УДК 004.02+004.05+005.93+ 510.3 https://doi.org/10.15407/pp2018.04.082

Є.С. Родін

МЕТОД ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ПІДТРИМКИ УПРАВЛІННЯ РИЗИКАМИ БЕЗПЕКИ РЕСУРСІВ ВІДОМЧИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Запропоновано формалізацію вразливостей та загроз за допомогою введення лінгвістичних змінних. Практично використано гібридні моделі та soft computing при побудові залежності рівня ризику виникнення помилок за двома факторами. Запропоновано два варіанти оцінювання впливу вразливостей на рівень ризику результуючого фактора. Запропоновано комбінацію використання статистичних даних та експертних оцінок для аналізу стану інформаційної безпеки організації. Запропоновано визначення сукупного ризику інформаційного ресурсу.

Ключові слова: ризик, інформація, безпека, загроза, вразливість, нечіткість, логіка, модель.

Вступ

Актуальність досліджень у галузі управління ризиком інформаційної безпеки зумовлена:

- ростом кількості інцидентів інформаційної безпеки як в державному, так і в бізнес-секторі України;
- нестачею спеціалістів в області інформаційної безпеки;
- нестачею автоматизованих методів визначення та управління ризиками інформаційної безпеки.

Насамперед об'єктом даного дослідження є процес інформаційно-аналітичної підтримки управління ризиками безпеки ресурсів інформаційних систем. Предмет дослідження – це метод інформаційно-аналітичної підтримки процесів аналізу та оцінювання ризиків безпеки ресурсів відомчих інформаційних систем.

Етапи методу оцінювання ризику

Метод управління ризиком інформаційної безпеки ресурсу (рис. 1) передбачає:

- аналіз інфраструктури та опис інформаційних ресурсів за встановленими характеристиками;
- побудову дерева варіантів;
- перетворення елементів дерева варіантів (вразливостей, загроз, наслідків) на лінгвістичні змінні та нечіткі правила;
- побудову моделі впливу вразливостей, загроз, наслідків на рівень ризику [1].

Згідно з нормативними документами ДСТУ, НД ТЗІ 1.1-003-99, ISO, NIST, наведемо визначення базових понять.

Ризик – функція ймовірності використання загрозою вразливості та величини збитку від події (наслідку), що сталася внаслідок цього використання [2].

Загроза – подія, що веде до втрат. Джерела загроз: природні, людські, оточення [3].

Вразливість – слабкість організації, що проявляється в організаційній структурі, процедурах функціонування організації, в програмному забезпеченні, матеріальному забезпеченні. Відповідно до статистики NIST (https://nvd.nist.gov/), наразі налічується більше ніж 94000 вразливостей інформаційної безпеки [2].

Наслідок – якісна та кількісна величина, що характеризується втратою конфіденційності, цілісності, доступності [4].

Управління ризиком являє собою сукупність заходів щодо оцінювання ризику, вибору, реалізації і впровадження заходів безпеки, спрямованих на досягнення прийнятного рівня залишкового ризику. Управління ризиком передбачає три процеси: оцінювання ризику, зменшення ризику (прийняття ризику), оцінювання заходів щодо зменшення ризику [5].

Оцінювання ризику складається з таких етапів:

1) опис системи;
2) визначення загроз;
3) визначення вразливостей;

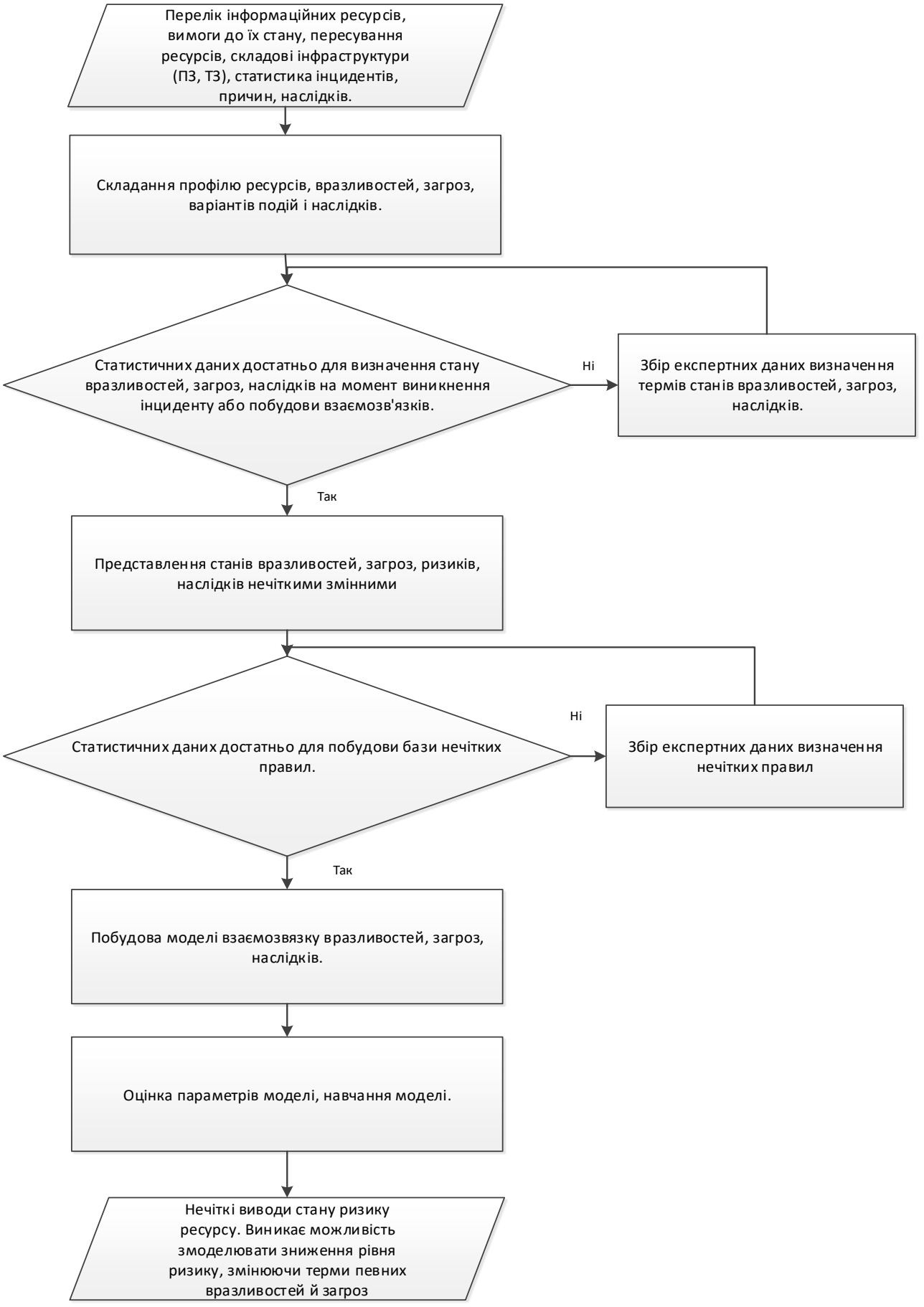

Рис. 1. Процесна схема методу інформаційно-аналітичної підтримки управління ризиками безпеки ресурсів відомчих інформаційних систем

4) аналіз системи контролю безпеки, визначення ймовірності використання загрозою вразливості, аналіз наслідку, визначення ризику;

5) розробка рекомендацій;

6) документування результатів [6].

Сучасні підходи оцінювання ризику

Існуючі методи оцінювання ризику можна охарактеризувати такими тезами:

- аналіз системи контролю безпеки забезпечується проходженням перевірочного списку максимальної кількості вимог;
- визначення ймовірності використання загрозою вразливості забезпечується експертним методом, здебільшого − наданням трьох рівнів ступеня ймовірності;
- аналіз наслідку забезпечується експертним методом, здебільшого − наданням трьох рівнів ступеня можливих втрат;
- визначення ризику забезпечується експертним методом складання матриці перетину рейтингів ймовірності та наслідку;
- ризик приймається, якщо витрати ймовірного порушника перевищують його ймовірний заробіток або якщо передбачувані втрати не перевищують допустимий поріг [7].

Сучасні фреймворки з управління ризиками інформаційної безпеки базуються на засадах NIST і ISO та відтворені в однойменних продуктах:

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation);
- COBIT (Control Objectives for Information and Related Technologies);
- CRAMM (CCTA Risk Analysis and Management Method);
- FRAP (Facilitated Risk Analysis Process);
- RiskWatch [7].

Важливу проблематику сучасних досліджень у галузі інформаційної безпеки становлять підходи щодо формалізації управління ризиком. Наразі найбільш поширеними підходами є Soft computing (неоднозначні обчислення) або Hybrid models (гібридні моделі).

Soft computing базується на використанні:

- Machine learning (машинне навчання, моделі, що здатні навчатися);
- нечітка логіка;
- еволюційні обчислення (штучний інтелект);
- ймовірнісні обчислення [8].

Основою гібридних моделей є Аналітичний ієрархічний процес (Analytic hierarchy process, AHP).

Приклад застосування методу

Комбінуючи досвід сучасних підходів щодо оцінювання ризику інформаційної безпеки та намагаючись націлити оцінювання ризику на конкретні інформаційні ресурси системи, можна запропонувати такий перелік завдань, що забезпечить подальше моделювання взаємодії вразливостей, загроз, ризиків, наслідків, протидій:

- визначити профіль інформаційних ресурсів;
- визначити ролі суб’єктів (у тому числі порушників);
- визначити шляхи пересування інформаційних ресурсів (IP);
- ідентифікувати вразливості по кожному IP;
- ідентифікувати загрози по кожному IP;
- визначити фактори впливу (вразливості, загрози, наслідки) на величини ризику (вагомості) реалізації кожної загрози;
- визначити рівень ризику по кожній загрозі [4].

Наведемо приклад визначення рівня ризику ресурсу «Клієнтська база даних».

Виконання завдань 1–5 забезпечується проходженням перевірочного переліку характеристик інформаційного ресурсу, що консолідується в анкеті ресурсу [9].

Інформаційний ресурс: база даних клієнтів.

1. Форма представлення: електронна база CRM, документ у форматі ms-excel.

2. Статичність: ресурс переміщується.

3. Оригінальність: оригінал на зовнішній CRM, є декілька експортних копій.

4. Місце появи: на персональних пристроях (ПК, флеш-накопичувач, мобі-

льний телефон), на серверах зовнішньої мережі (зовнішня CRM, хмарне сховище).

5. Шляхи пересування: на флеш-накопичувачі, електронна пошта, через чати, доступ на хмарі.

6. Варіанти доступу: обмежений доступ для внутрішнього персоналу. Управління доступом мають генеральний директор та директор з маркетингу. Права читання та редагування мають: генеральний директор, директор з маркетингу, менеджер з продажів.

7. Загрози ресурсу:

a) при порушенні конфіденційності:

i) втрата репутації перед клієнтами (так, ні, вірогідність),

ii) порушення договору про нерозголошення – грошовий штраф (так, ні, вірогідність),

iii) можлива втрата клієнта – втрата доходу (так, ні, вірогідність);

b) при порушенні цілісності: є копії;

c) при порушенні доступності: є копії;

d) при порушенні керованості: простій у роботі відділу продажів, веде до порушення a, b, c;

e) порушення відновлюваності: втрата клієнтів, доходу, репутації, простій у роботі відділу продажів.

Вразливості першого рівня ресурсу:

- збереження та пересування на флеш-накопичувач;
- пересування електронною поштою;
- помилки при керуванні правами доступу;
- вразливості настроювання внутрішньої сітки та наявність фаєрвол, IDS.

Вразливості другого рівня:

- рівень кваліфікації персоналу;
- рівень якості Політики інформаційної безпеки;
- рівень надійності внутрішнього серверного ПЗ;
- рівень надійності внутрішнього серверного ТЗ;
- ненадійна зовнішня CRM;
- відсутність резервної копії.

Завдання 6 виконується побудовою зв'язків впливу вразливостей, загроз та наслідків на сумарний рівень ризику (рис. 2).

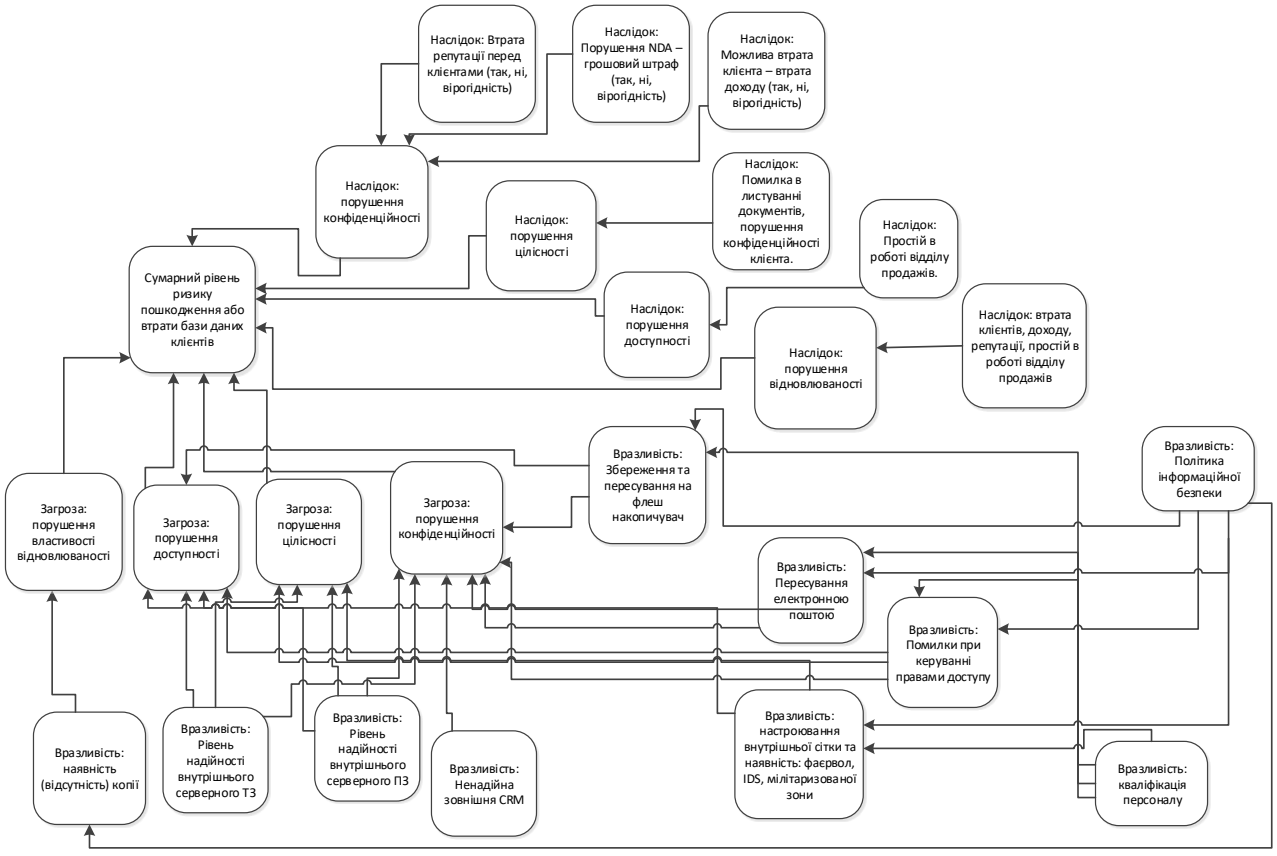

Рис. 2. Зв'язки впливу вразливостей, загроз та наслідків на сумарний рівень ризику ресурсу База даних клієнтів

Завдання 7 розбивається на послідовне визначення впливу окремих вразливостей і загроз на величину ризику.

Розглянемо *задачу побудови моделі впливу вразливостей другого рівня* Рівень кваліфікації персоналу та Рівень якості Політики інформаційної безпеки на вразливість першого рівня Помилки при керуванні правами доступу.

Постановка задачі така:

- Побудова моделі взаємозв'язку трьох вразливостей за статистичними даними.
- Навчання моделі.
- Побудова моделі взаємозв'язку трьох вразливостей за експертними даними.
- Порівняння моделей.

Представлення вразливостей лінгвістичними змінними наведено в табл. 1.

Таблиця 1. Представлення вразливостей лінгвістичними змінними

Лінгвістична змінна – Рівень якості політики інформаційної безпеки		
b1		
Стани якості документа політики ІБ (терми)	Універсальна множина (рейтинг якості 0–10)	Значення функції належності =1
документ політики відсутній	0	0
документ є в наявності, але не досконалий	1–3	2
документ досконалий, але не оновлюється	4–7	5.5
документ повний та оновлюється щороку	7–10	10
Лінгвістична змінна – Рівень кваліфікації персоналу		
b2		
Терми рівня кваліфікації	Універсальна множина: процент співробітників з досвідом роботи більше 5 років (0–100 %)	Значення функції належності =1
персонал слабо кваліфікований	0–40	20
персонал середньо кваліфікований	41–70	55.5
персонал достатньо кваліфікований	71–100	85.5
Лінгвістична змінна – Помилки при керуванні правами доступу		
b8		
Стани події: кількість помилок за останній рік (терми)	Універсальна множина (кількість помилок за рік 0–10)	Значення функції належності =1
Недопустимо багато помилок	5–10	7.5
Помірна кількість помилок	1–4	2.5
Немає помилок	0	0

Будуємо ANFIS-модель за статистичними даними, а також функції належності шляхом використання методу нечіткої кластеризації к-середніх (Fuzzy C-Means Clustering) і статистичних даних (рис. 3, 4).

Формуємо систему нечітких правил (рис. 5) [10]. За Sugeno: кожен терм змінної b1 і кожен терм змінної b2 мають давати терм змінної b8. Отже, маємо 12 термів для b8. Будуємо 12 кластерів для b8 за статистичними даними. Для Sugeno функції належності не потрібні – лише центри кластерів. Зв'язок між термами змінних b1, b2 та b8 встановлюється також по центрах кластерів (шукаємо за статистичними даними відповідне значення b8 і найближчий центр кластера, за яким і визначаємо необхідний терм b8).

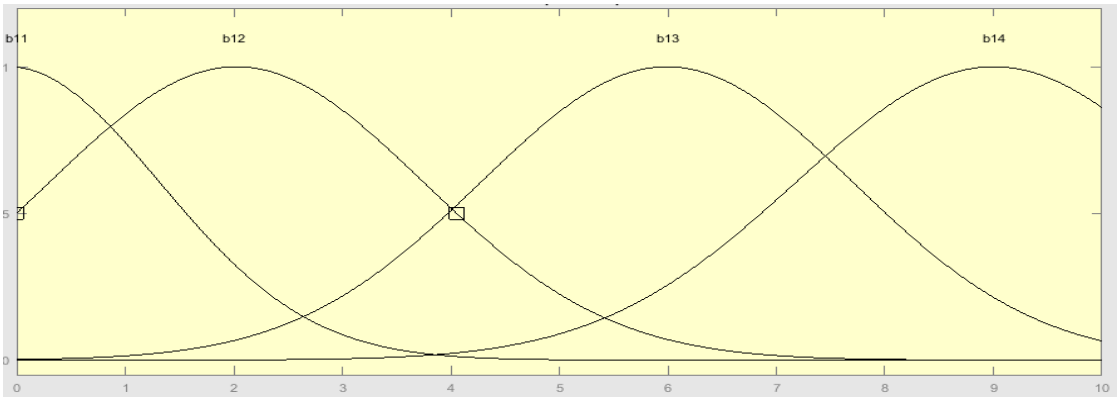

Рис. 3. Функція належності рівня якості політики інформаційної безпеки

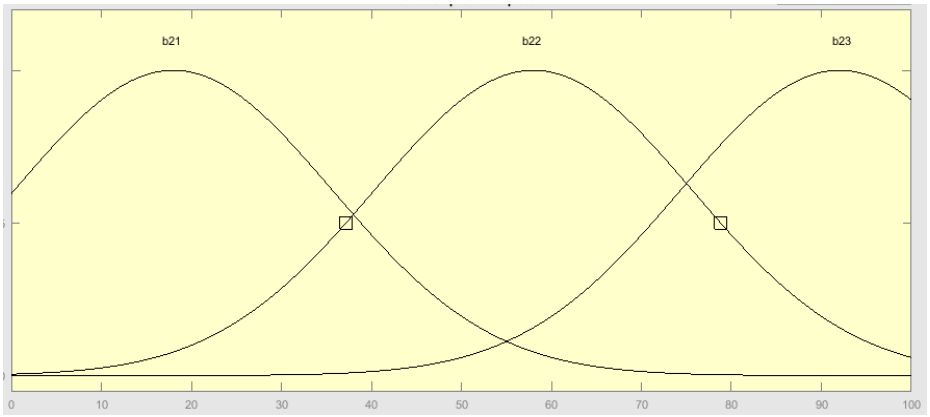

Рис. 4. Функція належності рівня кваліфікації персоналу

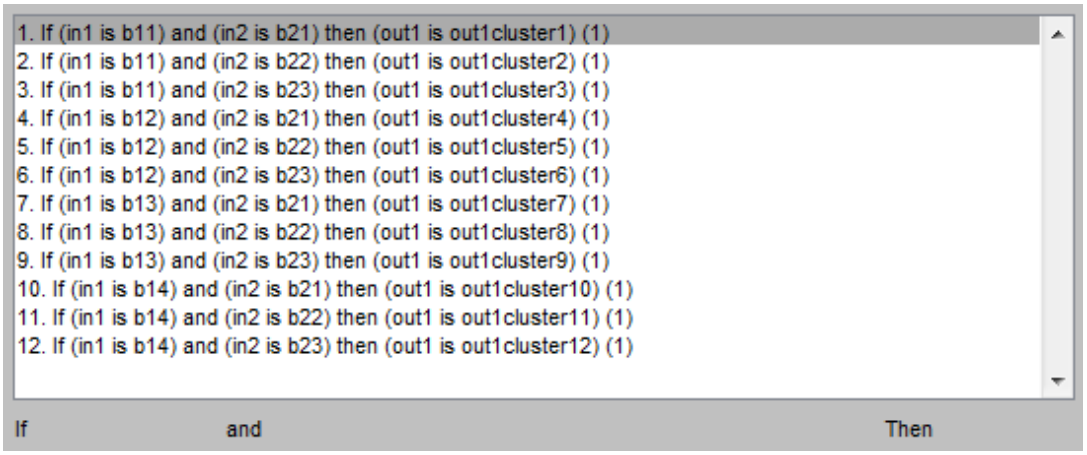

Рис. 5. Система нечітких правил

Проводимо навчання моделі (рис. 6). Навчання ANFIS відбувається за допомогою гібридного методу, який базується на рекурсивному МНК та градієнтному спуску.

Перевіряємо побудову моделі розрахунком b8 до кожної пари b1, b2 та порівнюємо зі статистичними даними (сині кола на рис. 7).

Спробуємо визначити функцію належності b8 за побудованою моделлю. Генеруємо всі нечіткі виводи за побудованою моделлю ANFIS та ділимо їх на три групи вже згідно з експертними правилами [11].

Виконуємо процедуру оцінювання функції належності за частотами. Будуємо гістограми (рис. 8).

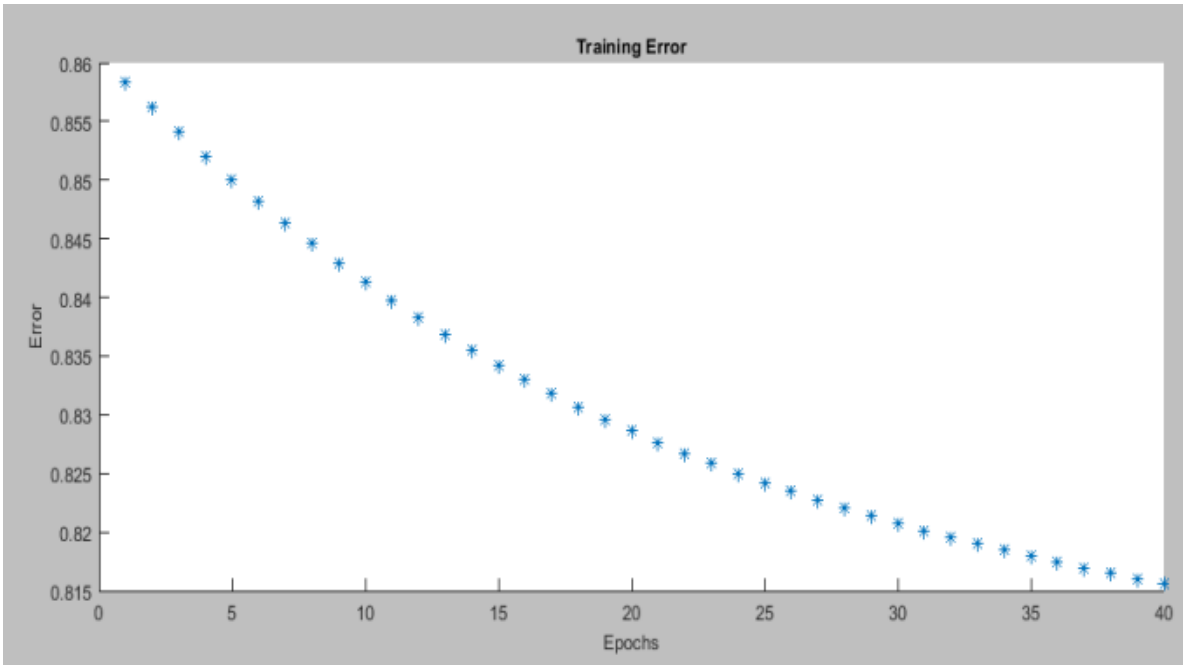

Рис. 6. Крива помилок

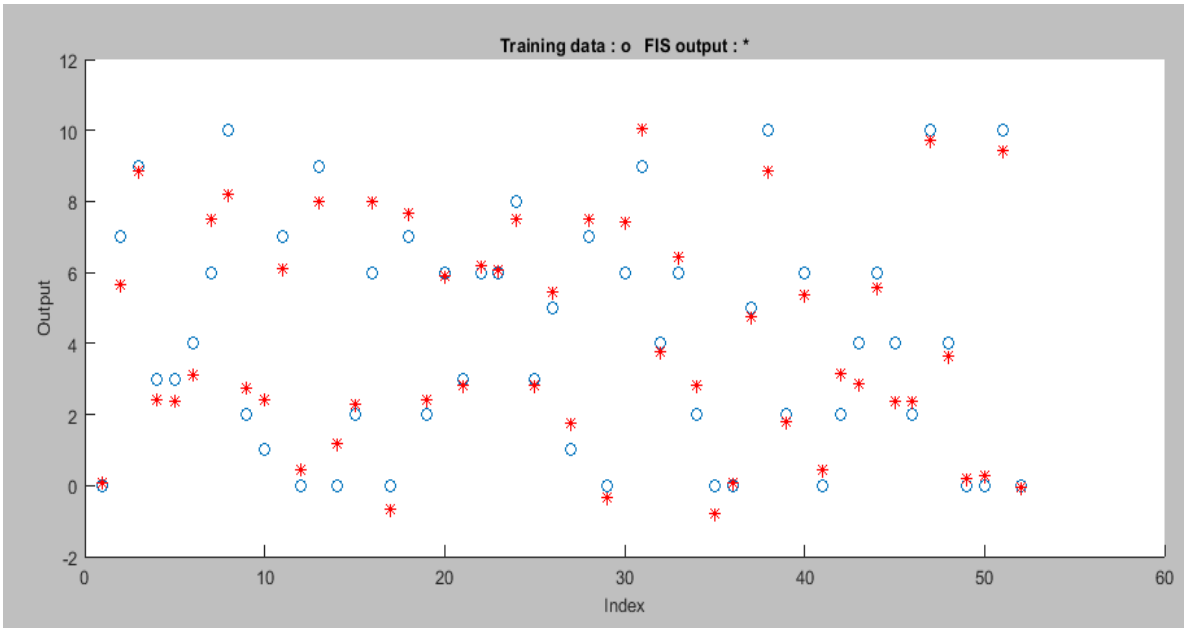

Рис. 7. Графік порівняння моделей

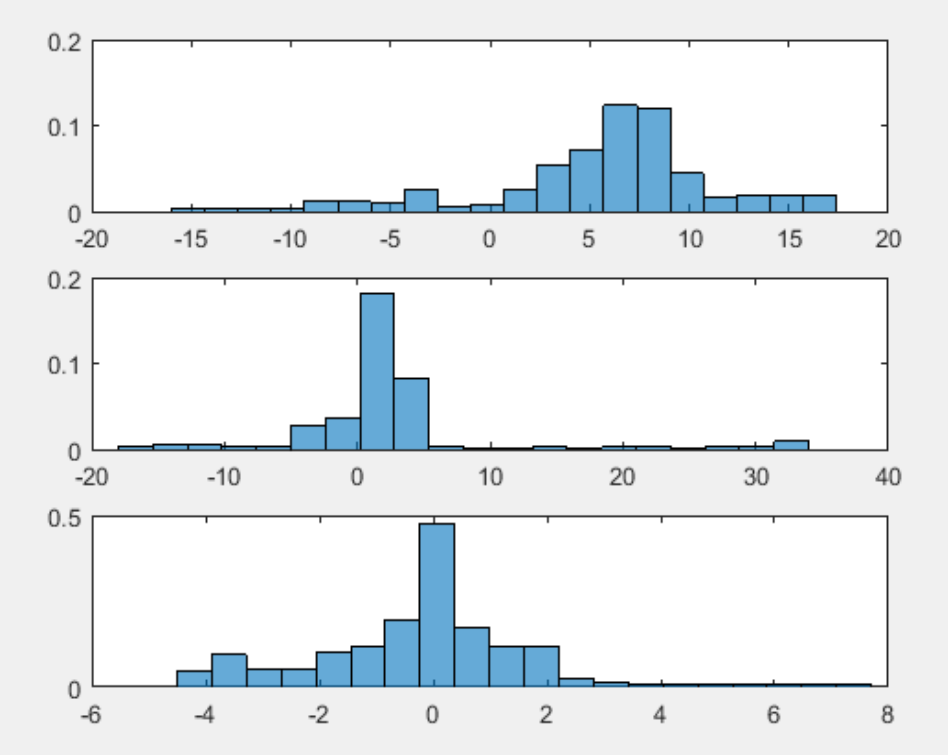

Рис. 8. Оцінювання функцій належності

Із гістограм видно, що функції належності близькі до функцій Гаусса. Отже, оцінимо їх параметри: середнє та дисперсію:

середнє	дисперсія
6.1631	2.1658
2.5439	1.2682
1.2130	1.4284

Результуючі функції належності для b8, отримані за моделлю ANFIS із використанням припущення щодо їх гауссовості, показано на рис. 9.

Будуємо модель за допомогою апарата нечіткої логіки експертних оцінок, а також функції належності b1, b2, b8 відповідно до методу прямого рейтингу (рис. 10).

Будуємо модель Mamdani за експертними нечіткими правилами (рис. 11).

Порівняємо побудовані моделі, будуючи графіки нечітких виводів b8 при фіксації однієї змінної для всіх значень іншої (рис. 12).

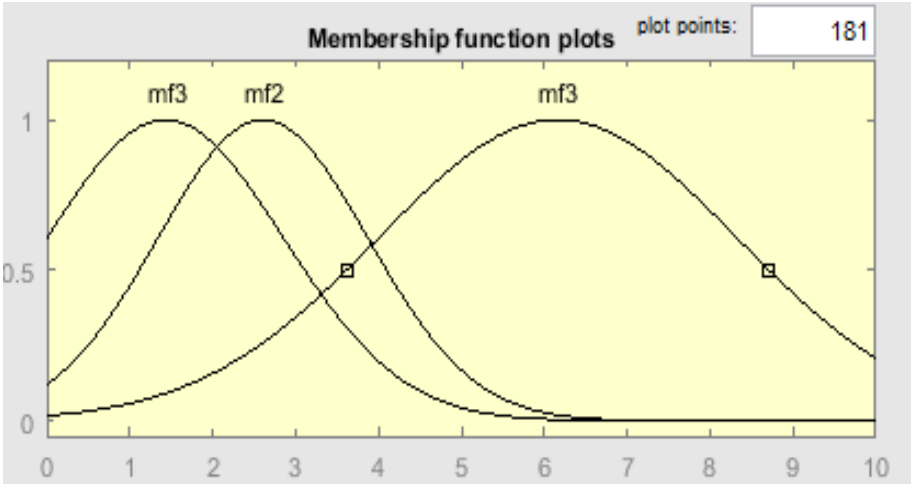

Рис. 9. Результуючі функції належності для b8

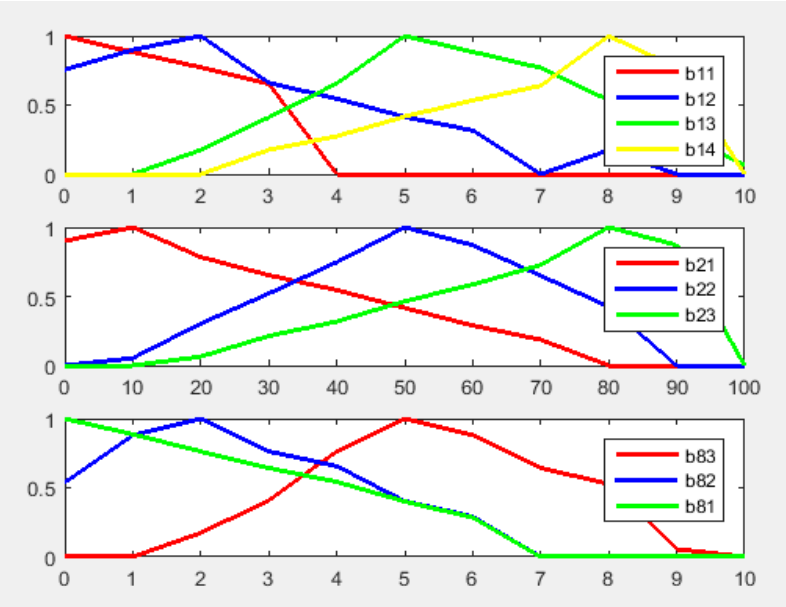

Рис. 10. Функції належності b1, b2, b8

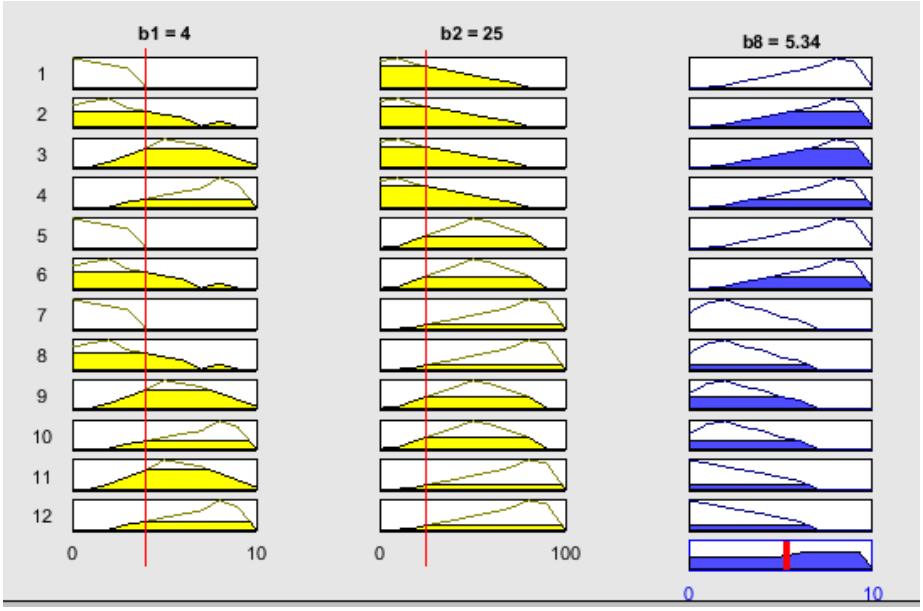

Рис. 11. Результуючі правила за моделлю Mamdani

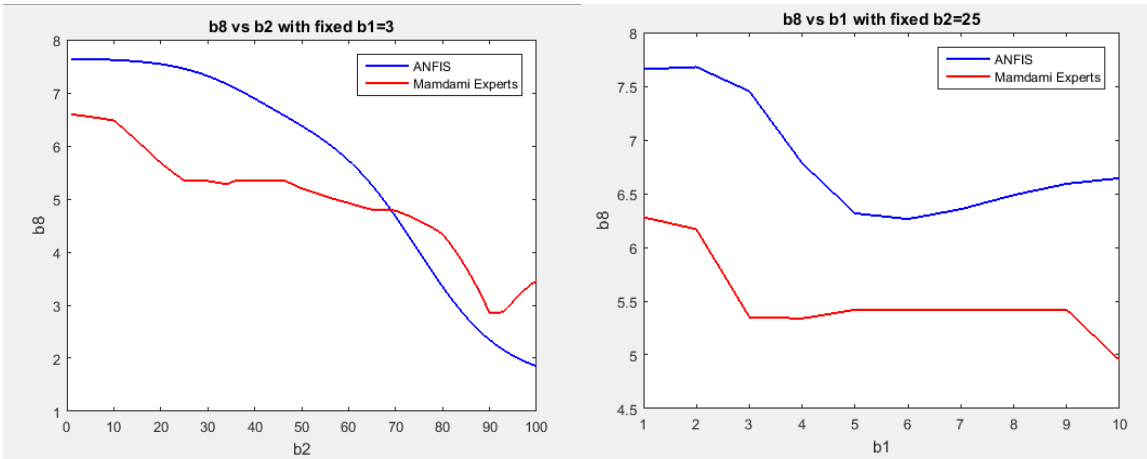

Рис. 12. Порівняння моделей за ANFIS та Mamdani

Порівняємо достовірність моделей. Отримаємо нечіткі виводи двох моделей за тестовими даними.

Середньоквадратичні помилки (Mean Square Error):

-ANFIS: 2.4681,

-Expert: 5.0442.

Відносні процентні помилки (Relative Percentage Error):

-ANFIS: -4.0967 %,

-Expert: -13.5927 %.

Отже, експертне оцінювання показує гірші результати, ніж самонавчальна модель за статистичними даними.

Висновки

1. Існуючі методи управління ризиком інформаційної безпеки передбачають певну послідовність кроків, направлених на оцінювання системи, її вразливостей, загроз та наслідків випадку з безпеки.

У роботі пропонується метод, який передбачає моделювання взаємодії та впливу вразливостей і загроз для стану ризику ресурсу. Це дозволить відстежити, які саме вразливості та загрози певною мірою впливають на стан безпеки ресурсу.

2. Існуючі методи управління ризиком інформаційної безпеки передбачають вимірювання рівня ризику за значенням вірогідності небезпечного випадку загрози та рівня наслідку небезпечного випадку.

У роботі пропонується вимірювати рівень ризику для конкретного інформаційного ресурсу за сумарними рівнями ризику небезпечних подій з дерева подій, що відображає багатофакторність впливу вразливостей та загроз.

3. За допомогою апарату нечіткої логіки та підходів щодо побудови самонавчальних моделей у роботі пропонується будувати адаптивні моделі впливу факторів вразливостей та загроз на кількість та якість небезпечних випадків.

Література

1. Боровська О.М., Сініцин І.П., Родін Є.С. Порівняння національного та міжнародного підходів побудови системи захисту інформації в грід. *Проблеми програмування.* 2011. № 5. С. 99−109.
2. Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf.
3. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99. http://dstszi.kmu.gov.ua.
4. International standard BS ISO/IEC 27005:2008, 2008-06-15.
5. Загородній А.Г., Боровська О.М., Свістунов С.Я., Сініцин І.П., Родін Є.С. Створення комплексної системи захисту інформаційних ресурсів у національній ґрід-інфраструктурі України. К.: Сталь, 2014. 373 с.
6. Боровська О.М., Свістунов С.Я., Сініцин І.П., Шилін В.П., Родін Є.С. Підходи до створення комплексної системи захисту інформації в Національній грід-інфраструктурі. К., 2010. 51 с. (Препр. / НАНУ. Ін-т теоретичної фізики ім. Боголюбова М.М.).
7. Родін Є.С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки. *Математичні машини і системи.* 2012. № 4. С. 142−148.
8. Ming-Chang Lee. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. *International Journal of Computer Science & Information Technology (IJCSIT).* 2014. Vol. 6, N 1.
9. Integrated Site Security for Grids. https://isseg-training.web.cern.ch/ISSeG-training/
10. Zadeh L.A. The concept of linguistic variable and its application to approximate reasoning. *Information sciences*. 1975. № 8. P. 199−249.
11. Малышев Н.Г., Берштейн Л.С., Боженюк А.В. Нечеткие модели для экспертных систем в САПР. М.: Энергоатомиздат, 1991. 136 с.

References

1. Borovska O., Sinitsyn I., and Rodin Y. (2011). Comparing national and worldwide approaches in developing grid information security system. Programming Problems. 5, P. 99–109. (In Ukrainian)
2. Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf.
3. Terminology in the field of information security in computer systems from unauthorized access. ND TZI 1.1-003-99. http://dstszi.kmu.gov.ua. (In Ukrainian)
4. International standard BS ISO/IEC 27005:2008, 2008-06-15.
5. Zagorodnyy A., Borovska O., Svistunov S., Sinitsyn I., Rodin Y. (2014) Creation of an integrated information resource protection system in the national grid infrastructure. K.: Stal, 373 p. (In Ukrainian)
6. Borovska O., Svistunov S., Sinitsyn I., Shilin V., Rodin Y. (2010). Approaches in developing information security system in the national grid infrastructure. Kyiv: Bogolyubov Institute for Theoretical Physics, 51 p. (In Ukrainian)
7. Rodin Y. (2012). Processing approaches in the field of information security risk management modeling. Mathematical Machines and Systems, 4, P. 142–148.
8. Ming-Chang Lee. (2014). Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. International Journal of Computer Science & Information Technology (IJCSIT). Vol. 6, N 1.
9. Integrated Site Security for Grids. – https://isseg-training.web.cern.ch/ISSeG-training/
10. Zadeh L. (1975). The concept of linguistic variable and its application to approximate reasoning. Information sciences, 8, P. 199−249.
11. Malyshev N., Bershtein L., Bozhenyuk A. (1991). Fuzzy modeling for experts systems in SAPR. Moscow: Energoatomizdat, p. 136. (In Russian)

Одержано 28.09.2018

***Про автора*:**

Родін Євген Сергійович,
молодший науковий співробітник.
Кількість наукових публікацій в українських виданнях – 6.
http://orcid.org/0000-0003-2416-8572.

***Місце роботи автора*:**

Інститут програмних систем
НАН України.
03187, м. Київ-187,
проспект Академіка Глушкова, 40.
Тел.: (044) 526 5507.
Моб. тел.: (067) 407 0962.
E-mail: yevheniy.s.rodin@gmail.com