельних значень близько 6% відносно висновків, сформованих експертами, що свідчить про високу ефективність застосування запропонованої моделі для попередньої автоматизованої оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем.

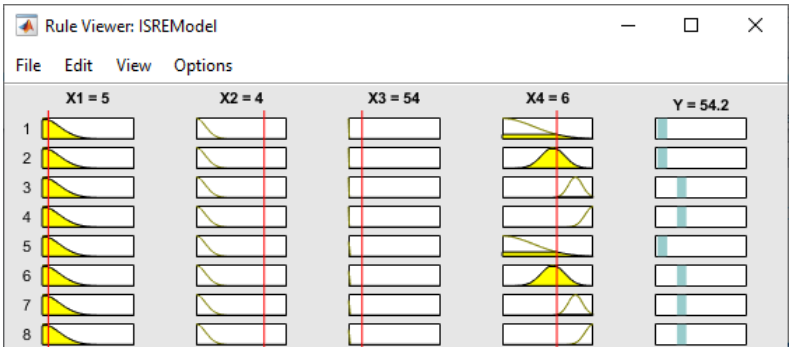

Рис. 3. Приклади результатів роботи логічного висновку продукційної моделі для вхідних даних X_1=5, X_2=4, X_3=54, X_4=6 (тестові правила 1-8)

4. Висновки. Використання нечіткої моделі забезпечує більш гнучке опрацювання неточних/якісних факторів ризиків інформаційної безпеки та дозволяє перейти до числового представлення будь-яких якісних характеристик. Запропонована нечітка модель та методи можуть бути використані як для оцінки конкретних видів ризиків інформаційної безпеки ресурсів ERP-системи, так і загального ризику інформаційної безпеки ERP-системи. В умовах реального підприємства використання нечіткої моделі передбачає виконання певного блоку підготовчих робіт, як от: ідентифікувати конкретні об'єкти захисту ERP-системи; скласти перелік загроз та можливих вразливостей; скласти перелік актуальних для ERP-систем пар загроза/вразливість (з врахуванням особливостей бізнес-процесів); виконати оцінку ймовірностей реалізації загрози з використанням вказаної вразливості; виконати оцінку наслідків від реалізації загрози, впливу реалізації загрози на цілісність, конфіденційність, доступність та спостережуваність інформації; виконати оцінку ризику від реалізації загрози; визначити рівень ризику та надати рекомендації до необхідності його обробки; виконати оцінку ризику інформаційної безпеки за активом та бізнес-процесом. Перспективою розвитку запропонованої моделі є використання адаптивної нейро-нечіткої продукційної моделі, що дозволить виконувати переоцінки ризиків у разі змін значень факторів, змін у продукційній базі правил або при виникненні нових ризиків.

Список використаної літератури

1. Leighton J. Security Controls Evaluation, Testing, and Assessment Handbook / J. Leighton, Syngress, 2016. 678 p.

2 Методи захисту системи управління інформаційною безпекою: ДСТУ ISO/IEC 27001:2015. – 2016. – Чин. 2017.01.01. – Київ.: ДП «УкрНДНЦ», 2016. – 22с.

3. Abhishek kumar srivastav, Irman Ali, Shani Fatema. A Quantitative Measurement Methodology for calculating Risk related to Information Security. IOSR Journal of Computer Engineering (IOSR-JCE). Volume 16, Issue 1, Ver. IX (Feb. 2014), PP 17-20.

4. Ехлаков Ю.П. Нечеткая модель оценки рисков продвижения программных продуктов / Ю. П. Ехлаков // Бизнес-информатика. – 2014. – №3 (29). – С. 69-78.

5. Гладыш С.В. Представление знаний об управлении инцидентами информационной безопасности посредством нечетких временных раскрашенных сетей Петри / С.В. Гладыш // Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». – 2010. – №1 (17), 2010. – С. 57-64.

6. Nieto-Morote A.A. Fuzzy approach to construction project risk assessment / A. Nieto-Morote, F. Ruz-Vila. // International Journal of Project Management. – 2011. – Vol. 29, Issue 2. – P. 220–231.

7. Інформаційна безпека України в умовах євроінтеграції. Поняття загроз інформаційній безпеці. Види загроз інформаційної безпеки [Електронний ресурс] // Навчальні матеріали онлайн (pidruchniki.website). – Режим доступу: https://pidruchniki.com/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi.

8. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: НД ТЗІ 2.5-004-99. – 1999. – Чин. 1999.07.01. – К. : ДСТСЗІ СБ України, 1999. – 57 с.

9. Шевченко В. Л. Несанкціонований доступ до інформаційних ресурсів ERP-системи [Електронний ресурс] / В. Л. Шевченко, В. І. Кулажський, О. С. Кульчицький // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2014. – № 1. – С. 9-12.

10. Круглов В.В. Нечеткие модели и сети / В.В. Круглов, В. В. Борисов, А.С. Федулов – М.: Горячая линия–Телеком, 2012. – 284с.: ил.

11. Common Vulnerability Scoring System version 3.1: Specification Document. CVSS Version 3.1 Release [Електронний ресурс] // Forum of Incident Response and Security Teams. – Режим доступу: https://www.first.org/cvss/ specification-document.

12. National vulnerability database Release [Електронний ресурс] // National Institute of Standards and Technology. – Режим доступу: https://nvd.nist.gov.

13. National vulnerability database Release. Vulnerability Metrics [Електроний ресурс] // National Institute of Standards and Technology. – Режим доступу: https://nvd.nist.gov/vuln-metrics/cvss.

References

1. Leighton J. (2016) Security Controls Evaluation, Testing, and Assessment Handbook, Syngress, 678 p.

2 Methods of information security management system protection: SSU ISO/IEC 27001:2015. 2016. Valid 2017.01.01. Kyiv.: State enterprise "UkrNDNC", (2016). 22 p.

3. Abhishek kumar srivastav, Irman Ali, Shani Fatema. A (2014) Quantitative Measurement Methodology for calculating Risk related to Information Security. IOSR Journal of Computer Engineering (IOSR-JCE). Volume 16, Issue 1, Ver. IX, Feb. 2014, P. 17-20.

4. Ekhlakov Yu.P. (2014) Fuzzy model for assessing the risks of software product promotion. Business informatics. 3 (29): P. 69-78.

5. Gladysh S.V. (2010) Presentation of knowledge on information security incident management through fuzzy temporary colored Petri nets. International Scientific and Technical Journal "Information Technology and Computer Engineering".. 1 (17): P. 57-64.

6. Nieto-Morote A.A. Ruz-Vila F. (2011) Fuzzy approach to construction project risk assessment. International Journal of Project Management. Vol. 29, Issue 2. P. 220–231.

7. Information security of Ukraine in the conditions of European integration. The concept of threats to information security. Types of information security threats. Learning materials online. https://pidruchniki.com/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi.

8. Criteria for assessing the security of information in computer systems from unauthorized access ND TPI 2.5-004-99. 1999. Valid 1999.07.01. K. : SSIPS SS Of Ukraine. 57 p.

9. Shevchenko V.L., Kulazhsky V.I., Kulchytsky O.S. (2014) Unauthorized access to information resources of the ERP-system. Collection of scientific works of the Center for Military Strategic Studies of the Ivan Chernyakhovsky National University of Defense of Ukraine. 1. P. 9-12.

10. Kruglov V.V., Borisov V.V., Fedulov A.S. (2012) Fuzzy models and networks. Hotline - Telecom,. 284p.

11. Common Vulnerability Scoring System version 3.1: Specification Document. CVSS Version 3.1 Release. Forum of Incident Response and Security Teams. https://www.first.org/cvss/ specification-document.

12. National vulnerability database Release . National Institute of Standards and Technology. https://nvd.nist.gov.

13. National vulnerability database Release. Vulnerability Metrics. National Institute of Standards and Technology. https://nvd.nist.gov/vuln-metrics/cvss.