МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 338.242+004.056
DOI: https://doi.org/10.32782/2224-6282/177-13

Огліх В. В.
кандидат фізико-математичних наук, доцент,
Дніпровський національний університет імені Олеся Гончара
ORCID: https://orcid.org/0000-0003-3193-7931
Патока Г. В.
Дніпровський національний університет імені Олеся Гончара

Oglih Valentina, Patoka Hanna
Oles Honchar Dnipro National University

МОДЕЛЮВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ НЕВИЗНАЧЕНОСТІ ВПЛИВУ ДЕСТАБІЛІЗАЦІЙНИХ ФАКТОРІВ НА ОСНОВІ НЕЙРОНЕЧІТКИХ МЕРЕЖ

Найважливішим результатом формування інформаційного суспільства XXI століття стало виникнення глобального інформаційного простору, в якому розгорнулася гостра боротьба за досягнення інформаційної переваги. Внаслідок цього в сучасному суспільстві інформаційна безпека є найважливішим компонентом національної, регіональної та міжнародної безпеки. Система забезпечення інформаційної безпеки повинна бути націлена на забезпечення інформаційної безпеки як властивості і як стану, а також на створення безпечних умов для використання інформаційного ресурсу як виду діяльності. Концептуальні і науково-методологічні основи інформаційної безпеки ще перебувають у процесі дослідження, проте вже існує необхідність розробки моделей інформаційної безпеки та захисту інформаційних систем, які б дали можливість оцінити ризик виходу системи з ладу та зменшити ймовірність загроз.

Ключові слова: *інформація, безпека, невизначеність, нейронечіткі мережі, ризик.*

FORMATION OF INFORMATION SECURITY SYSTEM UNDER CONDITIONS OF UNCERTAINTY OF INFLUENCE OF DESTABILIZATION FACTORS ON THE BASIS OF NEUROFACLE NETWORKS

The most important result of the formation of the information society of the XXI century was the emergence of a global information space, which unfolded a fierce struggle for information excellence. As a result, in modern society, information security is a critical component of national, regional and international security. The information security system should be aimed at ensuring information security as a property and as a state, as well as to create secure conditions for the use of information resources as an activity. Information is increasingly being used as a threat to competitors, information systems, software. Conceptual and scientific-methodological foundations of information security are still in the process of development and research. However, there are already models of information security and protection of information systems that try to answer the question: how to reduce the risk of system failure, what types of attacks can be eliminated, what types of threats exist. That is why the development of an economically determined risk assessment model for the information security system of the enterprise is an important aspect for the organization of the enterprise. Imbalances and failures in the information system can cause significant economic damage. That is why the creation of an ideal system that is certainly able to withstand the full set of threats requires significant costs, so the formation of an economically viable system to minimize information security risks at the level of the business entity is extremely important. At the enterprise level, the first step towards the formation of information security should be the development of a conceptual scheme, the overall structure of the information security model, which should be based on other models related to the protection of tangible and intangible assets and reduce the likelihood of information. At the organizational and managerial level, after a deep analysis under the guidance of a person directly responsible for the information security of the organization, coordinating and controlling it, aware of business goals, risks and threats, taking into account the opinions of experts, mathematical and functional models are formed, the organizational and corporate component of security is determined information system. Accordingly, the information security of an organization can be defined as the protection of information and supporting infrastructure from accidental or intentional impacts, natural or artificial, that could cause unacceptable damage.

Keywords: *information, security, uncertainty, neural networks, risk.*

JEL Classification: *C02, C61, D 29, D70, D89*

Постановка проблеми. Діджиталізація сучасного суспільства, масовий перехід в online, спровокований пандемією COVID-19, постійний розвиток інформаційних технологій, удосконалення комп'ютерних систем зберігання й обробки інформації ставлять економічні суб'єкти перед необхідністю вирішення комплексного завдання. З одного боку, суб'єкти повинні протистояти впливу внутрішніх та зовнішніх інформаційних загроз, які дестабілізують систему, а з іншого, не допустити створення інформаційних загроз для елементів зовнішнього середовища. В умовах збільшення кількості випадків хакерських атак, поширення комп'ютерних вірусів та комп'ютерного піратства слід кардинально підвищити рівень захисту інформації. Розбалансування і збої в інформаційній системі здатні завдати істотного економічного збитку. Однак створення ідеальної системи, безумовно здатної протистояти повному набору загроз вимагає істотних витрат, тому формування економічно виправданої системи оцінки ризиків інформаційної безпеки в умовах впливу дестабілізаційних факторів на рівні суб'єкта господарювання є вкрай важливим. Водночас, інноваційність інформаційної сфери, зростання складності архітектури зберігання даних, стрімке вдосконалення комп'ютерних технологій, недостатність теоретичної бази та наукових напрацювань в інформаційній царині роблять тему даного дослідження актуальною з практичної й теоретичної точок зору.

Аналіз останніх досліджень і публікацій. Проблемі захисту інформаційного простору, інформаційній безпеці надано увагу багатьох науковців. Проблемні питання забезпечення кібернетичної безпеки досліджували Ю. Даник [1], Р. Грищук [1], А. Дудатьєв [2], О. Войтович [2], Т. Булдакова [3], В. Пилипчук [4] та інші науковці. Однак у працях вищезазначених фахівців інформаційна безпека досліджувалась, радше, як складова національної безпеки, її невіддільна компонента. Поза увагою науковців залишились проблеми чіткого окреслення інформаційних загроз, вивчення їхніх джерел, визначення та обґрунтування методів протидії інформаційним атакам. Зважаючи на вищевикладені малодосліджені аспекти проблеми інформаційної безпеки, метою статті є формування економічно виправданої системи мінімізації ризиків інформаційної безпеки на рівні суб'єкта господарювання, захисту інформаційного простору суб'єкта з огляду на реальні й потенційні загрози виходу системи захисту інформації з ладу [5, с. 35].

Мета статті полягає в формування концептуальної та економічно-математичної моделі інформаційної безпеки на рівні підприємства за умови впливу дестабілізуючих факторів, які впливають на систему, в умовах невизначеності.

Виклад основного матеріалу. На рівні підприємства першим кроком на шляху формування інформаційної безпеки має стати розробка концептуальної схеми, тобто загальної структури моделі інформаційної безпеки, на якій як на стрижні мають будуватися інші моделі пов'язані з захистом матеріальних і нематеріальних цінностей і зниженням ймовірності різноманітних руйнувань до мінімуму, гарантуванням точності й цілісності інформації.

Маємо розуміти, що забезпечення реалізації надійного захисту має перейти від разових заходів до постійної системи процедур, які здійснюються на всіх рівнях керування та поєднує управлінські, організаційні, економічні, технічні рішення [6, с. 105]. Сформована концептуальна модель інформаційної безпеки системи має поєднувати в єдине ціле бізнес-цілі, аналіз ризиків та загроз, стан та надійність наявної системи, економічно, математично та функціонально обґрунтовані технічні та організаційні заходи.

На організаційно-управлінському рівні, після глибокого аналізу під керівництвом особи, яка безпосередньо відповідає за інформаційну безпеку організації, координує та контролює її, усвідомлює бізнес-цілі, ризики та загрози, враховуючи думки експертів формуються математична та функціональна моделі, визначається організаційна та корпоративна складова безпеки інформаційної системи [6, с.106].

Задля забезпечення надійного захисту інформаційних підсистем, конкретних сервісів або груп сервісів приймаються рішення стосовно:

– архітектури інформаційної системи;

– механізмів, засобів та методів захисту;

– технічних засобів, які мають бути включені в систему;

– обладнання, яке доцільно закупити та встановити;

– повсякденного адміністрування;

– моніторингу системи інформаційної безпеки в цілому, відстеження та стану слабких місць та дій персоналу;

– первинного та поточного навчання колективу тощо [7, с. 403].

Вкрай важливо розуміти схему оцінки критичності як самого сервісу, так і даних, які з його допомогою будуть оброблятися, знати потенційні наслідки технічних збоїв, хакерських та вірусних атак, порушення конфіденційності, цілісності та доступності інформації.

Базуючись на системному підході, інформаційну безпеку підприємства пропонується розглядати як комплекс (систему), який складається з окремих рівнів (організаційно-управлінський та сервісний рівень) та блоків (підсистем): ресурсів; наявної інформації; витрат на уникнення чи усунення загроз; системи заходів; результатів досягнених цілей (рис. 1).

Блок ресурсів – це сукупність усіх ресурсів, які використовуються у господарському процесі підприємства. Ресурси підприємства, які характеризують його інформаційну безпеку наявні у вигляді:

– обслуговуючого персоналу для підтримання роботи системи різних рівнів кваліфікації та оплати праці (програмістів серверної, програмної частин ПК, інженерів апаратної частини ПК, менеджерів з роботи персоналу, адміністраторів системи);

– фонду оплати праці працівників;

– наявного програмного, апаратного забезпечення.

Наступний блок охоплює саму інформацію як центральну частину системи захисту підприємства. Мають бути визначені: джерела інформації, пріоритети або ступінь важливості інформації, джерела та цілі загроз, самі загрози, способи доступу, напрямки, методи та засоби захисту.

Третій блок охоплює наявні витрати на:

– підтримку системи у захищеному від загрози стані (вимкнення, припинення роботи, виходу з ладу);

– уникнення загроз (зв'язаних з ризиком її настання);

– полагодження системи.

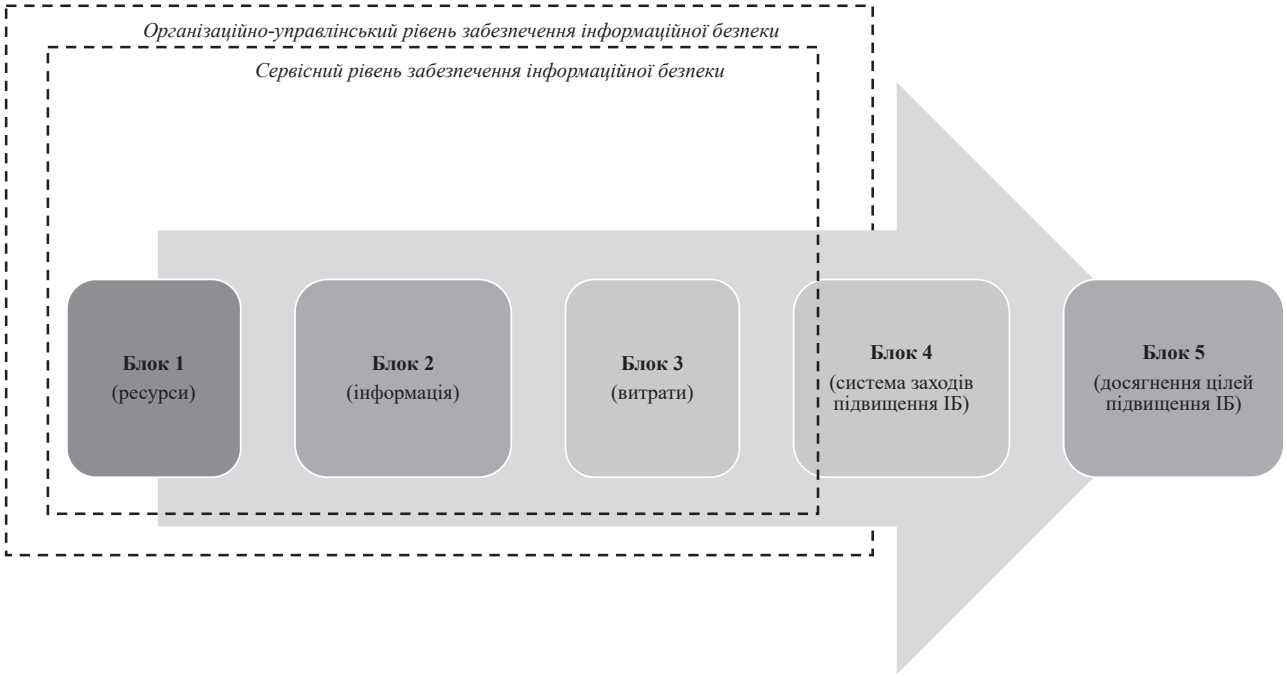

Рис. 1. Комплексна модель системи інформаційної безпеки підприємства.

Джерело: запропоновано автором

Четвертий блок містить систему заходів, спрямованих на забезпечення оптимального (ефективного) поєднання ресурсів та наявних можливостей з приводу підвищення ефективності їх використання. Дані заходи спрямовані на виявлення, запобігання, нейтралізацію, припинення, локалізацію, відображення небезпек і загроз, а у випадку необхідності – відшкодування збитків, відтворення об'єктів захисту, що постраждали внаслідок протиправних дій, халатності, форс-мажорних обставин тощо.

П'ятий блок – результативний – містить перелік основних складових, які становлять суть інформаційної безпеки підприємства. Ефективне забезпечення інформаційної безпеки підприємства має бути спрямовано на досягнення таких цілей:

– стабільність функціонування системи;

– виявлення можливих атак;

– зниження ризику припинення роботи системи;

– зменшення витрат на уникнення загрози та полагодження системи,

– підвищення кваліфікації персоналу, який обслуговує систему;

– зменшення часу, потрібного на усунення загрози.

Узагальнюючи вище наведене, запропоновано концептуальну модель інформаційної безпеки підприємства, яка відбиває її бачення як комплексної системи, що являє сукупність окремих блоків, поєднання яких дозволяє досягти визначених цілей досягнення ефективності системи (рис. 2).

Реалізація запропонованої концепції інформаційної безпеки підприємства можлива лише за наявності оптимальних взаємопов'язаних економіко-математичної та функціональної моделі інформаційної безпеки, базуючись на обраних методах оцінки факторів ризику.

Однією з особливостей роботи є вибір методу моделювання системи інформаційної безпеки за умови невизначеності впливу дестабілізаційних факторів на основі нейронечітких мереж. Згідно концептуальної моделі інформаційної безпеки виявлено, що ризик інформаційної безпеки – це комплексне поняття, яке складається із значної кількості впливаючих дестабілізаційних факторів, основними з яких на етапі аналізу підприємства обрано:

– загрози інформаційної безпеки (програмні або людські злодіяння, які можуть призвести до руйнування чи втрати працездатності системи інформаційної безпеки);

– потенційно можливі збитки (фінансові втрати підприємства на полагодження системи інформаційної безпеки вразі її руйнування чи втрати працездатності);

– вразливість інформаційної системи (вразливі (непокриті концептуальною моделлю) місця інформаційної системи).

Методи, що вирішують завдання оцінки факторів системи, що дестабілізаційно впливають на систему інформаційної безпеки, можна розділити на кількісні та якісні (з числовою та лінгвістичною шкалою виміру цих факторів відповідно). Для кожного виду цих методів існують свої переваги та недоліки. Звести недоліки до мінімуму спільне використання числових коефіцієнтів разом з лінгвістичними. Тому саме такі змішані методи слід використовувати для оцінки ризику інформаційної системи на основі наявних дестабілізаційних факторів та експертної оцінки [8, с. 6].

Задача моделювання системи інформаційної безпеки в умовах невизначеності впливу дестабілізаційних факторів на основі нейронечітких мереж полягає у кількісному визначенні значення ризику підприємства за допомогою нечіткої логіки за наявних факторів ризику, значення яких на вході подані у лінгвістичній терм-множині.

Для моделювання ризику інформаційної безпеки підприємства, нечіткі моделі доцільно представляти у

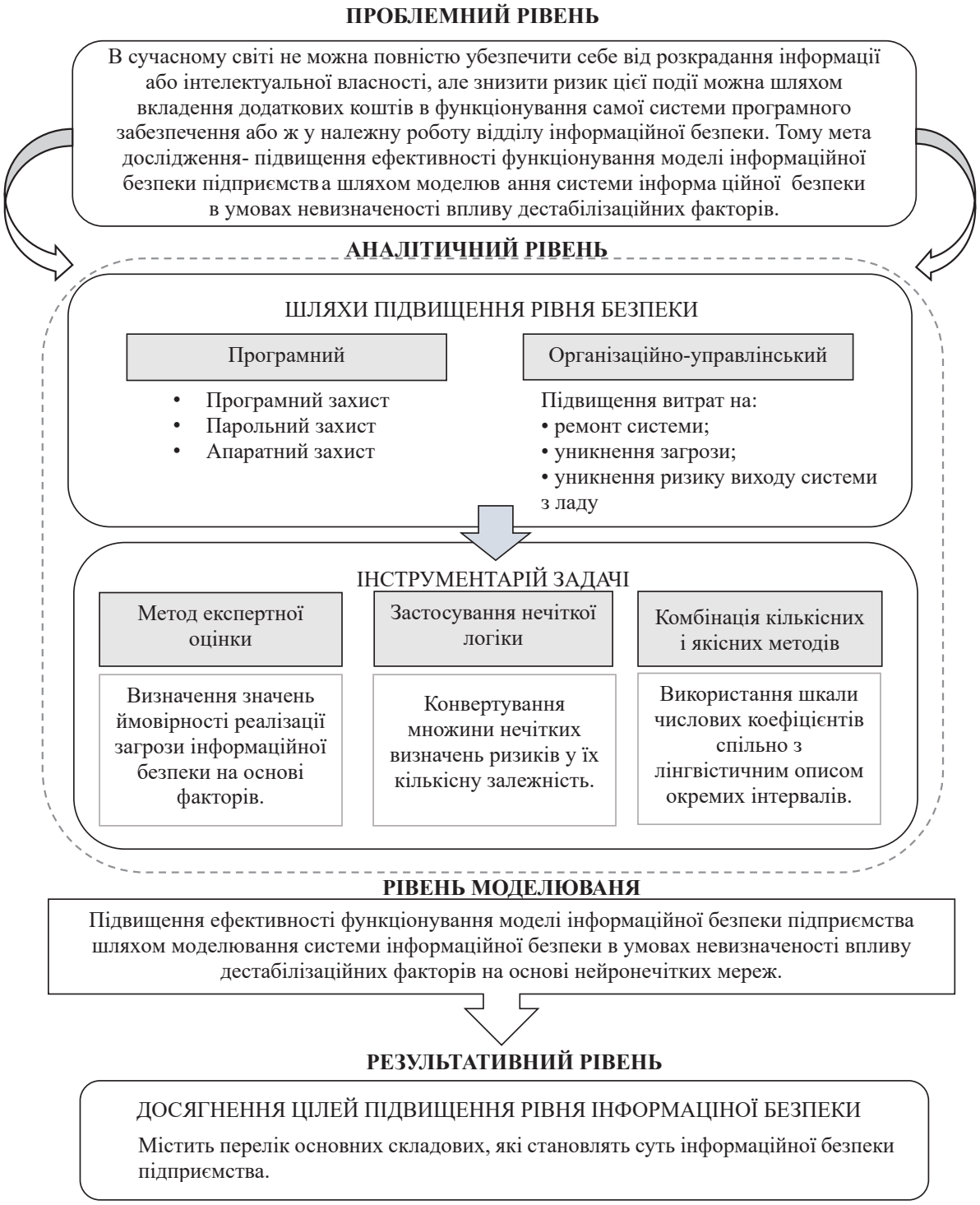

Рис. 2. Концептуальна модель інформаційної безпеки підприємства

Джерело: запропоновано автором

вигляді нечітких мереж, елементи та сукупності елементів яких реалізують різні компоненти нечітких моделей та етапи нечіткого висновку.

Для розв'язання цієї задачі були виконані такі кроки:

Крок 1.

Виявлені показники (x_i , i = 1,…,N):, які можуть бути факторами ризику інформаційної безпеки підприємства:

– загрози інформаційній безпеці (x_1);

– потенційно можливі збитки (x_2);

– вразливість інформаційної системи (x_3).

У свою чергу, кожен з факторів інформаційного ризику включає кілька складових: природні загрози (x_{11}); загрози через людський фактор (x_{12}); збитки через втрату конфіденційності (x_{21}); збитки через втрату цілісності системи (x_{22}); технічні вразливості (x_{31}); системні вразливості (x_{32}); вразливості управління системою (x_{33}).

Крок 2.

Формування експертної бази для оцінки A_i, $i = 1,\ldots,N$ потужності загрози x_1, величини збитків x_2 та ступеня вразливості x_3 в інтервалі

$$A_i \in [0,5] \quad (1)$$

Крок 3.

Формування правила, згідно якого група цих факторів x_1, x_2, x_3, визначають ймовірність I_i, $i = 1,\ldots,N$ настання несприятливої події.

$$0 < I_i, < 1 \quad (2)$$

Складність визначення ступеню потужності A_i, $i = 1,\ldots,N$ загрози x_1, величини збитків x_2 та ступеня вразливості x_3 полягає у тому, що оцінити їх можна лише за допомогою суб'єктивної експертної оцінки. Особливо це стосується оцінки можливих збитків. При оцінці інших факторів як допоміжної інформації експерти можуть використовувати результати аналізу потоків даних в інформаційній системі та накопичені статистичні дані про загрози, вразливості та ефективності існуючих заходів безпеки.

Для того, щоб мати впевненість у адекватності експертної оцінки факторів інформаційної безпеки, було виконано наступний крок:

Крок 4.

Обрано використати коефіцієнт конкордації (W) для виявлення міри узгодженості думок експертів:

$$W = \frac{12S}{n^2 * (m^3 - m)}, \quad (3)$$

де S – сума квадратів відхилень сум оцінок, наданих усіма експертами на від середнього арифметичного сум оцінок, n – число експертів, m – число факторів.

$$W \in [0,1] \quad (4)$$

Чим ближче значення коефіцієнта до одиниці, тим вищий рівень узгодженості оцінок експертів. При узгодженому результаті $W > 0{,}4$.

Крок 5.

Було визначено, що ризик інформаційної безпеки (R) є вихідної величиною у задачі моделювання системи інформаційної безпеки в умовах невизначеності впливу дестабілізаційних факторів та є комплексною величиною, що визначається як функція факторів x_i, $i = 1,\ldots,N$. Таким чином, ризик інформаційної безпеки можна представити у вигляді наступної функції:

$$R = f(x_1, x_2, x_3) \quad (5)$$

Згідно першого кроку, ризик інформаційної безпеки, враховуючи складові факторів ризику x_{ij}, можна представити у вигляді наступної функції:

$$R = f([x_{11}, x_{12} \ldots x_{1j}], [x_{21}, x_{22} \ldots x_{2j}], [x_{31}, x_{32} \ldots x_{3j}]) \quad (6)$$

Крок 6.

Для характеристики вхідних і вихідних змінних були сформовані наступні терм-множини (Т), що визначають фактори (T_1) та показники (T_2) ризику:

$$T_1 = \{\text{Низький; Середній; Високий}\}; \quad (7)$$

$$T_2 = \{\text{Незначний; Низький; Середній; Високий; Критичний}\} \quad (8)$$

Крок 7.

Найчастіше функції приналежності будуються суб'єктивно за результатами опитування експертів, тому є у певному сенсі «наближеними», тобто не абсолютно адекватно відбивають явище чи об'єкт. Власне, із суб'єктивності випливає, що абсолютної адекватності не існує в принципі. Тому потрібно вибирати таку функцію, з якою можна було б якомога простіше вести розрахунки. Такими функціями є трапецієподібні функції та трикутноподібні функції.

Для розв'язання наявної задачі обрано трапецієподібну функцію приналежності, яка визначається трійкою чисел (a, b, c, d), і її значення в точці x обчислюється відповідно до виразу:

$$MF(x) = \begin{Bmatrix} 0, x \le a \\ \frac{x-a}{b-a}, a \le x \le b; \\ 1, b \le x \le c \\ \frac{d-x}{d-c}, c \le x \le d; \\ 0, d \le x \end{Bmatrix}, \quad (9)$$

де [a, d] – носій нечіткої множини, песимістична оцінка значень змінної;

[b, c] – ядро нечіткої множини, оптимістична оцінка значень змінної.

Крок 8.

Нечітке причинно-наслідкове відношення між вхідною та вихідною змінними задається у вигляді нечіткої продукції на основі правил.

Конвертування множини нечітких визначень ризиків у їх кількісну залежність, враховуючи експертні оцінки A_i, $i = 1,\ldots,N$ ймовірності несприятливої події I_i, $i = 1,\ldots,N$ вимагає розв'язання такої задачі математичного програмування, у якій необхідно визначити залежність вихідної лінгвістичної змінної (R) від вхідних значень змінних x_i, i = 1,…,N на основі нечіткої логіки, враховуючи те, що R є функцією від усіх складових факторів ризику x_{ij}:

$$R = f([x_{11}, x_{12} \ldots x_{1j}], [x_{21}, x_{22} \ldots x_{2j}], [x_{31}, x_{32} \ldots x_{3j}])$$

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \le r_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \le r_2 \\ \ldots \\ a_{n1}x_1 + a_{n2}x_2 + a_{n3}x_3 \le r_n \end{cases}, \quad (10)$$

$aij \in [0,1], ri \in [0,1], i \in 1,2 \ldots N, j \in 1,2,3$, a_{i1} – експертні оцінки потужності небезпеки; a_{i2} – експертні оцінки величини збитків; a_{i3} – експертні оцінки ступеня вразливості; r_i – оцінки ризику; n – кількість експертів.

Побудована система повністю задовольняє критеріям адекватності оцінки інформаційних ризиків за умови врахування якості вхідної інформації та надійності (ступеня довіри) джерелам інформації.

Висновки. Розглядаючи особливості інформаційної функції системи управління економічною безпекою підприємства, слід зазначити, що для організації відповідного рівня інформаційної безпеки на підприємстві має бути обрана відповідна модель економічної безпеки, згідно з якою мають бути враховані методи заподіяння шкоди елементам системи та системи в цілому, вибір яких ґрунтується на аналізі та оцінці наявних ризиків відмови інформаційної системи підприємства. Апробація запропонованого підходу, реалізація для конкретної фірми підтвердила його ефективність та позначила напрямки подальших досліджень та удосконалень.

Список використаних джерел

1. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки : монографія / за ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 536 с.
2. Дудатьєв А. В. Моделі інформаційної підтримки управління комплексною інформаційною безпекою. Радіоелектроніка, інформатика, управління. 2017. № 1. С. 107–114.
3. Булдакова Т. І., Міков Д. А. Оцінка інформаційних ризиків в автоматизованих системах за допомогою нейро-нечіткої моделі. Наука та освіта. 2013. №11. С. 295–310.
4. Пилипчук В.Г., Брижко В.М., Баранов О.А. та ін. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / за ред. Брижка В.М., Пилипчука В.Г. Київ : ТОВ «Видавничий дім «АртЕк», 2017. 226 с.
5. Бельфер Р.А., Калюжний Д.А., Тарасова Д.В. Анализ зависимости уровня риска информационной безопасности сетей связи от экспертных данных при расчетах с использованием модели нечетких множеств. Вопросы кибербезопасности. 2014. № 1(2). С. 33–39.
6. Миков Д.А. Основные этапы оценки информационных рисков и способы их реализации. Теоретические и прикладные аспекты современной науки. 2014. № 3. С. 103–106.
7. Компьютерная преступность и информационная безопасность / за ред. А.П. Леонова. Минск : АРИЛ, 2017. 452 с.
8. Атаманов А. Н. Модуль нечеткого вывода на основе нейронных сетей для динамического итеративного анализа рисков информационной безопасности. Безопасность информационных технологий. 2011. Т. 18. С. 7–9.

References:

1. Dany`k Yu.G., Gry`shhuk R.V. (2016) Osnovy` kibernety`chnoyi bezpeky`: monografiya [Fundamentals of Cyber Security]. Zhy`tomy`r: ZhNAEU.
2. Dudatiev A.V. (2017) Modeli informatsiinoi pidtrymky upravlinnia kompleksnoiu informatsiinoiu bezpekoiu [Models of information support for integrated information security management]. Radioelectronics, computer science, upravlinnia, no. 1, pp. 107–114.
3. Buldakova T.I., Mikov D.A. (2013) Otsenka informatsionnykh riskov v avtomatizirovannykh sistemakh s pomoshch'yu neyronetchyotkoy modeli [Assessment of information risks in automated systems using a neuro-fuzzy model]. Science and education, no. 11, pp. 295–310.
4. Pylypchuk V.H., Bryzhko V.M., Baranov O.A., Miller K.C. (2017) Stanovlennia i rozvytok pravovykh osnov ta systemy zakhystu personalnykh danykh v Ukraini [Formation and development of legal foundations and system of personal data protection in Ukraine]. Kyiv: ArtEk Publishing House LLC.
5. Belfer R.A., Kaliuzhnyi D.A., Tarasova D.V. (2014) Analyz zavysymosty urovnia ryska ynformatsyonnoi bezopasnosty setei sviazy ot ekspertnikh dannikh pry raschetakh s yspolzovanyem modely nechetkykh mnozhestv [Analysis of the dependence of the level of information security risk of communication networks on expert data when calculating using the fuzzy sets model]. Cybersecurity issues, no. 2, pp. 33–39.
6. Mikov D.A. (2014) Osnovni etapy otsinky informatsiinykh ryzykiv ta sposoby yikh realizatsii [The main stages of information risk assessment and how to implement them]. Theoretical and applied aspects of modern science, no. 3, pp. 103–106.
7. Leonov A.P. (ed.) (2017) Komp'yuternaya prestupnost' i informatsionnaya bezopasnost' [Computer crime and information security]. Minsk: ARIL.
8. Atamanov A.N. (2011) Modul' nechetkogo vyvoda na osnove neyronnykh setey dlya dinamicheskogo iterativnogo analiza riskov informatsionnoy bezopasnosti [Fuzzy inference module based on neural networks for dynamic iterative analysis of information security risks]. Information technology security, no. 1, pp.7–9.