УДК 004.42
DOI https://doi.org/10.15589/znp2025.2(500).38

DEVELOPMENT OF A DECISION SUPPORT SYSTEM IN DETERMINING INFORMATION SECURITY OF AN ACCOUNTING COMPANY BASED ON FUZZY LOGIC

РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ВИЗНАЧЕНІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БУХГАЛТЕРСЬКОЇ КОМПАНІЇ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Irina V. Fedosova
fedosova_i_v@pstu.edu
ORCID: 0000-0003-3923-8270
Lyudmila D. Kotykhova
kotykhova_l_d@pstu.edu
ORCID: 0009-0006-5008-622X
Olha I. Pronina
pronina_o_i@pstu.edu
ORCID: 0000-0001-7085-8027

І. В. Федосова,
канд. пед. наук, професор
Л. Д. Котихова,
асистент
О. І. Проніна,
канд. техн. наук, доцент

Pryazovskyi State Technical University, Dnipro
Приазовський державний технічний університет, м. Дніпро

Abstract. *The purpose* of the study is to increase the efficiency of determining information security in accounting companies. The article is devoted to the development of a decision support system in determining information security of an accounting company based on fuzzy logic. Currently, the threat to information security remains an urgent issue as never before. In particular, this concerns security in accounting companies. *Method.* To achieve the goal, existing research in this area and approaches to solving this problem were analyzed. The object, subject and methods of research were identified. After that, a mathematical model was developed, based on the fuzzy inference algorithm. Also, to verify the developed rules, the system was simulated in the MatlabFuzzy environment. *Results.* Using the developed model, a web-based decision support system in determining information security of an accounting company was created, based on the Mamdani algorithm. To evaluate the system's operation, an experimental study was conducted, during which it was noticed that the assessment of information security in this form takes much less time. Therefore, the development of a decision support system based on fuzzy logic is the optimal solution for this problem. *Scientific novelty.* The issue of using fuzzy logic models in determining the information security of an accounting company in the analyzed studies has not received enough attention. This work is notable for its scientific contribution, because it focuses on fuzzy logic as a tool for assessing the security of an accounting company. *Practical importance.* The system that was developed during the study allows analyzing an accounting company and determining the influence of all key parameters on the degree of confidence in information security, which in turn will allow improving the quality of information security in the company. And the fact that the system is implemented in a web-based form provides its advantages, because it provides the opportunity to work on any computer without additional software.
Key words: decision support system; information security; information security management system; cybersecurity; cyber threat; fuzzy logic.

Анотація. *Мета* дослідження полягає в підвищенні ефективності визначення інформаційної безпеки в бухгалтерській компаній. Стаття присвячена розробці системи підтримки прийняття рішень у визначені інформаційної безпеки бухгалтерської компанії на основі нечіткої логіки. Наразі загроза інформаційній безпеці залишається як ніколи актуальним питанням. Зокрема це стосується безпеки в бухгалтерських компаніях. *Методика.* Для досягнення мети було проаналізовано наявні дослідження в цій області та підходи до вирішення цього завдання. Було виділено об'єкт, предмет та методи дослідження. Після цього було розроблено математичну модель, в основі якої покладено алгоритм нечіткого виводу. Також для перевірки розроблених правил було змодельовано систему в середовищі MatlabFuzzy. *Результати.* На основі розробленої моделі була створена веборієнтована система підтримки прийняття рішень у визначені інформаційної безпеки бухгалтерської компанії,

в основі якої використано алгоритм Мамдані. Щоб оцінити роботу системи було проведено експериментальне дослідження, під час якого помічено, що оцінка інформаційної безпеки у такому вигляді займає набагато менше часу. А отже розробка системи підтримки прийняття рішень на основі нечіткої логіки є оптимальним рішенням для даної задачі. *Наукова новизна.* Питанню застосування моделей з нечіткою логікою при визначенні інформаційної безпеки бухгалтерської компанії в проаналізованих дослідженнях було приділено недостатньо уваги. Дана робота відзначається науковим внеском, адже акцентує увагу саме на нечіткій логіці, як інструменті оцінки безпеки бухгалтерської компанії. *Практична значимість.* Система, що її було розроблено під час дослідження, дозволяє проводити аналіз бухгалтерської компанії та визначати вплив всіх ключових параметрів на ступень впевненості в інформаційній безпеці, що в свою чергу дозволить підвищити якість інформаційної безпеки в компанії. А те, що систему реалізовано у веборієнтованому вигляді, надає свої переваги, адже вона надає можливість працювати на будь-якому комп'ютері без додаткового програмного забезпечення.
Ключові слова: система підтримки прийняття рішень; інформаційна безпека; система управління інформаційною безпекою; кібербезпека; кіберзагроза; нечітка логіка.

ПОСТАНОВКА ЗАДАЧІ

Бухгалтерські послуги вже давно є необхідною складовою успішного функціонування будь-якого підприємства [1]. Бухгалтерський облік та фінансова звітність вимагають великої уваги, точності та експертизи, і тому багато компаній обирають звертатися до фахівців, які надають бухгалтерські послуги.

З розвитком інформаційних технологій зростають і можливі загрози з боку зловмисників, бо бухгалтерія є головною частиною будь-якої компанії. Оскільки це не лише про гроші, а і про дозвіл на роботу, то інформаційна безпека бухгалтерської діяльності є надважливою задачею.

Кожна фізична та юридична особа має різного роду інформацію. У людини вона, як правило, в особистому смартфоні чи комп'ютері. Це листування в месенджерах, особисті фотографії і сторінки в соціальних мережах. Підприємство зберігає дані про бухгалтерію, клієнтські бази та особисті справи співробітників. Всім важливо, щоб конфіденційна інформація не поширилася, і нею не змогли оволодіти «непотрібні» люди.

Тобто, загроза інформаційної безпеки – це комплекс факторів та умов, які наражають інформацію на витік або розголошення.

Надійне зберігання даних – ось для чого потрібна інформаційна безпека. Усі заходи та роботи проводять з метою забезпечення збереження матеріалів компанії, держави чи фізичної особи.

Для перевірки якості інформаційної безпеки бухгалтерської компанії існує ряд оцінок відповідно до серії стандартів ISO27001. Згідно цих стандартів описуються можливі ризики в компанії та необхідні дії для системи управління інформаційною безпекою (СУІБ) – частини загальної системи корпоративного управління. Таким чином у бухгалтерській компанії після проходження оцінки буде оцінка процесів, технічних засобів та підготовленості чи наявності необхідних людей та їх компетенцій.

Стандарт ISO/IEC 27001:2022 [2] – це стандарт управління безпекою, що формулює рекомендації з управління безпекою та характеризує комплексні елементи контролю безпеки відповідно до посібника з дотримання рекомендацій ISO/IEC 27002. В основі цієї сертифікації лежить розробка та впровадження суворої програми забезпечення безпеки, яка включає розробку та впровадження системи управління інформаційною безпекою (ISMS), що визначає безперервний, цілісний і всеосяжний процес управління безпекою в компанії.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Для визначення актуальності поставленої проблематики та для виявлення оптимального метода вирішення задачі було проведено аналіз літературних джерел. Так в роботі [3] обґрунтовано, що несанкціоноване використання інформації, що формується у системі бухгалтерського обліку, може призвести до шкідливих наслідків, пов'язаних із втратою інформації, неправильним введенням даних та неправомірним використанням конфіденційної інформації. Тому питання захисту інформації, що формується в системі обліку, є вкрай актуальним, а забезпечення її безпеки є пріоритетом у багатьох компаніях.

В статті [4] описуються наслідки кібератак на підприємства, які обирають стаціонарне та хмарне програмне забезпечення. Обґрунтовано недоцільність використання хмарного програмного забезпечення для великого та середнього бізнесу в умовах гібридної війни.

Робота [5] присвячена аналізу структури та типів основних порушень у сфері кібербезпеки українських підприємств. Спираючись на результати всеукраїнського експертного опитування-анкетування бухгалтерів, була визначена важливість окремих категорій та структура ризиків забезпечення обліково-аналітичної діджиталізації. Розроблено адаптивну систему забезпечення кібербезпеки підприємства залученням експертної групи з інформаційної безпеки.

Метою статті [6] є вивчення електронних ризиків для інформаційних систем бухгалтерського обліку в лівійських банках, визначення електронних ризиків для інформаційної системи бухгалтерського обліку в банківському середовищі, дослідження

найважливіших причин, які призводять до виникнення цих ризиків, дослідження процедур, які запобігають виникненню цих ризиків, і дослідження ролі заходів захисту.

Стаття [7] присвячена загрозам інформаційні системи бухгалтерського обліку, які надходять із різних джерел. Якщо їх ігнорувати, вони можуть зруйнувати актуальність та надійність фінансової інформації, що призводить до неправильних рішень різних зацікавлених сторін.

Робота [8] присвячена проблемі зростаючої залежність як державних, так і приватних фірм від інформаційних технологій і мереж для їхніх систем управління фінансами, що підвищує їхню вразливість до кіберзагрози. Сьогодні внутрішній аудит знову стикається з необхідністю адаптації. В роботі розглядають критичні ризики, пов'язані з кібербезпекою, і це дослідження підкреслює, що кібербезпека стає все більш важливою для бухгалтерського обліку та державної політики.

Робота [9] розкриває складність інформаційних процесів в бухгалтерському обліку. Швидкі зміни в комп'ютерних і комунікаційних технологіях призводять до різноманітних кіберзагроз, яким піддається облікова інформація. Використання цієї класифікації кіберризиків, яка дає комплексну характеристику кіберзагроз для бухгалтерської інформації, є важливим для розробки заходів щодо запобігання, уникнення та усунення можливих наслідків.

Стаття [10] присвячена дослідженню обґрунтування використання технології Blockchain у сфері бухгалтерського обліку та аудиту. Аналіз ризиків показав, що впровадження Blockchain може допомогти зменшити ймовірність облікових помилок і забезпечити більш високий рівень інформації безпеки. Використання Blockchain в обліку транзакцій може призвести до зниження в штрафних санкціях, пов'язаних з обліковими помилками, а також сприяє швидшому виявленню та виправленню помилок без додаткових фінансових витрат.

Робота [11] присвячена надзвичайно важливій темі – організації безпеки інформації, оскільки загрози інцидентів інформаційної безпеки, які можуть вплинути на інформацію, продовжують зростати. Тривожні факти в літературі підтверджують поточну відсутність адекватних практик захисту інформації та спонукають до визначення додаткових методів, які допоможуть організаціям захистити свою конфіденційну та критичну інформацію.

Багато областей бухгалтерського обліку мають неоднозначність через невизначені та неточні терміни. Багато неясностей породжує людський розум. У сфері бухгалтерського обліку ці неоднозначності призводять до створення невизначеної інформації. Багато з цілей і концепцій бухгалтерського обліку з бінарною класифікацією не узгоджуються. Подібним чином в роботі [12] наведено обговорення суттєвості чи надійності бухгалтерського обліку, що не є двоскладовою концепцією, тому що існують ступені суттєвості чи надійності.

Ще одна робота присвячена нечіткій логіці в сфері бухгалтерського обліку. Метою статті [13] є показати впровадження нечіткої логіки в бізнес, адміністрування та бухгалтерський облік.

ВІДОКРЕМЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

На основі сучасних методів аналізу інформаційної безпеки бухгалтерських компаній можна ефективно вирішувати багато проблем у бухгалтерській галузі. Невирішеною частиною загальної проблеми є застосування моделей з нечіткою логікою для визначення інформаційної безпеки бухгалтерської компанії. Саме нечітка логіка, як інструмент оцінки безпеки бухгалтерської компанії дає якісний результат при прийнятті рішень.

МЕТА, МЕТОДИ, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Метою даної роботи є підвищення ефективності прийняття рішень визначення інформаційної безпеки бухгалтерської компаній за рахунок розробки моделі нечіткої логіки.

В роботі було використано наступні **методи**: аналіз літературних джерел, збір даних, розробка математичної моделі та її впровадження, розробка веборієнтованої системи підтримки прийняття рішень (СППР), проведення експериментального дослідження.

Об'єктом дослідження є інформаційна безпека бухгалтерської компанії.

Предметом дослідження є розробка СППР для визначення інформаційної безпеки бухгалтерської компанії.

ОСНОВНИЙ МАТЕРІАЛ

Для опису моделі інформаційної безпеки бухгалтерської компанії використовується нечітка модель розрахунку ступеня впевненості у інформаційній безпеці, представлена в наступному вигляді:

$$L = \left\langle \{\beta_1, \beta_2, \beta_3, \beta_4\}; \{R_1, R_2, ..., R_{180}\}; \{w_1\} \right\rangle, \qquad (1)$$

де $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ – набір чотирьох вхідних лінгвістичних змінних: ефективність комунікацій, складність паролів, ступінь навантаження, кваліфікація бухгалтера;

$\{R_1, R_2, ..., R_{180}\}$ – множина продукційних правил у кількості 180;

$\{w_1\}$ – вихідна лінгвістична змінна: ступінь впевненості в інформаційній безпеці.

По кожній змінній було проведено аналіз для виявлення оптимальної кількості термів та їх назв для зручності користувачів.

Лінгвістична змінна «Ефективність комунікації» характеризується трьома термами: «внутрішня

система комунікації» (internal), «змішана система комунікації» (mixed), «зовнішня система комунікації» (external).

Лінгвістична змінна «Ступень навантаження» характеризується чотирма термами: «високий відсоток відмовності» (hight), «середній відсоток відмовності» (average), «низький відсоток відмовності» (low), «безвідмовна» (trouble-free).

Лінгвістична змінна «Складність паролів» характеризується трьома термами: «короткий» (short), «середній» (medium), «довгий» (long).

Лінгвістична змінна «Кваліфікація бухгалтера» характеризується п'ятьма термами: «junior», «middle», «senior», «lead», «expert».

Після заповнення всіх вхідних змінних, визначення їх термів та функцій приналежності разом зі шкалою оцінювання кожної змінної описується вихідна змінна – «Ступінь впевненості в інформаційній безпеці». Вона описується трьома термами: «низька», «середня», «висока».

Для опису залежності кожного терму були вибрані емпіричним шляхом подібні функції приналежності: асиметрична сигмоїдна та узагальнений дзвін.

В основі розробленої математичної моделі покладено алгоритм нечіткого виводу, основні кроки якого наведено на рисунку 1 у вигляді діаграми станів.

Рис. 1. Діаграма діяльності процесу нечіткого виведення

Була змодельована система в середовищі MatlabFuzzy для перевірки розроблених правил. Моделювання дозволило перевірити якість продукційних правил, що лежать в основі системи та підтвердити в цілому адекватність розробленої моделі.

Для зручності всі вхідні змінні та терми були написані англійською мовою, як переклад з української. Загальна структура моделі та налаштування алгоритму нечіткого висновку наведено на рисунку 2.

На основі розробленої математичної моделі була створена веборієнтована система підтримки прийняття рішень у визначені інформаційної безпеки бухгалтерської компанії. В основі системи лежить алгоритм Мамдані. Веборієнтована система повністю повторює правила та налаштування термів кожної лінгвістичної змінної, що попередньо було змодельована в середовищі MatlabFuzzy. Система представлена на рисунку 3.

Для оцінки роботи розробленої системи було проведено експериментальне дослідження, для цього

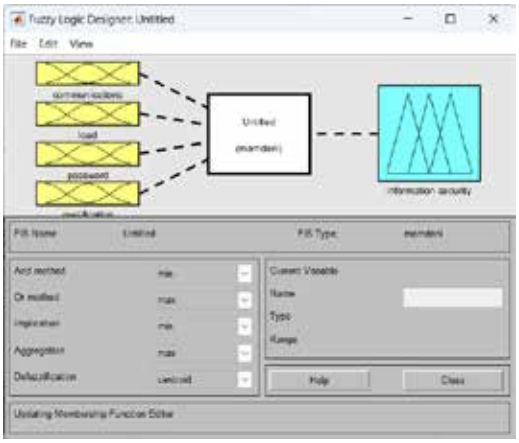

Рис. 2. Модель нечіткого виведення

Рис. 3. Результат розрахунку розробленої системи

обрано передбачувані дані по 15 ймовірних бухгалтерських компаніях. Серед тестування були всі можливі варіанти поєднання вхідних змінних.

При моделюванні експерименту були обрані різні варіанти співвідношення інформаційної безпеки, що дозволяє дослідити предметну область в цілому та оперувати більш достовірними даними.

В експерименті брали участь 2 користувачі, їх завданням було на основі наданих термів зробити свою оцінку ефективності інформаційної безпеки для кожної вказаної бухгалтерської компаній.

ОБГОВОРЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Під час проведення експерименту було помічено, що швидкість відповідей кожного користувача відносно вхідних даних є різною, тобто оцінка інформаційної безпеки у такому вигляді, як вона розроблена, займає набагато менше часу в цілому, оскільки користувачі все ж таки мають свій темп роботи. Тож система є більш швидкою.

Користувачі під час аналізу не бачили результати один одного та результати системи, при цьому в числовому варіанті вони не збігаються, проте в лінгвістичному варіанті збіг повний. Тобто це в свою чергу ще раз підтверджує, що розробка системи підтримки прийняття рішень на основі нечіткої логіки є оптимальним рішенням для даної задачі, хоч раніше цьому питанню було приділено недостатньо уваги.

ВИСНОВКИ

Розроблена система підтримки прийняття рішень дозволяє робити аналіз бухгалтерської компанії та визначати вплив всіх ключових параметрів на ступень впевненості в інформаційній безпеці. Реалізація у вигляді веборієнтованої системи дозволяє працювати на будь-якому комп'ютері та проводити аналіз дуже швидко.

Розроблену систему можна використовувати для прийняття рішення стосовно поточної ситуації з інформаційною безпекою в компанії при моніторингу чи для поліпшення якихось показників.

REFERENCES

[1] Oshurkov S. (2025). *Bukhhalterskyi oblik v Ukraini [Accounting in Ukraine]*. URL: https://www.buhoblik.org.ua/uchet/organizacziya-buxgalterskogo-ucheta/1081-buxgalterskij-oblk.html [in Ukrainian].

[2] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001

[3] Lehenchuk S. F., Vyhivska I. M., Hryhorevska O.O. (2022). Protection of accounting information in the conditions of cyber security. *Problems of Theory and Methodology of Accounting, Control and Analysis.* Vol. 2 (52), pp. 40–46. DOI: 10.26642/pbo-2022-2(52)-40-46

[4] Hrabchuk I. L. (2018). Orhanizatsiia zakhystu oblikovoi informatsii v umovakh hibrydnoi viiny [Organization of protection of accounting information in a hybrid war]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu – Problems of Theory and Methodology of Accounting, Control and Analysis*, Vol. 3 (41), p. 20–24. DOI: 10.26642/pbo-2018-3(41)-20-24 [in Ukrainian].

[5] Vasylyshyn S. (2021). Udoskonalennia vazheliv upravlinnia didzhytalizatsiinymy ryzykamy ekonomichnoi bezpeky ta formuvannia kiberbezpeky oblikovoi systemy [Improving the levers of digitalization risks management of economic security and formation of cybersecurity of the accounting system]. *Visnyk economiky – Herald of Economics*, Vol. 1 (99), pp. 97–110. DOI: https://doi.org/10.35774/visnyk2021.01.097 [in Ukrainian].

[6] Ayedh, Abdullah (2018). Risk of computerizing accounting information systems in the Libyan bank. *South East Asia Journal of Contemporary Business, Economics and Law*, Vol. 10, Issue 1, pp. 74–79.

[7] Deborah Beard, H. Joseph Wen (2017). Reducing the Threat Levels for Accounting Information Systems, *Challenges for Management, Accountants, Auditors, and Academicians The CPA Journal, [Online]*. URL: http://archives.cpajournal.com/2007/507/essentials/p34.htm

[8] Elina Haapamäki, Jukka Sihvonen (2019). Cybersecurity in accounting research. *Managerial Auditing Journal* Vol. 34, № 7, pp. 808–834. DOI: 10.1108/MAJ-09-2018-2004

[9] Muravskyi V., Pochynok N., Farion V. (2021). Classification of cyber risks in accounting. *Visnyk ekonomiky – Herald of Economics*, Vol. 2, pp. 129–144. DOI: https://doi.org/10.35774/visnyk2021.02.129

[10] Kolisnyk O., Hurina N., Druzhynska N., Holovchak H., Fomina T. (2023). Innovative technologies in accounting and auditing: the use of blockchain technology. *Financial & Credit Activity: Problems of Theory & Practice*, Vol. 3 (50), pp. 24–41. DOI: 10.55643/fcaptp.3.50.2023.4082

[11] Otero, Angel & Tejay, Gurvirender & Otero, Luis & Ruiz-Torres, Alex (2012). A fuzzy logic-based information security control assessment for organizations. *IEEE Conference on Open Systems, ICOS 2012*. DOI: 10.1109/ICOS.2012.6417640

[12] Imeni, M. (2020). Fuzzy logic in accounting and auditing. *Journal of fuzzy extension and application*, Vol. 1 (1), 66–72. DOI: 10.22105/jfea.2020.246647.1002

[13] Alexander Báez Hernández, Debrayan Bravo Hidalgo (2020). Fuzzy Logicin Business, Management and Accounting, *Open Journal of Business and Management*, Vol.8, №.6, p. 2524–2544. DOI: 10.4236/ojbm.2020.86157

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Ошурков С. (2025). *Бухгалтерський облік в Україні.* URL: https://www.buhoblik.org.ua/uchet/organizacziya-buxgalterskogo-ucheta/1081-buxgalterskij-oblk.html

[2] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001

[3] Легенчук С. Ф., Вигівська І. М., Григоревська О. О. (2022). Захист облікової інформації в умовах забезпечення кібербезпеки. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу.* Вип. 2 (52), с. 40–46. DOI:10.26642/pbo-2022-2(52)-40-46.

[4] Грабчук І. Л. (2018). Організація захисту облікової інформації в умовах гібридної війни. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу.* Вип. 3 (41), с. 20–24. DOI: 10.26642/pbo-2018-3(41)-20-24

[5] Василішин С. (2021). Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи. *Вісник економіки.* Вип. 1, с. 97–110. DOI: https://doi.org/10.35774/visnyk2021.01.097

[6] Ayedh, Abdullah (2018). Risk of computerizing accounting information systems in the Libyan bank. *South East Asia Journal of Contemporary Business, Economics and Law*, Vol. 10, Issue 1, pp. 74–79.

[7] Deborah Beard, H. Joseph Wen (2017). Reducing the Threat Levels for Accounting Information Systems, *Challenges for Management, Accountants, Auditors, and Academicians The CPA Journal, [Online]*. URL: http://archives.cpajournal.com/2007/507/essentials/p34.htm

[8] Elina Haapamäki, Jukka Sihvonen (2019). Cybersecurity in accounting research. *Managerial Auditing Journal,* Vol. 34, № 7, pp. 808–834. DOI: 10.1108/MAJ-09-2018-2004

[9] Муравський В., Починок Н., Фаріон В. (2021). Класифікація кіберризиків у бухгалтерському обліку. *Вісник економіки.* Вип. 2, с. 129–144. DOI:10.35774/visnyk2021.02.129

[10] Колісник О., Гуріна Н., Дружинська Н., Головчак Г., Фоміна Т. (2023). Інноваційні технології в бухгалтерському облікові та аудиті: до питання використання технології блокчейн. *Фінансово-кредитна діяльність: проблеми теорії та практики*, Том 3 (50), с. 24–41. DOI: 10.55643/fcaptp.3.50.2023.4082

[11] Otero, Angel & Tejay, Gurvirender & Otero, Luis & Ruiz-Torres, Alex (2012). A fuzzy logic-based information security control assessment for organizations. *IEEE Conference on Open Systems, ICOS 2012.* DOI: 10.1109/ICOS.2012.6417640

[12] Imeni, M. (2020). Fuzzy logic in accounting and auditing. *Journal of fuzzy extension and application*, Vol. 1 (1), 66–72. DOI: 10.22105/jfea.2020.246647.1002

[13] Alexander Báez Hernández, Debrayan Bravo Hidalgo (2020). Fuzzy Logicin Business, Management and Accounting, *Open Journal of Business and Management*, Vol.8 No.6, p. 2524–2544. DOI: 10.4236/ojbm.2020.86157

Дата надходження статті до редакції: 12.05.2025
Дата затвердження статті до друку: 25.05.2025