УДК 004.02+004.05+005.93+ 510.3

Є.С. Родін

ЗАДАЧІ З КЕРУВАННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АПАРАТА ПРИЙНЯТТЯ РІШЕНЬ

Запропоновано перелік завдань, вирішення яких веде до побудови моделі залежності рівня ризику інформаційної безпеки ресурсу від наявності зв'язків та ступеню впливу вразливостей, загроз і наслідків на даний інформаційний ресурс та організацію в цілому. Наведено приклади побудови для окремого інформаційного ресурсу дерев зв'язків між вразливостями, загрозами, наслідками подій інформаційної безпеки, а також приклади математичної формалізації залежності рівня ризику реалізації певної загрози пошкодження або втрати інформаційного ресурсу від стану вразливостей та їх послідовного впливу на даний ресурс.

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

Вступ

Актуальна проблема сьогодення – це прийняття рішень у багатофакторному середовищі. Аналіз багатофакторності ускладнюється відсутністю достовірної фактичної інформації про суб'єкти, події, процеси. Залежність реалізації одних подій від інших, представлення реалізації різних сценаріїв ґрунтуються переважно на експертних оцінках. Багато сучасних моделей процесів прийняття рішень намагаються врахувати якомога більше факторів впливу та водночас нівелювати суб'єктивізм експертних оцінок. Саме такі умови притаманні сфері керування ризиками інформаційної безпеки апарата прийняття рішень.

Стаття пропонує до уваги читача приклади моделей і методів, які б у доступному вигляді допомогли непрофесіоналу в галузі оцінювання ризиків інформаційної безпеки (ІБ) побудувати її модель керування в сегменті своєї відповідальності.

Проблематика

Ключова модель, використовувана в сфері керування ризиками інформаційної безпеки (КРІБ), є процесна модель, що знайшла відображення в усіх стандартних підходах до КРІБ та являє собою основу стандартів ISO/IEC 27005 і BS 7799-3 [1]. Процесна модель дає перелік, послідовність та розкриває сутність таких необхідних для керування ризиками ІБ процесів, як планування, реалізація, перевірка, дія [2−5].

Базою для визначення рівня ризику майже в усіх методиках є ймовірність виникнення тієї чи іншої події, яка впливає на ймовірність реалізації загрози. У більшості методик визначення ймовірності здійснюється експертним методом або за основу береться статистика минулих періодів щодо таких самих подій.

Чи відповідає така методика реаліям, наскільки вона точна? По-перше, необхідно внести поправку на помилку експертів, по-друге, статистика минулих періодів не буде відповідати реальності, особливо у випадках швидкої зміни програмного та технічного забезпечення (вразливості якого ще невідомі), по-третє, існує більше факторів впливу на визначення ризику, ніж ймовірність реалізації загрози та сума збитків.

Пропоноване рішення полягає у застосуванні інструментів нечіткої логіки для розв'язання задач керування ризиком інформаційної безпеки [6−8].

Ціль керування ризиком – це визначення пріоритетів бюджетування напрямків зменшення ризику ІБ апарата прийняття рішень, а саме – зменшення або ліквідація вразливостей, загроз, можливих наслідків. Керування ризиком являє собою безперервне циклічне виконання певного переліку завдань. Окреслимо коло задач, вирішення яких дозволить досягнути поставленої цілі.

Задачі, що стоять перед менеджментом інформаційної безпеки

Перелік завдань може змінюватись залежно від того, на якому етапі та якісному рівні знаходиться процес керування ризиком ІБ в організації. Але навіть якщо деякі завдання вже виконані на якісному рівні, спеціаліст з безпеки має повернутися до них в наступному циклі керування ризиком ІБ.

1. Визначити профіль інформаційних ресурсів апарата прийняття рішень (АПР).

2. Визначити ролі суб'єктів АПР (у тому числі порушників).

3. Визначити шляхи пересування інформаційних ресурсів (ІР).

4. Ідентифікувати вразливості по кожному ІР.

5. Ідентифікувати загрози по кожному ІР.

6. Визначити фактори впливу (вразливості, загрози, наслідки) на величини ризику (вагомості) реалізації кожної загрози.

7. Визначити рівень ризику по кожній загрозі.

8. Розподілити річний бюджет витрат на ІБ та пріоритетність дій плану впровадження політики ІБ.

Розглянемо сутність цих задач і деякі способи їх розв'язання.

1. Визначити профіль ІР АПР.

Задача передбачає визначення переліку ІР АПР, опис кожного за стандартним профілем. Даний профіль може бути змінено відповідно до специфіки роботи організації.

Опис профілю ІР може бути проведений за такими ознаками:

- форма представлення:
  - дані в електронному вигляді,
  - дані в паперовому вигляді;
- статичність:
  - ресурс не переміщується (архіви),
  - ресурс переміщується;
- оригінальність ресурсу:
  - оригінал,
  - копія;
- місця появи ресурсу:
  - персональні пристрої,
  - сервери замкнутої внутрішньої мережі,
  - сервери зовнішньої мережі,
  - аналогові сховища;
- шляхи пересування:
  - всередині організації,
  - зовні організації;
- варіанти доступу до ресурсу:
  - повний внутрішній та зовнішній доступ,
  - обмежений внутрішній та зовнішній доступ,
  - доступ тільки внутрішньому персоналу,
  - обмежений доступ для внутрішнього персоналу;
- методи оцінювання:
  - критеріальний,
  - вартісний.

2. Визначити ролі суб'єктів АПР (у тому числі порушників).

Задача передбачає визначення переліку ролей суб'єктів АПР, побудову їх профілів щодо кожного ІР на базі рівнів доступу до ІР, побудову моделі порушника (мотиви, кваліфікація, рівень доступу).

На рис. 1 пропонується приклад моделі порушника.

3. Визначити шляхи пересування ІР.

Задача передбачає графічну побудову пересування ресурсів з урахуванням суб'єктів та технічних засобів АПР.

4. Ідентифікувати вразливості по кожному ІР.

При вирішенні задач 1−3, здійснюючи аналіз середовища ІБ, спеціаліст з

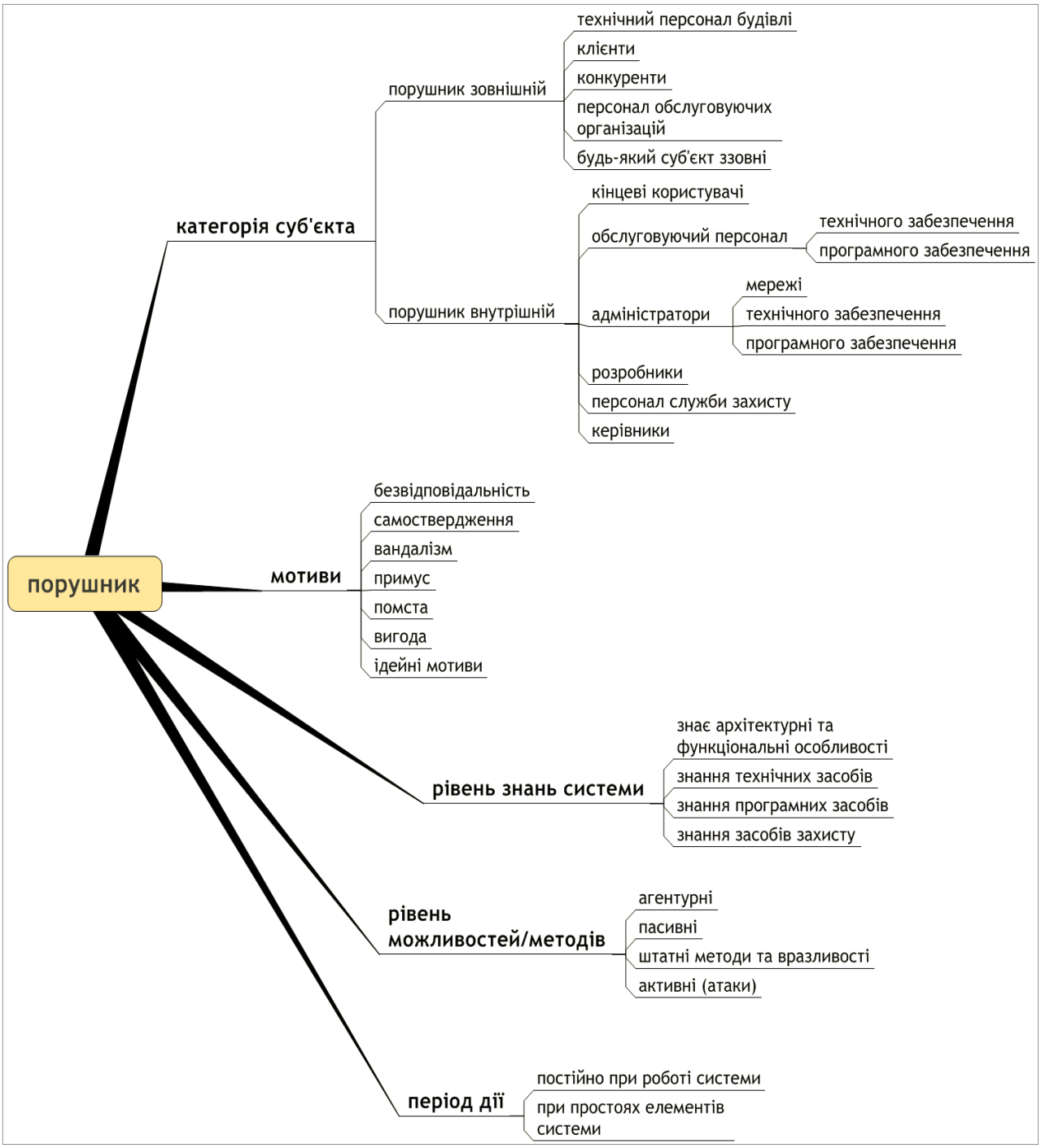

Рис. 1. Модель порушника

безпеки вже може виділяти слабкі місця організаційної структури, рівня обізнаності користувачів, мережевого обладнання, технічного забезпечення, програмного забезпечення. При виконанні завдання 4 визначені слабкі місця необхідно згрупувати у перелік вразливостей та співвіднести їх з кожним інформаційним ресурсом.

5. Ідентифікувати загрози по кожному ІР.

Виходячи з профілю ІР, ролей суб'єктів АПР, технічних засобів, необхідно визначити вразливості та загрози за правилом *вразливість - > загроза - >наслідок*.

Залежність величини ризику від рівня небезпеки вразливості, загрози та можливого наслідку можна переглянути на рис. 2 [8].

Наприклад:

Вразливість – відсутність внутрішнього документа «Політика інформаційної безпеки організації», що веде до виникнення іншої вразливості – недбале керування паролем. Загроза – втрата пароля. Наслідок – розкриття доступу до конфіденційної інформації.

Слід зазначити, що декілька вразливостей можуть впливати на рівень декількох загроз, або рівень небезпеки однієї вразливості може залежати від рівня безпеки декількох інших вразливостей.

6. Визначити фактори впливу на величини ризику реалізації кожної загрози.

Задача передбачає визначення факторів впливу на рівень ризику реалізації певної загрози та представлення факторів у контексті апарата нечіткої логіки.

Приклад визначення вразливостей та наслідків, що впливають на рівень ризику втрати доступу до робочих файлів, показано на рис. 3. Таке представлення можна також назвати деревом подій, що ведуть до виникнення загрози втрати інформаційного ресурсу.

Приклад переліку лінгвістичних змінних (βі), що впливають на величину ризику реалізації загрози втрати пароля до приватного ключа:

β1 – рівень кваліфікації персоналу, Х – процент співробітників з досвідом більше 5 років;

β2 – рівень ймовірності реалізації загрози, Х – ймовірність (або кількість інцидентів за останні 5 років) – може складатися з ймовірностей реалізації декількох подій;

β3 – рівень ймовірності реалізації найгіршого сценарію, Х – ймовірність (або – кількість інцидентів за останні 5 років);

β4 – рівень вартості контрзаходів, Х – вартість;

β5 – рівень критичності ресурсу, Х – можливий час роботи системи без ресурсу;

β6 – рівень втрати репутації, доступності, конфіденційності, цілісності;

β7 – час дії загрози, Х – шкала часу;

β8 – рівень наслідків дії загрози у вартісному представленні;

β9 – наявність та якість політики інформаційної безпеки організації.

Приклад представлення атрибутів лінгвістичної змінної, що описує рівень кваліфікації персоналу:

β1– рівень кваліфікації персоналу – лінгвістична змінна,

Х – універсальна множина – процент співробітників з досвідом більше 5 років,

Т – терми (значення лінгвістичної змінної): персонал досить кваліфікований, середньо, слабо кваліфікований,

α − нечітка змінна – <найменування нечіткої змінної> – персонал досить кваліфікований, область визначення – від 0 до 100 %, нечітка множина по даній змінній – від 70 % до 100 %.

Приклад представлення нечіткої множини по кваліфікації персоналу:

$S=\{x \mid x \in X \ \& \ M(x)>0\}$ [6], X – процент співробітників з досвідом роботи більше 5 років, x – значення кількості кваліфікованого персоналу в %, що описують нечітку змінну «персонал досить кваліфікований», $M(x)$ – ступінь належності x до нечіткого визначення «персонал досить кваліфікований».

У такий спосіб можна описати й інші вразливості.

Наприклад, розглянемо вразливість, що стосується низької якості політики інформаційної безпеки. Універсальна множина – рівень якості документа, що описує політику інформаційної безпеки, приймає значення на числовій множині від 0 до 10. Приклад термів: документ політики відсутній (нечітка множина від 0 до 2), документ є в наявності, але не досконалий (нечітка множина від 3 до 4),

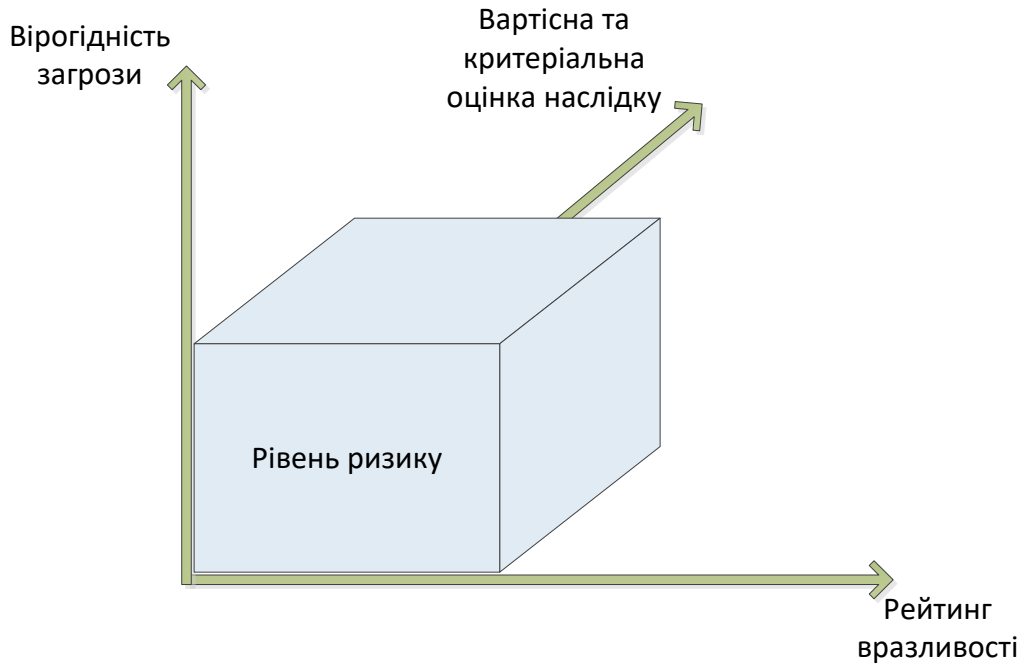

Рис. 2. Функція рівня ризику

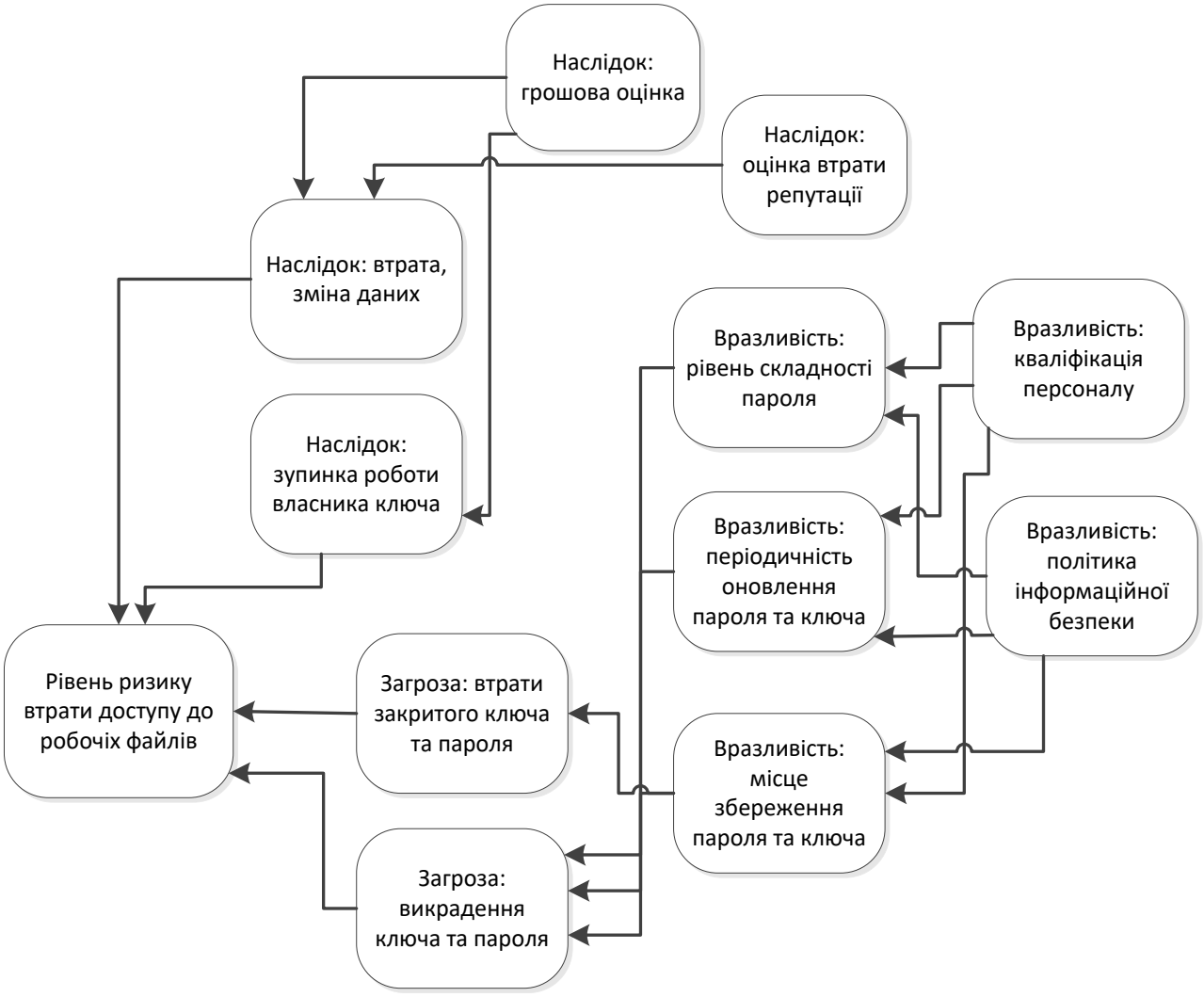

Рис. 3. Чинники виникнення ризику втрати доступу

документ досконалий, але не оновлюється (нечітка множина від 5 до 8), документ повний та оновлюється щороку (нечітка множина від 9 до 10).

7. Визначити рівень ризику по кожній загрозі.

Задача передбачає визначення бази нечітких правил, на вході яких йдуть умови впливу на рівень ризику (вразливості, загрози, наслідки), на виході – значення лінгвістичної змінної рівня ризику із заданої множини нечітких змінних.

Визначення рівня ризику втрати закритого ключа доступу до хмарного сервера показано рис. 4–6 (для даного прикладу використано інструменти MATLAB).

Обрані фактори впливу: вартість контрзаходів, кількість інцидентів минулого періоду, рівень кваліфікації персоналу.

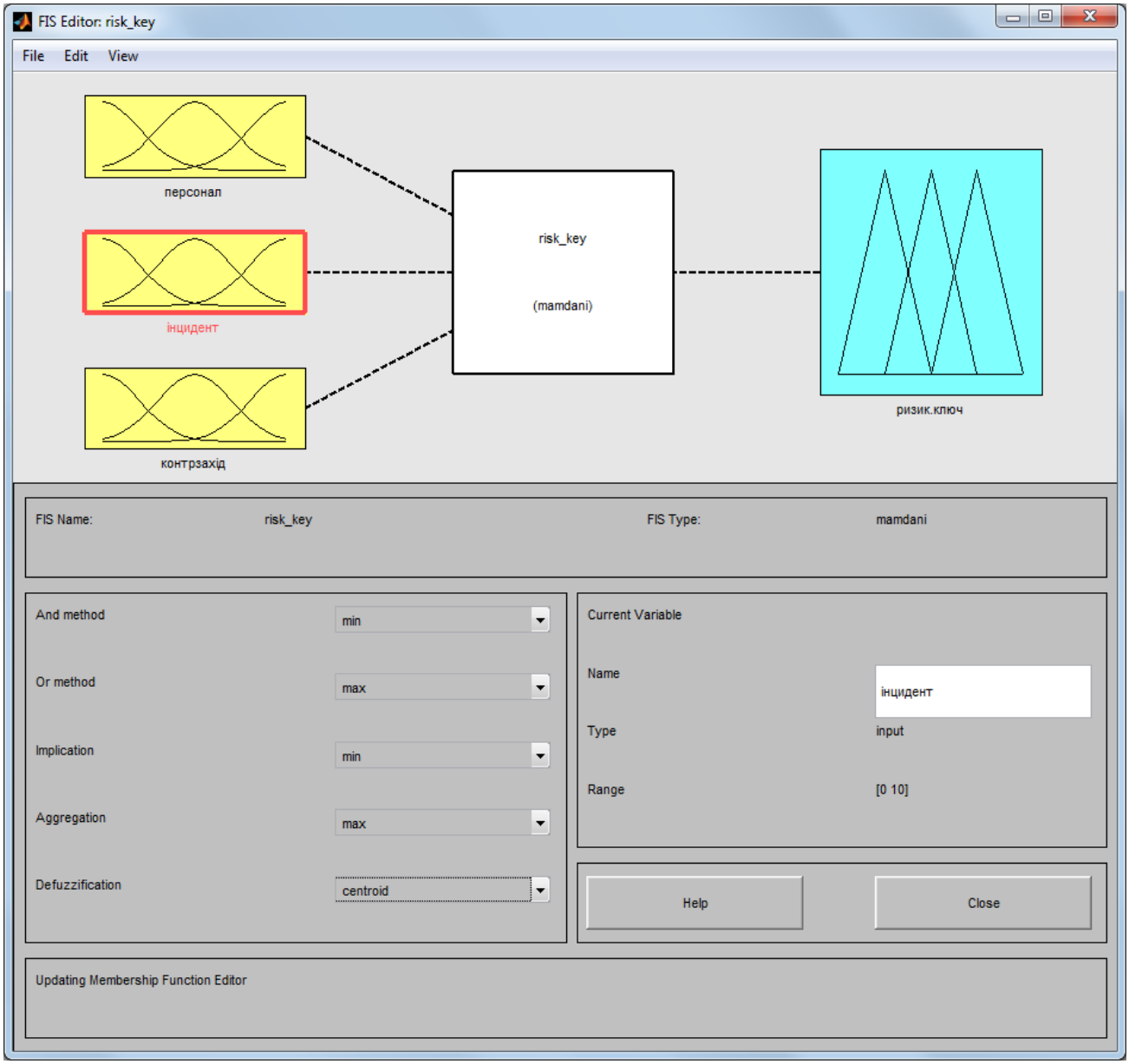

Рис. 4. Параметри вводу даних та виводу оцінки ризику втрати закритого ключа

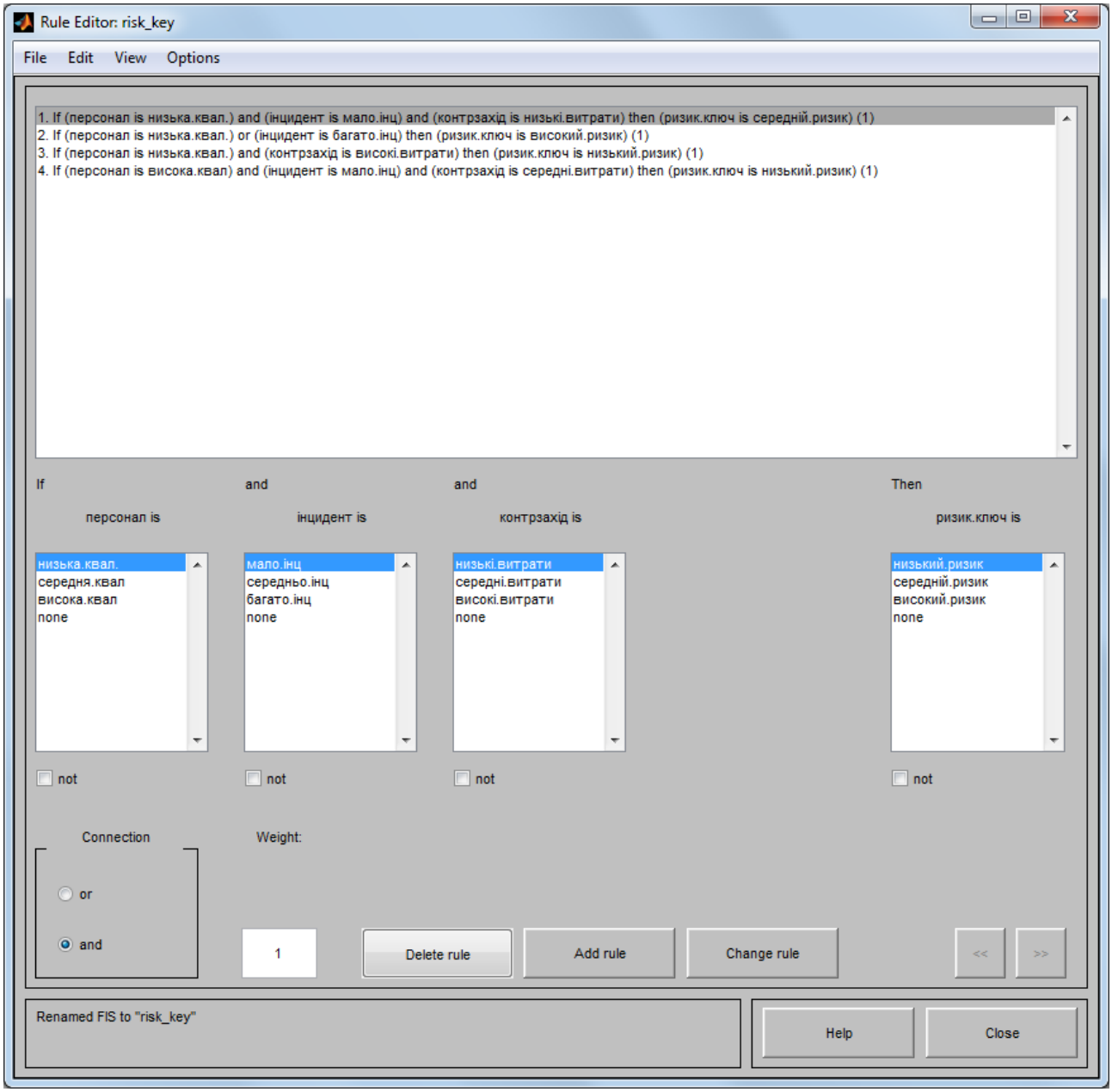

Рис. 5. Формування нечітких правил

8. Розподілити річний бюджет витрат на ІБ та пріоритетність дій плану впровадження політики ІБ.

У даному випадку статті бюджету можуть бути представленими за двома категоріями:

а) як резерв витрат на ліквідацію наслідків реалізації загрози;

б) як витрати на технічні засоби, програмні засоби, організаційні заходи, навчальні програми за напрямками ліквідації або мінімізації вразливостей та відповідних загроз.

Представимо бюджет:

$$B = \sum_{i=1}^{n} Bi,$$

B – загальний бюджет, Bi – стаття бюджету, що відповідає вразливості, загрозі,

$$Bi = B * \frac{Wi}{\sum_{i=1}^{n} Wi},$$

Wi – рівень ризику, пріоритет статті витрат на ІБ.

При розрахунку необхідно враховувати базову вартість статті, у випадку повного фінансування статті із залишком – решту слід переформувати на інші статті.

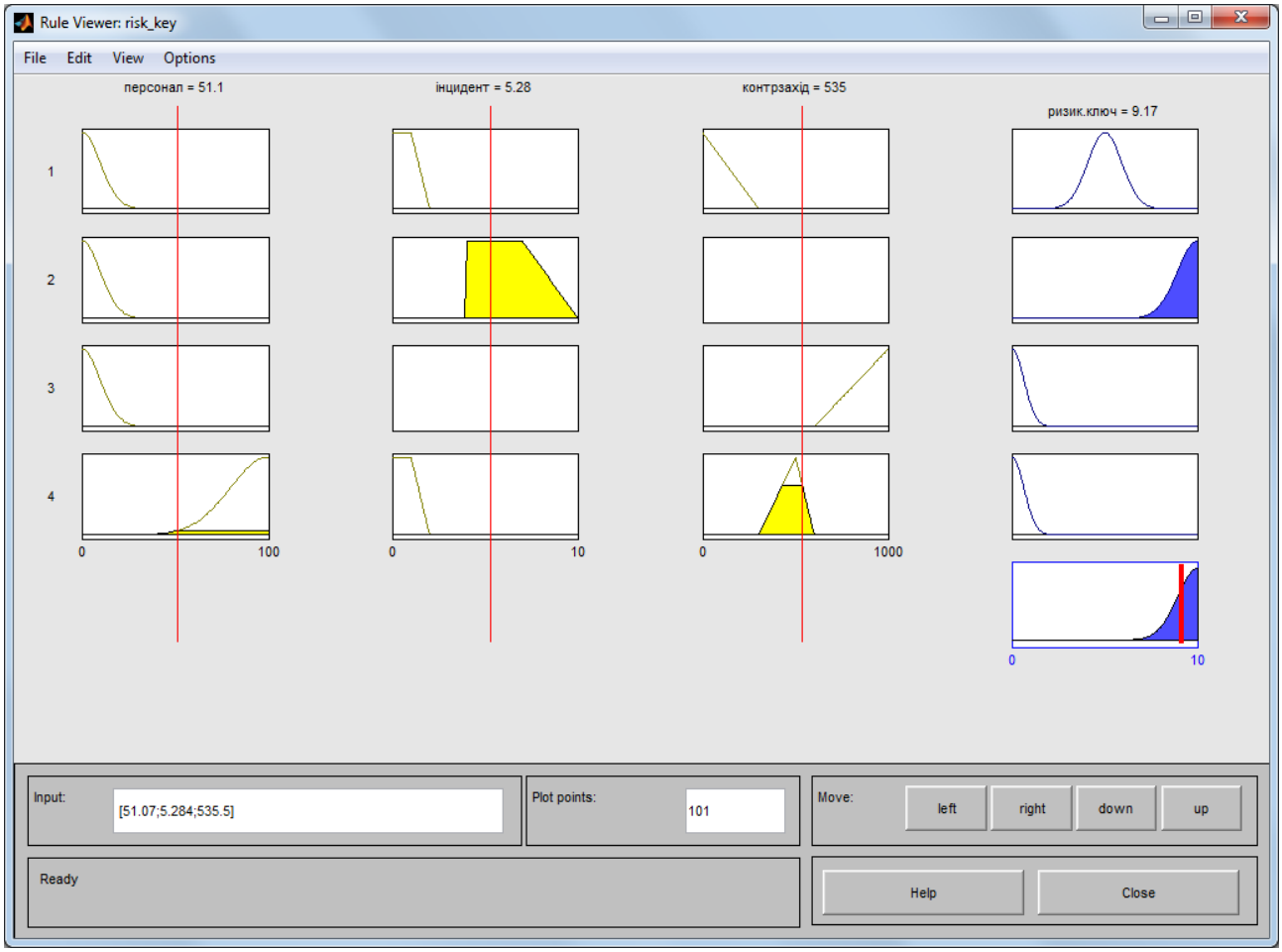

Рис. 6. Графічне зображення функцій належності та дефазифікація висновку

Висновки

Розв'язання запропонованих задач керування ризиком інформаційної безпеки передбачає використання комбінації процесних, експертних та математичних підходів. Задачі аналізу середовища, визначення вразливостей та загроз не потребують високої технічної кваліфікації. Виконання задач 1–3 дозволить майже паралельно створити документ політики інформаційної безпеки. Складнішим буде визначити дерево подій, що є наслідком, а що – причиною. Для збирання цієї інформації та подальшої побудови бази нечітких знань необхідно заохочувати експертів технічних відділів та аналізувати минулі періоди подій інформаційної безпеки. Апарат нечіткої логіки дозволяє перетворити будь-які зв'язки *причина* (*декілька причин*) – *наслідок* (*декілька наслідків*) у зручну математичну модель. Важливим питанням при використанні апарата нечіткої логіки є побудова функції належності. Правильно побудовану модель можна в майбутній життєдіяльності організації вдосконалювати та розширювати можливості її навчання.

1. International standard BS ISO/IEC 27005:2008, 2008-06-15.
2. Загородній А.Г., Боровська О.М., Свістунов С.Я., Сініцин І.П., Родін Є.С. Створення комплексної системи захисту інформаційних ресурсів у національній грід-інфраструктурі України. К.: Сталь, 2014. 373 с.
3. Родін Є.С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки. *Математичні машини і системи*. 2012. № 4. С. 142–148.
4. 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.

5. 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.).
6. Zadeh L.A. The concept of linguistic variable and its application to approximate reasoning. *Information sciences*. 1975. N 8. P. 199–249.
7. Малышев, Л.С. Берштейн, А.В. Боженюк. Нечеткие модели для экспертных систем в САПР. М.: Энергоатомиздат, 1991. 136 с.
8. Integrated Site Security for Grids. https://isseg-training.web.cern.ch/ISSeG-training/

References

1. International standard BS ISO/IEC 27005:2008, 2008-06-15.
2. Borovska, O., Sinitsyn, I., Svistunov, S., Rodin, Y. and Zagorodniy, A. (2014). Development of information resources security system in the national grid infrastructure of Ukraine. Kyiv: Stal, p.373. (In Ukrainian)
3. Rodin, Y. (2012). Processing approaches in the field of information security risk management modeling. Mathematical machines and systems, 4, P. 142-148. (In Ukrainian)
4. Borovska, O., Sinitsyn, I., and Rodin, Y. Comparing national and worldwide approaches in developing grid information security system. Programming Problems, 5, P. 99-109. (In Ukrainian)
5. Borovska, O., Sinitsyn, I., Svistunov, S., Rodin, Y. and Shilin, V. (2010). Approaches in developing information security system in the national grid infrastructure. Kyiv: Bogolyubov Institute for Theoretical Physics, p. 51. (In Ukrainian)
6. Zadeh, L. (1975). The concept of linguistic variable and its application to approximate reasoning. Information sciences, 8, pp. 199–249.
7. Bershtein, L., Bozhenyuk, A, Malyshev, L. (1991). Fuzzy modeling for experts systems in SAPR. Moscow: Energoatomizdat, p. 136. (In Russian)
8. Integrated Site Security for Grids. https://isseg-training.web.cern.ch/ISSeG-training/

Одержано 27.06.2017

Про автора:

Родін Євген Сергійович,
молодший науковий співробітник.
Кількість наукових публікацій в українських виданнях – 5.
http://orcid.org/0000-0003-2416-8572.

Місце роботи автора:

Інститут програмних систем
НАН України,
м. Київ, 03187,
проспект Академіка Глушкова, 40, корп.5.
Тел.: 044 526 5507.
E-mail: yevheniy.s.rodin@gmail.com.