P-ISSN 2411-1031, E-ISSN 2518-1033
Information Technology and Security. January-June 2026. Vol. 14. Iss. 1 (26)

DOI 10.20535/2411-1031.2026.14.1.365479
УДК 004.056.5:004.7

ГЕННАДІЙ ГУЛАК

ГІБРИДНА МОДЕЛЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

У статті досліджено проблему підвищення ефективності управління інформаційною безпекою підприємства в умовах динамічних кіберзагроз і невизначеності інформаційного середовища. Показано, що існуючі підходи здебільшого базуються на детермінованих або ймовірнісних моделях оцінювання ризиків, які не забезпечують достатньої гнучкості при обробці нечіткої, неповної та суперечливої інформації щодо загроз, вразливостей і стану активів. Об'єктом дослідження є процес управління інформаційною безпекою підприємства, предметом – методи та моделі прийняття рішень в умовах невизначеності. Метою статті є розробка гібридної моделі управління інформаційною безпекою на основі нечіткої логіки для підвищення обґрунтованості та адаптивності прийняття рішень. Запропонована модель інтегрує нечітке логічне виведення типу Мамдані, багатокритеріальне оцінювання стану захищеності та інтегральну модель ризику. Стан безпеки формалізовано у вигляді вектору параметрів, що включає рівні загроз, вразливостей, критичності активів і захисту, із використанням лінгвістичних змінних і функцій належності. Реалізовано механізм адаптивного вибору заходів захисту на основі бази нечітких правил. Наукова новизна полягає у поєднанні нечіткого логічного виведення з динамічною інтегральною оцінкою ризику, що, на відміну від існуючих підходів, забезпечує адаптивне формування управлінських рішень з урахуванням змін середовища в реальному часі. Отримані результати демонструють підвищення точності оцінювання ризиків та ефективності прийняття рішень порівняно з класичними моделями. Практичне значення полягає у можливості застосування моделі в інтелектуальних системах управління інформаційною безпекою підприємств.

Ключові слова: інформаційна безпека, нечітка логіка, управління ризиками, гібридна модель, прийняття рішень, кіберзагрози, адаптивні системи.

Постановка проблеми. Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням кількості та складності кіберзагроз, що безпосередньо впливає на рівень захищеності інформаційних ресурсів підприємства. Традиційні підходи до управління інформаційною безпекою базуються переважно на детермінованих або статистичних моделях оцінювання ризиків [1], які передбачають використання чітко визначених параметрів і не враховують високий рівень невизначеності сучасного інформаційного середовища.

У реальних умовах функціонування підприємства процес управління інформаційною безпекою супроводжується неповнотою, неточністю та суперечливістю вхідних даних щодо рівня загроз, вразливостей системи, критичності активів та ефективності засобів захисту [2]-[3]. Це призводить до ускладнення процесу формалізації ризиків і, як наслідок, знижує якість прийняття управлінських рішень [4]-[5]. Крім того, більшість існуючих моделей не забезпечує адаптивності до динамічних змін середовища, що є критичним у контексті сучасних кіберінцидентів.

Важливою науково-практичною задачею є розробка моделей управління інформаційною безпекою, що інтегрують кількісні й якісні показники, враховують експертні знання та забезпечують прийняття рішень в умовах невизначеності [6]-[7]. Це особливо актуально для підприємств, де інформаційні ресурси є критичними, а помилки в управлінні можуть призводити до значних втрат.

Перспективним є застосування нечіткої логіки, яка дозволяє формалізувати лінгвістичні оцінки та поєднувати їх із математичними моделями ризику [7]-[9]. Водночас існуючі підходи часто не враховують динаміку середовища, що обмежує їхню ефективність.

У зв'язку з цим виникає проблема розробки гібридної моделі управління інформаційною безпекою підприємства, яка поєднує нечітке виведення з інтегральною оцінкою ризику та забезпечує адаптивне прийняття рішень в умовах сучасних кіберзагроз.

Аналіз останніх досліджень та публікацій. Проблематика управління інформаційною безпекою в умовах невизначеності, динамічних кіберзагроз і неповноти вхідних даних активно розвивається в сучасних дослідженнях. Одним із важливих напрямів є перехід від статичних схем захисту до адаптивних моделей, які змінюють параметри або архітектуру засобів захисту залежно від поточного ризикового сценарію [7]. Саме таку ідею розвинуто в роботі M. Calvo та M. Beltrán, в якій запропоновано модель RiAS для майже реального часу, здатну адаптувати засоби захисту до різних ризикових ситуацій на основі багатошарової архітектури та ризикоорієнтованого керування [1]. Водночас ця праця зосереджена переважно на адаптації контролів безпеки й не формує повноцінного гібридного механізму прийняття рішень на рівні підприємства з використанням лінгвістичних оцінок і нечіткого інтегрального опису стану безпеки.

Помітний внесок у розвиток нечітких підходів до оцінювання ризику зробили A.A. Religia та D.N. Utama, які у 2023 році запропонували інтелектуальну модель підтримки прийняття рішень для оцінювання ризику інформаційної безпеки в публічному секторі [2]. Перевагою цієї роботи є поєднання методів підтримки прийняття рішень із нечіткою логікою та практична апробація моделі. Проте запропонований підхід орієнтований на вузьку предметну область і не враховує динамічну зміну параметрів середовища в реальному часі.

У 2024 році F. Merola та співавтори запропонували нечітку методологію оцінювання кіберризику для автомобільних систем [3]. Автори показали, що нечітка логіка дозволяє більш адекватно враховувати невизначеність експертних оцінок порівняно з традиційними дискретними шкалами. Однак дана модель має доменно-специфічний характер і не охоплює комплексне управління інформаційною безпекою підприємства як багатокритеріальний процес.

Подальший розвиток ідеї нечіткої оцінки ризиків представлений в роботі A. Mashaleh та співавторів, де запропоновано модель оцінювання ризику IoT-пристроїв на основі нечіткої логіки та методу PSO [4]. Автори враховують еволюцію сучасних загроз, проте дослідження обмежене конкретним класом об'єктів і не інтегрує оцінку ризику з механізмами прийняття управлінських рішень на рівні підприємства.

У роботі Y. Nakonechna та співавторів досліджено застосування нечіткої логіки для оцінювання ризиків багатокрокових кібератак на мережі критичної інфраструктури [5]. Запропонований підхід враховує динаміку розвитку атак і невизначеність вхідних параметрів, що є важливим кроком до адаптивних моделей. Водночас дослідження не розглядає повний контур управління інформаційною безпекою підприємства.

Окрему групу досліджень становлять роботи, присвячені використанню нечіткої логіки для виявлення вторгнень. Зокрема, C. Kim та співавтори запропонували модель FLSec-RPL для захисту IoT-мереж, яка поєднує нечітке логічне виведення та механізми виявлення аномалій [6]. Хоча результати підтверджують ефективність нечітких методів для обробки невизначених даних, такі підходи орієнтовані переважно на рівень IDS/IPS і не охоплюють стратегічне управління безпекою.

Узагальнення сучасних підходів наведено в оглядовій праці E. Krzysztoń та співавторів, де проаналізовано застосування нечітких методів у безпеці IIoT [7]. Автори відзначають ефективність нечіткої логіки для роботи з невизначеністю, однак підкреслюють фрагментарність існуючих рішень і відсутність інтегрованих моделей управління безпекою.

Сучасні гібридні підходи розглянуто в роботі A. Rehman та співавторів, де поєднано нечітку логіку з федеративним навчанням для задач кібербезпеки [8]. Хоча це демонструє

перспективність інтеграції різних інтелектуальних методів, запропонована модель має вузьке прикладне спрямування.

Близькою до тематики є робота Y. Zdorenko та співавторів, у якій запропоновано модель нечіткого оцінювання ризиків для управління інформаційною безпекою [9]. Дослідження спрямоване на удосконалення оцінювання ризику, однак не формує завершеного механізму управління, який би включав прийняття рішень і адаптацію політик безпеки.

Отже, аналіз сучасних досліджень [1]-[9] свідчить, що існуючі підходи зосереджені на окремих аспектах проблеми: оцінюванні ризиків, виявленні атак або адаптації засобів захисту. Разом із тим невирішеними залишаються такі ключові аспекти: відсутність універсальної гібридної моделі управління інформаційною безпекою підприємства; недостатня інтеграція оцінки загроз, вразливостей, критичності активів і вибору заходів захисту в єдиному контурі; обмежене врахування динаміки змін середовища та трансформації ризику в управлінське рішення на основі нечітких правил.

Формулювання цілей статті. Метою статті є розробка гібридної моделі управління інформаційною безпекою підприємства на основі нечіткої логіки для підвищення ефективності прийняття рішень в умовах невизначеності та динамічних кіберзагроз [1], [8], з урахуванням сучасних підходів до нечіткої гібридної оптимізації ризику [11]. Для цього передбачено аналіз існуючих підходів, формування математичної моделі стану безпеки з урахуванням загроз, вразливостей, критичності активів і рівня захисту, а також розробку нечіткого механізму на основі класичних підходів до моделювання ризиків [13]. Модель інтегрує оцінювання ризику та нечітке виведення в єдиний гібридний підхід, що забезпечує адаптивне прийняття рішень [23]. Завершальним етапом є обґрунтування ефективності моделі та можливостей її практичного застосування.

Виклад основного матеріалу дослідження. У межах дослідження розроблено гібридну модель управління інформаційною безпекою підприємства на основі нечіткої логіки, яка поєднує інтегральне оцінювання ризику, багатокритеріальне представлення стану захищеності та механізм нечіткого логічного виведення відповідно до сучасних підходів нечіткого оцінювання та прогнозування ризиків [15], [17]. На відміну від традиційних детермінованих підходів, запропонована модель орієнтована на роботу в умовах неповноти, неточності та лінгвістичної невизначеності вхідних даних щодо загроз, вразливостей, критичності активів і рівня реалізованого захисту.

Для формалізації поточного стану інформаційної безпеки підприємства введемо вектор стану:

$$S(t) = \langle T(t), V(t), C(t), A(t) \rangle, \tag{1}$$

де $T(t)$ – рівень актуальних загроз у момент часу t;

$V(t)$ – рівень вразливостей інформаційної системи;

$C(t)$ – критичність інформаційних активів підприємства;

$A(t)$ – рівень реалізованих засобів захисту [13].

Усі параметри нормуються на інтервалі $[0;1]$, де 0 відповідає мінімальному, а 1 – максимальному прояву відповідної характеристики.

На рис. 1 представлено архітектуру гібридної моделі управління інформаційною безпекою підприємства. Вхідні параметри формують вектор стану, на основі якого здійснюється оцінювання інтегрального ризику з можливістю його подальшої оптимізації на основі гібридних нечітких підходів [11]. Отримані значення використовуються в підсистемі нечіткого виведення для формування управлінського рішення. Реалізація захисної реакції супроводжується адаптивним зворотним зв’язком, що забезпечує оновлення параметрів системи. Така архітектура забезпечує замкнений контур управління, у якому оцінювання ризику, прийняття рішень і коригування параметрів здійснюються в режимі, наближеному до реального часу.

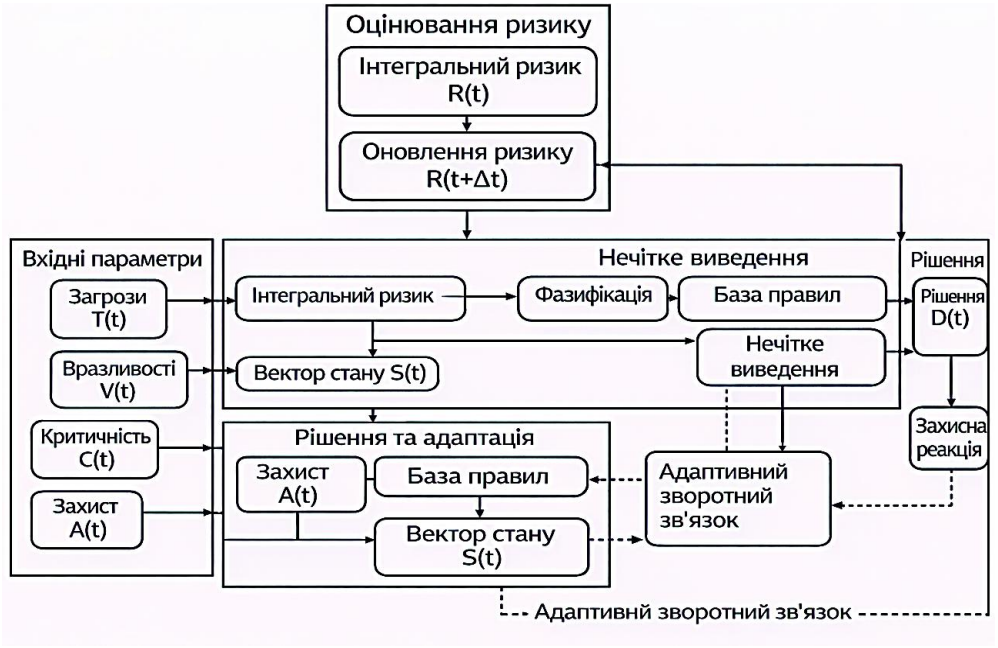

Рисунок 1 – Архітектура гібридної моделі управління інформаційною безпекою підприємства на основі нечіткої логіки

Інтегральний рівень ризику визначається як зважена сума часткових показників:

$$R(t) = \sum_{i=1}^{n} w_i \cdot r_i(t), \tag{2}$$

де $r_i(t)$ – часткові ризики, що відповідають окремим факторам (загрози, вразливості, вплив);

w_i – вагові коефіцієнти, які відображають важливість відповідного фактора, причому $\sum_{i=1}^{n} w_i = 1$.

Такий підхід дозволяє враховувати як кількісні, так і якісні характеристики ризику. Застосування вагових коефіцієнтів забезпечує можливість адаптивного налаштування моделі залежно від специфіки діяльності підприємства та пріоритетності окремих факторів безпеки. Крім того, така форма представлення інтегрального ризику дозволяє інтегрувати експертні оцінки та результати моніторингу в єдину узгоджену метрику для подальшого прийняття управлінських рішень.

Частковий ризик для і-го інформаційного активу або компонента системи доцільно подати як функцію основних факторів впливу:

$$r_i(t) = T_i(t) \cdot V_i(t) \cdot C_i(t), \tag{3}$$

де $T_i(t)$ – інтенсивність загроз для і-го компонента системи;

$V_i(t)$ – рівень вразливості;

$C_i(t)$ – критичність відповідного активу для функціонування підприємства, що узгоджується з підходами до аналізу інформаційних ризиків під час аудиту захищеності систем [4], [25].

Така форма запису дозволяє відобразити логіку ризик-орієнтованого підходу, за якої максимальний ризик реалізується за одночасної наявності значущої загрози, високої вразливості та високої критичності активу.

Однак класичне обчислення ризику не враховує нечіткість вхідних параметрів. Для подолання цього обмеження вводиться нечітка модель, у якій параметри $T_i(t), V_i(t), C_i(t)$ та $A(t)$ розглядаються як лінгвістичні змінні з відповідними терм-множинами, наприклад: “низький”, “середній”, “високий” [26]. Кожній лінгвістичній змінній відповідають функції

належності $\mu(x)$, які відображають ступінь належності конкретного значення параметра до відповідного терму.

Для формалізації нечітких оцінок використаємо трикутні та трапецієподібні функції належності. Загальний вигляд трикутної функції належності можна подати у вигляді:

$$\mu(x;a,b,c)=\begin{cases}0, & x\le a\\ \dfrac{x-a}{b-a}, & a<x\le b\\ \dfrac{c-x}{c-b}, & b<x<c\\ 0, & x\ge c\end{cases}, \quad (4)$$

де a,b,c – параметри функції належності, що визначають межі нечіткого терму [13], [26].

Така функція використовується для опису лінгвістичних оцінок типу «низький», “середній” або “високий” для показників загроз, вразливостей, критичності активів і рівня захисту. Використання трикутних функцій належності забезпечує простоту математичної реалізації та інтерпретації результатів нечіткого виведення. Крім того, вони дозволяють ефективно апроксимувати експертні оцінки параметрів безпеки, що є важливим для побудови адаптивних моделей управління в умовах невизначеності.

У випадках, коли необхідно задати розширену зону стабільної належності, доцільно використовувати трапецієподібну функцію:

$$\mu(x;a,b,c,d)=\begin{cases}0, & x\le a\\ \dfrac{x-a}{b-a}, & a<x\le b\\ 1, & b<x\le c\\ \dfrac{d-x}{d-c}, & c<x<d\\ 0, & x\ge d\end{cases}. \quad (5)$$

Така форма функції належності забезпечує більш гнучке моделювання параметрів безпеки, для яких характерна певна зона стійких значень. Застосування трапецієподібних функцій належності дозволяє виділити інтервали значень, у межах яких параметр безпеки однозначно відповідає певному лінгвістичному терму. Це підвищує стійкість моделі до незначних коливань вхідних даних і забезпечує більш надійну інтерпретацію стану системи управління інформаційною безпекою підприємства.

Наприклад, для змінної ризику $R(t)$ можуть бути визначені функції належності $\mu_{Low}(R)$, $\mu_{Medium}(R)$, $\mu_{High}(R)$, що задаються формулами (4)-(5) [9]. Це дозволяє перейти від жорстких числових меж до плавного представлення стану системи, яке більш адекватно відображає реальні умови функціонування підприємства. Процедура фазифікації вхідних параметрів полягає у визначенні ступенів належності конкретних значень до відповідних нечітких множин:

$$\mu_T^{(k)}=\mu_k(T(t)),\quad \mu_V^{(l)}=\mu_l(V(t)),\quad \mu_C^{(m)}=\mu_m(C(t)),\quad \mu_A^{(p)}=\mu_p(A(t)), \quad (6)$$

де k,l,m,p – індекси термів відповідних лінгвістичних змінних [17] та підходами data-driven моделювання в кібербезпеці [21].

Завдяки цьому кожне чітке значення показника безпеки трансформується у множину нечітких оцінок, що надалі використовуються в процедурі логічного виведення.

На основі сформованих лінгвістичних змінних будується база нечітких правил виду:

$$IF\ T(t)\ is\ High\ AND\ V(t)\ is\ High\ AND\ C(t)\ is\ High\ AND\ A(t)\ is\ Low\ THEN\ U(t)\ is\ Block, \quad (7)$$

де $U(t)$ – керуючий вплив, який визначає обраний захід захисту (наприклад, моніторинг, обмеження доступу, блокування або ініціювання агентної протидії атаці) [17], [19].

Сукупність таких правил формує механізм нечіткого логічного виведення за методом Мамдані, який може бути розширений шляхом інтеграції з нейромережевими методами виявлення атак та класифікації аномалій [20].

У загальному вигляді j-те нечітке правило системи можна подати як:

$$IF\ T\ is\ \tilde{T}_j\ AND\ V\ is\ \tilde{V}_j\ AND\ C\ is\ \tilde{C}_j\ AND\ A\ is\ \tilde{A}_j\ THEN\ U\ is\ \tilde{U}_j, \tag{8}$$

де $\tilde{T}_j, \tilde{V}_j, \tilde{C}_j, \tilde{A}_j, \tilde{U}_j$ – нечіткі терми відповідних змінних.

Ступінь активації такого правила визначається за операцією мінімуму:

$$\lambda_j = \min\left\{\mu_{\tilde{T}_j}(T), \mu_{\tilde{V}_j}(V), \mu_{\tilde{C}_j}(C), \mu_{\tilde{A}_j}(A)\right\}, \tag{9}$$

де λ_j – сила активації j-го правила. Такий підхід відповідає класичній схемі нечіткого виведення Мамдані та дозволяє врахувати одночасний вплив усіх вхідних параметрів на формування управлінського рішення.

Процес прийняття рішення включає етапи фазифікації, нечіткого логічного виведення, агрегування результатів окремих правил і подальшої дефазифікації. На етапі агрегування формується єдина вихідна нечітка множина, яка відображає сумарний результат спрацювання всіх активованих правил:

$$\mu_U^{agg}(u) = \max_j\left[\min\left(\lambda_j, \mu_{\tilde{U}_j}(u)\right)\right], \tag{10}$$

де $\mu_U^{agg}(u)$ – агрегована функція належності вихідної змінної;

λ_j – сила активації j-го правила;

$\mu_{\tilde{U}_j}(u)$ – функція належності вихідного терму цього правила [23], [26].

Саме агрегована нечітка множина є основою для подальшого визначення чіткого значення керуючого впливу. Дефазифікація виконується за методом центру ваги:

$$U^*(t) = \frac{\int u \cdot \mu_U^{agg}(u)du}{\int \mu_U^{agg}(u)du}, \tag{11}$$

де $U^*(t)$ – чітке значення керуючого впливу, $\mu_U^{agg}(u)$ – агрегована функція належності вихідної змінної.

Використання методу центру ваги забезпечує одержання узагальненого числового рішення на основі всього спектра активованих нечітких правил та відповідає загальній логіці нечітких мультикритеріальних моделей прийняття рішень [14], [24].

Гібридність запропонованої моделі полягає в інтеграції нечіткого логічного виведення з інтегральною оцінкою ризику. Зокрема, інтегральний ризик $R(t)$ використовується як один із ключових вхідних параметрів нечіткої системи, що дозволяє враховувати як кількісні оцінки, так і експертні знання [10], [27]. Узагальнена функція управління може бути подана у вигляді:

$$U(t) = f_{fuzzy}\left(S(t), R(t)\right), \tag{12}$$

де f_{fuzzy} – оператор нечіткого логічного виведення.

Для переходу від безперервного значення $U^*(t)$ до конкретного управлінського заходу доцільно ввести множину дискретних рішень:

$$D(t) = \begin{cases} d_1, & 0 \le U^*(t) < \theta_1 \\ d_2, & \theta_1 \le U^*(t) < \theta_2 \\ d_3, & \theta_2 \le U^*(t) < \theta_3 \\ d_4, & \theta_3 \le U^*(t) \le 1 \end{cases}, \tag{13}$$

де $D(t)$ $D(t)$ – кінцеве управлінське рішення;

d_1 – пасивний моніторинг;

d_2 – посилення контролю;

d_3 – локалізація загрози;

d_4 – блокування або термінове втручання;

$\theta_1, \theta_2, \theta_3$ – порогові значення інтенсивності реагування [16], [18], [22].

Така формалізація дозволяє безпосередньо пов'язати результат нечіткого логічного виведення з практичними діями системи управління інформаційною безпекою підприємства. Це забезпечує інтерпретованість результатів моделі та спрощує інтеграцію механізму прийняття рішень у реальні системи управління інформаційною безпекою підприємства.

Запропонована модель також враховує динамічний характер зміни середовища. Для цього часовий аспект оцінювання ризику доцільно описати з урахуванням змін основних параметрів системи:

$$R(t+\Delta t) = R(t) + \beta_1 \Delta T + \beta_2 \Delta V + \beta_3 \Delta C - \beta_4 \Delta A, \quad (14)$$

де $\Delta T, \Delta V, \Delta C, \Delta A$ – зміни рівнів загроз, вразливостей, критичності активів і реалізованого захисту за інтервал часу Δt,

$\beta_1, \beta_2, \beta_3, \beta_4$ – коефіцієнти чутливості системи [10], [14].

Із формули (14) випливає, що зростання загроз, вразливостей і критичності активів збільшує інтегральний ризик, тоді як підвищення рівня захисту сприяє його зменшенню, що створює основу для подальшої оптимізації параметрів ризику в динаміці на основі гібридних нечітких моделей [11].

Для узагальненої оцінки рівня захищеності підприємства доцільно також ввести інтегральний показник інформаційної безпеки:

$$I_{\text{sec}}(t) = \alpha_1 \left(1 - R(t)\right) + \alpha_2 A(t) + \alpha_3 G(t), \ \sum_{j=1}^{3} \alpha_j = 1, \quad (15)$$

де $I_{\text{sec}}(t)$ – інтегральний показник стану інформаційної безпеки підприємства;

$R(t)$ – інтегральний ризик;

$A(t)$ – рівень реалізованих засобів захисту;

$G(t)$ – рівень готовності системи до реагування на інциденти;

$\alpha_1, \alpha_2, \alpha_3$ – вагові коефіцієнти відповідних складових.

Використання показника $I_{\text{sec}}(t)$ дозволяє оцінювати не лише ризик [16], [22], а й загальний рівень захищеності підприємства, що є важливим для формування адаптивної політики безпеки.

Таким чином, запропонована гібридна модель формує завершений контур управління інформаційною безпекою підприємства, що охоплює оцінювання загроз, вразливостей і критичності активів, розрахунок інтегрального ризику, фазифікацію, нечітке логічне виведення, дефазифікацію та вибір управлінського рішення [14], [27]. На відміну від детермінованих підходів, модель враховує невизначеність даних, використовує експертні знання у вигляді нечітких правил, а також може бути інтегрована із засобами кореляції подій безпеки та SIEM-аналізу [12], [18], [20]. Це підвищує обґрунтованість рішень, точність оцінки ризиків і ефективність вибору заходів захисту та створює основу для реалізації інтелектуальної системи підтримки управління інформаційною безпекою підприємства.

Сценарний аналіз роботи запропонованої моделі. Для перевірки працездатності запропонованої моделі доцільно розглянути кілька типових сценаріїв функціонування системи управління інформаційною безпекою підприємства, які відрізняються рівнем загроз, вразливостей, критичністю активів і рівнем реалізованого захисту [14], [27]. Такий підхід дозволяє оцінити логіку формування інтегрального ризику та відповідного управлінського рішення.

У сценарії $S1$ задаються низький рівень загроз $T = 0,2$, низький рівень вразливостей $V = 0,3$, середня критичність активів $C = 0,5$ і високий рівень захисту $A = 0,8$. У цьому випадку інтегральний ризик залишається низьким, а модель формує рішення типу $D(t) = d_1$, що відповідає пасивному моніторингу.

У сценарії $S2$ розглядається середній рівень загроз $T = 0,5$, середня вразливість $V = 0,5$, висока критичність активів $C = 0,8$ і середній рівень захисту $A = 0,5$. За таких умов модель визначає середній рівень ризику та формує рішення $D(t) = d_2$, що відповідає посиленню контролю й додатковому моніторингу.

У сценарії $S3$ приймаються високий рівень загроз $T = 0,9$, висока вразливість $V = 0,8$, висока критичність активів $C = 0,9$ і низький рівень захисту $A = 0,2$. У такій ситуації формується високий інтегральний ризик, а модель генерує рішення $D(t) = d_4$, що відповідає блокуванню або терміновому втручанню.

У сценарії $S4$ задаються високий рівень загроз $T = 0,8$, середня вразливість $V = 0,5$, середня критичність активів $C = 0,6$ і низький рівень захисту $A = 0,3$. За цих умов ризик оцінюється як підвищений, а результатом роботи моделі є рішення $D(t) = d_3$, що відповідає локалізації загрози та активізації захисних механізмів.

Для узагальнення отриманих результатів сценарного аналізу доцільно подати зведені значення вхідних параметрів, рів ня ризику та сформованих управлінських рішень у табличній формі.

Таблиця 1 – Результати сценарного аналізу роботи моделі

Сценарій	***T***	***V***	***C***	***A***	**Рівень ризику**	**Рішення**
$S1$	0,2	0,3	0,5	0,8	низький	d_1
$S2$	0,5	0,5	0,8	0,5	середній	d_2
$S3$	0,9	0,8	0,9	0,2	високий	d_4
$S4$	0,8	0,5	0,6	0,3	підвищений	d_3

Наведені в табл. 1 результати демонструють, що зі зростанням рівня загроз, вразливостей і критичності активів, а також зі зниженням рівня захисту, модель послідовно підвищує інтенсивність управлінського реагування – від пасивного моніторингу до локалізації загрози та блокування.

Отримані результати сценарного аналізу підтверджують, що запропонована модель забезпечує логічно узгоджений перехід від оцінювання параметрів стану інформаційної безпеки до вибору адаптивного управлінського рішення. Це свідчить про її придатність для використання в інтелектуальних системах підтримки управління інформаційною безпекою підприємства [16], [22]. Запропонований сценарний підхід також підтверджує практичну придатність моделі для використання в автоматизованих системах підтримки прийняття рішень у сфері інформаційної безпеки підприємства.

Висновки та перспективи подальших досліджень. У статті розв’язано актуальну задачу підвищення ефективності управління інформаційною безпекою підприємства в умовах невизначеності та динамічних кіберзагроз. Запропоновано гібридну модель на основі нечіткої логіки, що поєднує багатокритеріальне представлення стану захищеності, інтегральну оцінку ризику та механізм нечіткого логічного виведення для формування адаптивних рішень.

Стан інформаційної безпеки формалізовано у вигляді векторної моделі, що враховує загрози, вразливості, критичність активів і рівень захисту. Розроблено математичний апарат інтегрального оцінювання ризику та механізм фазифікації з базою нечітких правил.

Наукова новизна полягає у поєднанні нечіткого логічного виведення з динамічною оцінкою ризику, що забезпечує адаптивне прийняття рішень. Теоретичне значення визначається розвитком ризик-орієнтованих моделей управління, практичне – можливістю застосування моделі в інтелектуальних системах підтримки рішень і моніторингу кіберінцидентів. Сценарний аналіз підтвердив її адекватність.

Перспективи досліджень пов'язані з інтеграцією методів машинного навчання для налаштування функцій належності та бази правил, розробкою програмної реалізації, а також інтеграцією з архітектурами Zero Trust і SIEM-системами.

Декларація про використання штучного інтелекту. Під час підготовки даної статті інструменти генеративного штучного інтелекту не використовувалися. Усі результати дослідження, виклад матеріалу та формулювання висновків виконані автором самостійно.

Конфлікт інтересів. Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] M. Calvo, and M. Beltrán, "A Model for Risk-Based Adaptive Security Controls", *Computers & Security*, vol. 115, Art. no. 102612, 2022. doi: https://doi.org/10.1016/j.cose.2022.102612.

[2] A. Religia, and D. Utama, "A Fuzzy-based Simple Smart Decision Model for Assessing Information Security Risk in Public Sector Organization", 2023. doi: https://doi.org/10.1109/ICISS59129.2023.10291864.

[3] F. Merola, C. Bernardeschi, and G. Lami, "A Risk Assessment Framework Based on Fuzzy Logic for Automotive Systems", *Safety*, vol. 10, no. 2, Art. no. 41, 2024. doi: https://doi.org/10.3390/safety10020041.

[4] A. Mashaleh, N. Farizah, M. Alauthman, M. Almseidin, and A. Gawanmeh, "IoT smart devices risk assessment model using fuzzy logic and PSO", *Computers, Materials & Continua*, vol. 78, no. 2, p. 2245, 2245-2267. doi: https://doi.org/10.32604/cmc.2023.047323.

[5] Y. Nakonechna, B. Savchuk, and A. Kovalova, "Fuzzy logic in risk assessment of multi-stage cyber attacks on critical infrastructure networks", *Theoretical and Applied Cybersecurity*, vol. 6, 2025. doi: https://doi.org/10.20535/tacs.2664-29132024.2.318023.

[6] C. Kim et al., "FLSec-RPL: a fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks", *Cybersecurity*, vol. 7, Art. no. 27, 2024. doi: https://doi.org/10.1186/s42400-024-00223-x.

[7] E. Krzysztoń, D. Mikołajewski, and P. Prokopowicz, "Review of Fuzzy Methods Application in IIoT Security – Challenges and Perspectives", *Electronics*, vol. 14, no. 17, Art. no. 3475, 2025, doi: https://doi.org/10.3390/electronics14173475.

[8] A. Rehman et al., "A novel hybrid fuzzy logic and federated learning framework for enhancing cybersecurity and fraud detection in IoT-enabled metaverse transactions", *Egyptian Informatics Journal*, vol. 30, Art. no. 100668, 2025. doi: https://doi.org/10.1016/j.eij.2025.100668.

[9] Y. Zdorenko, A. Yanko, M. Myziura, and N. Fesokha, "Development of a fuzzy risk assessment model for information security management", *Technology Audit and Production Reserves*, vol. 4, no. 2(84), pp. 71-79, 2025. doi: https://doi.org/10.15587/2706-5448.2025.334954.

[10] V. Sokolov, Y. Kostiuk, P. Skladannyi, and N. Korshun, "Adaptation of Network Traffic Routing Policy to Information Security and Network Protection Requirements", in *Proc. 13th Int. Sci. and Practical Conf. Information Control Systems and Technologies (ICST 2025)*, Aachen, Germany: CEUR, vol. 4048, 2025, pp. 397-411. [Online]. Available: https://ceur-ws.org/Vol-4048/paper32.pdf. Accessed on: Feb. 19, 2026.

[11] M. Erdem, and A. Özdemir, “Evaluation of Cyber Security Risk Pillars for a Digital, Innovative, and Sustainable Model Utilizing a Novel Fuzzy Hybrid Optimization”, *Computers & Security*, vol. 153, Art. no. 104394, 2025. doi: https://doi.org/10.1016/j.cose.2025.104394.

[12] Ю.В. Костюк, і П.М. Складанний, “Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів”, *Сучасний захист інформації*, №. 1(65), с. 103-118, 2026. doi: https://doi.org/10.31673/2409-7292.2026.011393.

[13] A.D. Kozhukhivskyi, and O.A. Kozhukhivska, “Developing a fuzzy risk assessment model for ERP systems”, *Radio Electronics, Computer Science, Control*, no. 1, p. 106-119, 2022. doi: https://doi.org/10.15588/1607-3274-2022-1-12.

[14] P. Skladannyi, Y. Kostiuk, K. Khorolska, B. Bebeshko, and V. Sokolov, “Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats”, in *Proc. Workshop Cyber Security and Data Protection (CSDP 2025)*, Aachen, Germany: CEUR, vol. 4042, 2025, pp. 17-36. [Online]. Available: https://ceur-ws.org/Vol-4042/paper2.pdf. Accessed on: Feb. 19, 2026.

[15] O. Mulesa, and Y. Bohdan, “Development of a fuzzy production model for assessing the degree of information security in international cooperation”, *Technology Audit and Production Reserves*, vol. 6, no. 2(80), pp. 6-10, 2024. doi: https://doi.org/10.15587/2706-5448.2024.318446.

[16] Ю. Костюк, П. Складанний, С. Рзаєва, Ю. Самойленко, та Н. Коршун, “Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid”, *Кібербезпека: освіта, наука, техніка*, № 2(30), с. 125–156, 2025. doi: https://doi.org/10.28925/2663-4023.2025.30.956.

[17] H. Upadhyay, S. Sunori, A. Mittal, and P. Juneja, “Cybersecurity Risk Prediction Using Fuzzy Logic based Models”, pp. 717-722, 2025. doi: https://doi.org/10.1109/ICOEI65986.2025.11013181.

[18] Н. Довженко, Є. Іваніченко, та Ю. Костюк, “Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей”, *Кібербезпека: освіта, наука, техніка*, № 1(29), с. 762–776, 2025. doi: https://doi.org/10.28925/2663-4023.2025.29.938.

[19] Y. Kostiuk, “Multi-Agent System for Detecting and Counteracting Attacks on the Enterprise Information System”, in *Insider Threats and Security in Corporations*, 2025, pp. 205-232. doi: https://doi.org/10.36690/ITSC-205-232.

[20] П. Складанний, Ю. Костюк, С. Рзаєва, Ю. Самойленко, та Т. Савченко, “Розробка модульних нейронних мереж для виявлення різних класів мережевих атак”, *Кібербезпека: освіта, наука, техніка*, № 3(27), с. 534-548, 2025. doi: https://doi.org/10.28925/2663-4023.2025.27.772.

[21] I.H. Sarker et al., “Cybersecurity data science: an overview from machine learning perspective”, *J. Big Data*, vol. 7, art. no. 41, 2020. doi: https://doi.org/10.1186/s40537-020-00318-5.

[22] Ю. Костюк, К. Хорольська, Б. Бебешко, Н. Довженко, Н. Коршун, та А. Пазинін, “Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень”, *Кібербезпека: освіта, наука, техніка*, № 4(28), с. 633-655, 2025. doi: https://doi.org/10.28925/2663-4023.2025.28.857.

[23] H. Fang, S. Hou, and Q. Sun, “Network Security Risk Assessment Combining Fuzzy Logic and Genetic Algorithm”, pp. 1-5, 2025. doi: https://doi.org/10.1109/ICICACS65178.2025.10967899.

[24] J.F. Pérez-Pérez, P.I. Gómez, I. Bonet, M.S. Sánchez-Pinzón, F. Caraffini, and C. Lochmuller, “Assessing Climate Transition Risks in the Colombian Processed Food Sector: A Fuzzy Logic and Multi-Criteria Decision-Making Approach”, *Mathematics*, vol. 12, no. 17, Art. no. 2713, 2024. doi: https://doi.org/10.3390/math12172713.

[25] Y. Kostiuk, P. Skladannyi, V. Sokolov, H. Hulak, and N. Korshun, "Models and algorithms for analyzing information risks during the security audit of personal data information system", in *Proc. Third Int. Conf. Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)*, Aachen, Germany: CEUR, vol. 3925, 2024, pp. 155-171. [Online]. Available: https://ceur-ws.org/Vol-3925/paper13.pdf. Accessed on: Feb. 19, 2026.

[26] S. Kerimkhulle et al., "Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things", *Symmetry*, vol. 15, no. 10, Art. no. 1958, 2023. doi: https://doi.org/10.3390/sym15101958.

[27] Y. Kostiuk, P. Skladannyi, Y. Samoilenko, K. Khorolska, B. Bebeshko, and V. Sokolov, "A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps", in *Proc. Third Int. Conf. Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)*, Aachen, Germany: CEUR, vol. 3925, 2024, pp. 249–264. [Online]. Available: https://ceur-ws.org/Vol-3925/paper21.pdf. Accessed on: Feb. 19, 2026.

REFERENCES

[1] M. Calvo, and M. Beltrán, "A Model for Risk-Based Adaptive Security Controls", *Computers & Security*, vol. 115, Art. no. 102612, 2022. doi: https://doi.org/10.1016/j.cose.2022.102612.

[2] A. Religia, and D. Utama, "A Fuzzy-based Simple Smart Decision Model for Assessing Information Security Risk in Public Sector Organization", 2023. doi: https://doi.org/10.1109/ICISS59129.2023.10291864.

[3] F. Merola, C. Bernardeschi, and G. Lami, "A Risk Assessment Framework Based on Fuzzy Logic for Automotive Systems", *Safety*, vol. 10, no. 2, Art. no. 41, 2024. doi: https://doi.org/10.3390/safety10020041.

[4] A. Mashaleh, N. Farizah, M. Alauthman, M. Almseidin, and A. Gawanmeh, "IoT smart devices risk assessment model using fuzzy logic and PSO", *Computers, Materials & Continua*, vol. 78, no. 2, p. 2245, 2245-2267. doi: https://doi.org/10.32604/cmc.2023.047323.

[5] Y. Nakonechna, B. Savchuk, and A. Kovalova, "Fuzzy logic in risk assessment of multi-stage cyber attacks on critical infrastructure networks", *Theoretical and Applied Cybersecurity*, vol. 6, 2025. doi: https://doi.org/10.20535/tacs.2664-29132024.2.318023.

[6] C. Kim et al., "FLSec-RPL: a fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks", *Cybersecurity*, vol. 7, Art. no. 27, 2024. doi: https://doi.org/10.1186/s42400-024-00223-x.

[7] E. Krzysztoń, D. Mikołajewski, and P. Prokopowicz, "Review of Fuzzy Methods Application in IIoT Security – Challenges and Perspectives", *Electronics*, vol. 14, no. 17, Art. no. 3475, 2025. doi: https://doi.org/10.3390/electronics14173475.

[8] A. Rehman et al., "A novel hybrid fuzzy logic and federated learning framework for enhancing cybersecurity and fraud detection in IoT-enabled metaverse transactions", *Egyptian Informatics Journal*, vol. 30, Art. no. 100668, 2025. doi: https://doi.org/10.1016/j.eij.2025.100668.

[9] Y. Zdorenko, A. Yanko, M. Myziura, and N. Fesokha, "Development of a fuzzy risk assessment model for information security management", *Technology Audit and Production Reserves*, vol. 4, no. 2(84), pp. 71-79, 2025. doi: https://doi.org/10.15587/2706-5448.2025.334954.

[10] V. Sokolov, Y. Kostiuk, P. Skladannyi, and N. Korshun, "Adaptation of Network Traffic Routing Policy to Information Security and Network Protection Requirements", in *Proc. 13th Int. Sci. and Practical Conf. Information Control Systems and Technologies (ICST 2025)*, Aachen, Germany: CEUR, vol. 4048, 2025, pp. 397-411. [Online]. Available: https://ceur-ws.org/Vol-4048/paper32.pdf. Accessed on: Feb. 19, 2026.

[11] M. Erdem, and A. Özdemir, "Evaluation of Cyber Security Risk Pillars for a Digital, Innovative, and Sustainable Model Utilizing a Novel Fuzzy Hybrid Optimization", *Computers & Security*, vol. 153, Art. no. 104394, 2025. doi: https://doi.org/10.1016/j.cose.2025.104394.

[12] Y.V. Kostiuk, and P.M. Skladannyi, "A Cryptographic Model of Trust in Security Events in SIEM for Intelligent Formation of Network Incidents", *Modern Information Protection*, no. 1(65), pp. 103-118, 2026. doi: https://doi.org/10.31673/2409-7292.2026.011393.

[13] A.D. Kozhukhivskyi, and O.A. Kozhukhivska, "Developing a fuzzy risk assessment model for ERP systems", *Radio Electronics, Computer Science, Control*, no. 1, p. 106-119, 2022. doi: https://doi.org/10.15588/1607-3274-2022-1-12.

[14] P. Skladannyi, Y. Kostiuk, K. Khorolska, B. Bebeshko, and V. Sokolov, "Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats", in *Proc. Workshop Cyber Security and Data Protection (CSDP 2025)*, Aachen, Germany: CEUR, vol. 4042, 2025, pp. 17-36. [Online]. Available: https://ceur-ws.org/Vol-4042/paper2.pdf. Accessed on: Feb. 19, 2026.

[15] O. Mulesa, and Y. Bohdan, "Development of a fuzzy production model for assessing the degree of information security in international cooperation", *Technology Audit and Production Reserves*, vol. 6, no. 2(80), pp. 6-10, 2024. doi: https://doi.org/10.15587/2706-5448.2024.318446.

[16] Y. Kostiuk *et al.*, "Intelligent Systems for Control and Protection in Cyber-Physical and Cloud-Based Smart Grid Environments", *Cybersecurity: Education, Science, Technology*, no. 2(30), pp. 125-156, 2025. doi: https://doi.org/10.28925/2663-4023.2025.30.956.

[17] H. Upadhyay, S. Sunori, A. Mittal, and P. Juneja, "Cybersecurity Risk Prediction Using Fuzzy Logic based Models", pp. 717-722, 2025. doi: https://doi.org/10.1109/ICOEI65986.2025.11013181.

[18] N. Dovzhenko, Y. Ivanichenko, and Y. Kostiuk, "A Method for Detection and Localization of Cyber Threats in Cloud Environments with Integrated IoT Components Based on Graph Models", *Cybersecurity: Education, Science, Technology*, no. 1(29), pp. 762–776, 2025. doi: https://doi.org/10.28925/2663-4023.2025.29.938.

[19] Y. Kostiuk, "Multi-Agent System for Detecting and Counteracting Attacks on the Enterprise Information System", in *Insider Threats and Security in Corporations*, 2025, pp. 205-232. doi: https://doi.org/10.36690/ITSC-205-232.

[20] P. Skladannyi et al., "Development of Modular Neural Networks for Detecting Various Classes of Network Attacks", *Cybersecurity: Education, Science, Technology*, no. 3(27), pp. 534-548, 2025. doi: https://doi.org/10.28925/2663-4023.2025.27.772.

[21] I.H. Sarker et al., "Cybersecurity data science: an overview from machine learning perspective", *J. Big Data*, vol. 7, art. no. 41, 2020. doi: https://doi.org/10.1186/s40537-020-00318-5.

[22] Y. Kostiuk et al., "Tools for Ensuring Information Security Against Hidden Threats in Cloud Computing Infrastructure", *Cybersecurity: Education, Science, Technology*, no. 4(28), pp. 633-655, 2025. doi: https://doi.org/10.28925/2663-4023.2025.28.857.

[23] H. Fang, S. Hou, and Q. Sun, "Network Security Risk Assessment Combining Fuzzy Logic and Genetic Algorithm", pp. 1-5, 2025. doi: https://doi.org/10.1109/ICICACS65178.2025.10967899.

[24] J.F. Pérez-Pérez, P.I. Gómez, I. Bonet, M.S. Sánchez-Pinzón, F. Caraffini, and C. Lochmuller, "Assessing Climate Transition Risks in the Colombian Processed Food Sector: A Fuzzy Logic and Multi-Criteria Decision-Making Approach", *Mathematics*, vol. 12, no. 17, Art. no. 2713, 2024. doi: https://doi.org/10.3390/math12172713.

[25] Y. Kostiuk, P. Skladannyi, V. Sokolov, H. Hulak, and N. Korshun, "Models and algorithms for analyzing information risks during the security audit of personal data information system", in *Proc. Third Int. Conf. Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)*, Aachen, Germany: CEUR, vol. 3925, 2024, pp. 155-171. [Online]. Available: https://ceur-ws.org/Vol-3925/paper13.pdf. Accessed on: Feb. 19, 2026.

[26] S. Kerimkhulle et al., "Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things", *Symmetry*, vol. 15, no. 10, Art. no. 1958, 2023. doi: https://doi.org/10.3390/sym15101958.

[27] Y. Kostiuk, P. Skladannyi, Y. Samoilenko, K. Khorolska, B. Bebeshko, and V. Sokolov, "A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps", in *Proc. Third Int. Conf. Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)*, Aachen, Germany: CEUR, vol. 3925, 2024, pp. 249–264. [Online]. Available: https://ceur-ws.org/Vol-3925/paper21.pdf. Accessed on: Feb. 19, 2026.

HENNADII HULAK

HYBRID MODEL FOR INFORMATION SECURITY MANAGEMENT OF AN ENTERPRISE BASED ON FUZZY LOGIC

The article investigates the problem of improving the efficiency of information security management of an enterprise under conditions of dynamic cyber threats and uncertainty in the information environment. It is shown that existing approaches are mostly based on deterministic or probabilistic risk assessment models, which do not provide sufficient flexibility when processing vague, incomplete, and contradictory information about threats, vulnerabilities, and the state of assets. The object of the study is the process of information security management of an enterprise, while the subject is methods and models of decision-making under uncertainty. The aim of the article is to develop a hybrid model of information security management based on fuzzy logic to improve the validity and adaptability of decision-making. The proposed model integrates Mamdani-type fuzzy inference, multi-criteria assessment of the security state, and an integral risk model. The security state is formalized as a vector of parameters, including levels of threats, vulnerabilities, asset criticality, and protection, using linguistic variables and membership functions. A mechanism for adaptive selection of protection measures based on a fuzzy rule base is implemented. The scientific novelty lies in combining fuzzy logical inference with dynamic integral risk assessment, which, unlike existing approaches, ensures adaptive formation of management decisions considering real-time environmental changes. The obtained results demonstrate an increase in the accuracy of risk assessment and the effectiveness of decision-making compared to classical models. The practical significance lies in the possibility of applying the model in intelligent information security management systems of enterprises.

Keywords: information security, fuzzy logic, risk management, hybrid model, decision-making, cyber threats, adaptive systems.

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри кібербезпеки, центр кібербезпеки, Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України; професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, Київський столичний університет імені Бориса Грінченка, Київ, Україна, ORCID 0000-0001-9131-9233, h.hulak@ukr,net.

Hennadii Hulak, doctor of science, professor, professor at the academic department of cybersecurity, Cybersecurity center, Educational and scientific institute of information security and strategic communications, National academy of the Security service of Ukraine; professor at the academic department of information and cybersecurity named after professor Volodymyr Buriachok, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine.

Стаття надійшла до редакції 25.04.2026.
Стаття прийнята до друку після рецензування 01.06.2026.
Дата оприлюднення: 26.06.2026.